SEcure Cloud computing for CRitical Infrastructure IT

Contract No 312758

Deliverable D2.5
Initial Ethics Report

AIT Austrian Institute of Technology • ETRA Investigación y Desarrollo • Fraunhofer Institute for Experimental Software Engineering IESE • Karlsruhe Institute of Technology • NEC Europe • Lancaster University • Mirasys • Hellenic Telecommunications Organization OTE• Ayuntamiento de Valencia • Amaris

Document control information		
Title	Initial Ethics Report	
Creator	KIT legal	
Editor	Frank Pallas, Silvia Balaban	
Description	This document identifies the main ethical problems and derives respective safeguards for the SECCRIT project	
Classification	☐ **Red** – Highly sensible Information, limited access for: ☐ **Yellow** – restricted limited access for: ☐ **Green** – restricted to consortium members ☒ White – public	
Reviewers	☐ AIT ☐ ETRA ☐ IESE ☒ KIT ☐ NEC	☒ ULANC ☐ MIRASYS ☒ OTE ☐ VLC ☐ AMARIS
Review status	☐ Draft ☐ WP Manager accepted ☒ Co-ordinator accepted	
Action requested	☐ to be revised by Partners involved in the preparation of the Project Deliverable ☐ to be reviewed by applicable SECCRIT Partners ☐ for approval of the WP Manager ☐ for approval of the Project Co-ordinator	
Requested deadline	18/12/2013	

Versions			
Version	**Date**	**Change**	**Comment/Editor**
1	14/11/2013	Initial full version	Frank Pallas / Silvia Balaban
1-revdh	26/11/2013	Comments by DH	David Hutchison
2	06/12/2013	Incorporation of reviews	Silvia Balaban / Frank Pallas
3	16/12/2013	Incorporation of minor comments from second review round	Frank Pallas / Silvia Balaban
4	17/12/2013	Minor editorial fixes	Roland Bless

Abstract

The concept of cloud computing also affects the ethical domain. Whereas the law is setting regulations, framed by a governing power and which have to be accepted by everyone, ethics are the reflection on morals, forming the basis for a human interrelations. Many concerns and doubts about cloud computing have been raised, particularly concerning the fact that unwanted consequences like, for example, the transmission to non-authorized third parties or even a more general “loss of control” have not yet been recognized. Therefore, it not only becomes legally important to estimate the effects associated with the use of cloud computing but also ethically more urgent to identify potential risks. This is the reason why D2.5 focuses on ethical aspects that go beyond those already covered in the legal deliverables, D2.2 and further on in D2.7. This document therefore outlines the rather abstract ethical challenges of the project’s activities as well as the subject in general. This serves two main goals: on the one hand, providing a sound basis to ensure that the activities undertaken during the project are in line with the established ethical values, and explaining how this will be ensured; and on the other hand to provide first high-level considerations to serve as a starting point for discussing the regulatory framework relevant for cloud computing. In addition, this deliverable provides initial deliberations about a transformation into this regulatory framework, and, in so doing, links the ethics report with the deliverable D2.2 on the legal fundamentals already delivered in M6. Finally, this document shall also serve as guiding input for the Security Group when assessing security sensitive deliverables.

Table of Contents

1 Motivation, Scope, Methodology and Structure

It is an integral aspect of the SECCRIT project that relevant ethical issues are identified and integrated from the very beginning. Only then can it be ensured that potentially problematical ethical aspects are appropriately taken into account from the ground up during the design and implementation of the technologies that are to be developed. A sound analysis of at least the most relevant ethical issues and their reflection within technical concepts is thus required. Incorporating ethical considerations from the beginning, in turn, will significantly reduce the risk of the technologies not being in line with fundamental ethical values. This should help avoid essential ethical conflicts from arising during later project phases which could, in the end, prevent the developed technologies from being applicable in practice. The ethical considerations identified here will thereby serve the practical applicability of technological concepts developed in SECCRIT.

Particularly with regard to cutting-edge information technology, data protection considerations usually feature prominently in ethical deliberations. These are, however, well-reflected in the respective legal data protection framework. This legal framework, in turn, is extensively covered in deliverable D 2.2 already finished in M6, to be further considered throughout task T 2.4 (“Legal support for research activities”) and to be reported on in the forthcoming deliverable D 2.7. Ethical considerations on issues of data protection in the strict sense as covered by data protection legislation will therefore not be addressed in the following parts of the present deliverable.

However, ethics also cover more general aspects of moral, giving a basis for human living. Ethics as a critical reflection on how to behave are in – contrast to the law – not explicitly codified. Moral and ethics derive from the Latin word *mores* and the Greek word *ethos*, which signify the beliefs and customs guiding the interaction and conduct amongst human beings. Even if every legislation is (or, at least, should be) based on ethical considerations, the law covers in most cases only a short part of ethical problems. It might therefore very well happen that obeying the law does not automatically imply that the acting is also ethically acceptable. Laws for instance can also change in line with changed governmental preferences and views, while the morals and customs are transcend. On the other hand, novel technologies might not always immediately be incorporated within legal frameworks while ethical considerations already provide a direction for socially acceptable conduct. Finally, legal provisions are enforced through governmental sanctions in case of noncompliance, while ethical misconduct does not always lead to explicit punishment (aside from societal disrespect).

In the context of SECCRIT, there are numerous ethical questions which have to be taken into account and which go well beyond data protection in the strict sense. In particular, these arise from the employed use-cases of video surveillance of critical infrastructures and urban mobility services. Especially with regard to video surveillance, there is already a well-understood body of knowledge on its ethical dimension which will therefore be reflected in the following sections. Much less broad is the body of existing knowledge on the ethical dimension of (semi-) automated control of urban mobility, which will therefore also be addressed.

Different from other EU-funded projects such as INDECT[1], VideoSense[2], or the German Project CamInSense[3], SECCRIT is, however, not primarily a surveillance project. First and foremost, SECCRIT is a project about technologies for secure cloud computing for critical infrastructure IT. It would therefore be of questionable value to undertake extensive deliberations on the ethical dimension of (semi-) automated control of urban mobility and – in particular – video surveillance systems *as such* even though these are clearly not the primary subjects of the project. On the one hand, such considerations are to be left to projects focusing on research in these domains. On the other hand, video surveillance and urban mobility systems do clearly play a certain role as

[1] See http://www.indect-project.eu/

[2] See http://videosense.eu/

[3] See http://www.iais.fraunhofer.de/5925.html

specific use cases for the cloud computing technologies to be developed in SECCRIT and should therefore not be factored out completely.

In a nutshell, the ethical considerations to be studied in the following sections must, on the one hand, pay regard to the ethical problems and conflicts possibly arising from the employed use cases of video surveillance and urban mobility systems while, on the other hand, keeping focus on the project's development of technologies that enable secure cloud computing for critical infrastructure IT. In order to serve these two partially conflicting goals best, this document employs a "triangulation approach" to identify ethical aspects that are specific to *cloud-based* video-surveillance and urban mobility services. In a first step, the most relevant ethical aspects of video surveillance and (semi-) automated urban mobility systems are summarized. This is done in section 2. Following these fundamental considerations, several characteristic qualities of cloud computing with particular relevance in matters of potential ethical impact are identified – again as discussed in the scientific literature – even if research on "ethical aspects of cloud computing" is still in its infancy and has not yet reached a state of consolidation. A gathering of currently discussed ethical aspects of cloud computing is provided in section 3. The issues thereby identified then form a "delta" between cloud-based and non-cloud systems in matters of the ethical dimension, and can serve as a starting point for putting the rather generic ethical considerations on video surveillance and urban mobility systems into a SECCRIT-specific context. Section 4 does exactly this and identifies SECCRIT-specific potential ethical problems of *cloud-based* video surveillance and *cloud-based* urban mobility services, which are not yet adequately covered in the existing corpus of scientific literature and discussion.

For each of the identified SECCRIT-specific potential ethical problems, we then discuss how it can be addressed properly to ensure that the project is always acting in line with ethical values. Where necessary, this is also done for the rather generic ethical problems that arise from video surveillance, (semi-) automated traffic control and cloud computing. As a result of these discussions, safeguards ("SGs") are developed to be employed throughout the remainder of the project in addition to the measures taken in order to ensure legal compliance. Where applicable, we discuss whether the identified SECCRIT-specific problem already hint at more generic needs or even approaches for further normative regulations in matters of "ethical cloud computing" in general; these might be investigated in more detail during further activities on legal and ethical aspects. Finally, section 5 summaries this deliverable.

2 Ethical aspects in SECCRIT use cases

As depicted in the description of WP 6, two different demonstrators / use cases are inherent parts of the project in order to validate the practical applicability of the technologies to be developed in SECCRIT. The first demonstrator, particularly covering aspects of secure "storage and processing of sensitive data" in the cloud, will be based on video surveillance data. The second refers to "hosting critical urban mobility services" and especially focuses on questions of validation processes.[4] Following the "triangulation approach" outlined above, the main ethical aspects discussed for video surveillance and for (semi-) automated mobility services will therefore be gathered as a first step.

2.1 Ethical problems of video surveillance

As outlined above, this section gives a compact overview of the most important ethical aspects of video surveillance in general. Even if SECCRIT is not a video surveillance project, these will have to be carefully taken into account in the course of evaluating potential technologies for secure cloud computing in the context of video surveillance, in order not to violate fundamental ethical values. Furthermore, these serve as a basis for identifying potential ethical challenges of cloud

[4] „Electronic proofs" etc., see, e.g., D 2.2, section 2.2.2.

computing that would probably not have been seen without reflecting on the employment of this technology within a specific and sensitive application context.

Often-mentioned ethical aspects of video surveillance include the problem of people not being aware of being observed, the problem of well-informed statements of consent (or especially dissent) being hardly possible, the trend of surveillance being conducted excessively as compared to the original purpose, and the risk of video surveillance being conducted without a legitimate basis; for good reasons, these are addressed in existing national[5] data protection legislations. Such questions are therefore well covered by the principles-based considerations in the respective deliverables on legal aspects and will not be explicitly addressed here. It is, however, without any doubt that the respective legal givens have to be carefully taken into account during the implementation of the evaluation use case. The close coordination on the concrete implementation with responsible data protection authorities, reported in deliverable D 2.4, also requires that such aspects of data protection in the strict sense need to be appropriately addressed.

This being said, there are, however, further ethical aspects of video surveillance that go beyond questions of data protection. These have a long track of extensive scientific coverage that has been accompanying technological progress for decades. The history of ethical considerations on surveillance in general goes back even further, at least to Jeremy Bentham's well-known "**Panopticon**" concept (Bentham 1791), which refers to a specific architectural building structure explicitly targeted at manipulating inmates' behaviour and habits.

First described for prisons, manufactories, schools and other buildings where "*persons [..] are to be kept under inspection*", the concept consists of two factors. First is an architecture that allows any inmate to be seen at any time and without any exception from one central place of observation, for example a tower surrounded by circularly arranged cells with gratings facing to the centre ("*centrality of the Inspector's situation*", Bentham 1791, p. 23). This ensures that no "in-cell behaviour" can be hidden from an observer actually looking into the right direction. The second factor consists of a mechanism that prevents inmates from seeing whether an observer in the centre is currently looking into their direction or even whether an observer is actually present at all ("*seeing without being seen*", ibid., p. 23). This could, for example, be ensured by strong lights directed from the centre to the cells so that inmates are blinded when looking at the centre.

The ethically relevant impact of such surveillance situations is quite obvious: The mere knowledge of *possibly* being monitored makes people adapt their behaviour to the (assumedly) desired, normal, or least conspicuous-looking one and thereby leads to strong conformism. While Bentham himself intended exactly this for the context of prison inmates and other persons that are to be observed, and praised the so-called panopticon effect as a way for reaching a state of socially desirable behaviour. The effect is today usually ethically deprecated as it leads to the observed individuals having **zero privacy** (which is something completely different from "data protection") **even in most private situations** and because it raises the **risk of people negating themselves**, their beliefs and their needs in favour of being conformant with what the observer requests from them just to avoid punishments or even more subtle acts of enforcement.

The whole concept of the panopticon does, of course, apply to today's video surveillance in the same manner – and is of course the reason why most surveillance cameras are usually much larger and much more visible than technically required.[6] The **risk of people adapting their**

[5] In Germany, this is, for example, done in § 6b of the national data protection law. For a brief respective legal assessment of surveillance technologies as considered herein, see, for instance, Roßnagel, Desoi and Hornung (2012).

[6] The opposite problem of unnoticed, secret video surveillance, in turn, refers to traditional risks from the field of data protection. As mentioned above, these will not be addressed explicitly here as they are well covered in the respective legal deliverables (see, for instance, the respective sections on transparency in D 2.2). Nonetheless, the noteworthy dilemma of any planned use of video surveillance between possibly infringing

behaviour to a state of conformism might be neglected as actually being a "risk" as long as punishment or other acts of enforcement are only exerted and expected in cases of behaviour that is definitely not accepted by society (e.g. in case of robberies, where the deterrent effect will usually be highly welcome). But depending on the political situation (which might, nota bene, be subject to change), the same systems can also be used to restrain people from, for instance, demonstrating against the government. The panopticon effect of people adapting to some (assumed) state of "target" behaviour is therefore one of the most important ethical risks of video surveillance in general, independently from the concrete technical design and capabilities.

Current surveillance technologies do, however, differ from the original panopticon concept in several regards. Under the term of "new surveillance", Marx (2002) identifies some specific characteristics of modern, **technology-mediated surveillance** as opposed to the traditional concept. First of all, modern surveillance is in most cases done by technological means, thereby **heightening the observer's capacity for recognition** (omnipresent video-cameras, heat sensors, etc. and, not to forget, the possibilities of modern data processing). Based on these technological means, current surveillance practices **break up the previously existing strong ties in matters of time, location and context** between the monitored behaviour, its actual recognition and interpretation, and the reactive response. While in the buildings described by Bentham, behaviour, notice, interpretation and reaction follow each other immediately and happen in direct local proximity, today's surveillance technologies allow the recording of plenty of manifold facts first and to analyse them later – be it on a periodic basis or in the case of specific events. And finally, it is a core characteristic of the so-called "new surveillance" that data (or **information of multiple kinds and from multiple sources) is integrated and combined**, leading to a much more encompassing basis for in-depth analysis. The fact of data being shareable and often shared among different parties strengthens this effect even further. This, in turn, lets the observers discover connections between different bits of information that would otherwise have been unnoticed and thereby potentially derive all-embracing images about personality and activities of those under surveillance – or rather, those under analysis.

Beyond these, there are plenty of further dimensions that distinguish current surveillance practices and technologies from former ones. Marx (2002) alone mentions 27 of them and there will presumably be more. An ethical assessment of all aspects of this shift is hardly doable in a non-extensive way, especially because any of the changed characteristics can, depending on the context, lead to ethically welcome as well as undesirable implications. Marx himself gives the example that, "*[t]hrough offering high quality documentary evidence and audit trails, the new surveillance may enhance due process, fairness and legitimacy*" (p. 22) while the same evidence could unquestionably also be used for ethically undesirable purposes. Furthermore, the ethical assessment of a concrete application of a certain technology also has to take into account the respective local cultural values.[7]

Due to these highly context-dependent implications, Marx (1998, p. 174) proposes an exhaustive "*set of questions to help determine the ethics of surveillance" without even trying to make strict normative arguments. Instead, he highlights* (ibid., p. 182):

> *„in matters so complex and varied we are better served by an imperfect compass than a detailed map. Such a map can lead to the erroneous conclusion that ethical directions can be easily reached or to a statement so far in the stratosphere that only angels can see and apply it."*

upon individuals' data protection rights (unnoticed surveillance) and unwillingly pushing individual behaviour towards conformism (clearly visible surveillance) will not be ignored. For the cases covered in project SECCRIT, however, this dilemma does not arise practically as data protection laws require any video surveillance to be announced and be made visible to the potential subject of surveillance.

[7] For a vivid depiction of significant differences in the perception of social acceptability in matters of privacy even between the closely related cultures of Europe and North America, see especially Whitman (2004).

Therefore, these "compass questions" provided by Marx can very well guide the process of reflecting on the ethical dimension of a concrete application of technology-based surveillance and will therefore be applied throughout the establishment of the video demonstrator. They are reproduced in They are reproduced in section 0 (Annex).

This leads us to the first safeguard that is to be applied throughout the establishment of both demonstrators in order to ensure that fundamental ethical values are kept in mind and appropriately addressed:

- **SG1 – Compass Questions: The "compass questions" reproduced in section 0 (Annex) will be applied in the design and implementation of the demonstrators.**

The strong context dependence notwithstanding, one aspect of the "new surveillance" as described by Marx is unquestionable: through the possibilities for strong integration of different sources of information, for their combined analysis and for their exchange amongst different observing parties, the fact that surveillance is increasingly based on technology leads to a significant strengthening of the observers' informational position, as opposed to the observed. This is even truer for the next qualitative shift of surveillance practices as noted by Graham and Wood (2003) under the term **"*digital* surveillance".**

Graham and Wood argue that novel digital surveillance technologies and practices, as opposed to former video surveillance technologies and practices, not only increase the amount of video data being collected and of areas being covered significantly but that these technologies and practices also lead to changed social practices and a novel category of ethical problems: Of particular relevance in this regard is the shift towards **automated analysis** ("algorithmic video surveillance", "algorithmic CCTV", Graham and Wood, 2003, p. 231, 235ff) with backend systems fed by digital cameras (and potentially other kinds of sensors) automatically analysing recorded data in order to recognize individuals and their movement, thereby allowing for far more **"meaning" to be automatically extracted** within video surveillance systems. This general concept can come in different flavours from comparing faces, or gaits of people walking along the street, against a "watch list" database of to-be-recognized individuals[8] over the automated movement tracking of single persons across areas covered by different cameras and other sensors to the automatic "detection" of "suspicious" or otherwise unwanted behavioural patterns that can, for instance, be used for social segregation within privately controlled, semi-public areas like a mall (Kang and Cuff, 2005, sect. IV.A).

In this model, decisions based on the video data captured by surveillance systems thus increasingly shift from being made by human operators under (conscious or unconscious) comprehension of social values as well as human experience and discretion, to a mode where decisions are made or at least "suggested" automatically by means of algorithms explicitly directed at the detection of certain "patterns" that define, for instance, "usual", "unwanted" or "suspicious" behaviour. It is, however, **questionable to what extent such codified patterns actually match with what a well-trained human observer would identify as noteworthy**. Even worse, any algorithmic assessment is, at least to a certain extent, made on the basis of "*social and political assumptions that software producers embed (consciously or unconsciously) into their algorithms years before and thousands of miles away from the site of application*" (Graham and Wood, 2003, p. 242), provoking considerable "misinterpretations". And finally, the actual capabilities of technology are all too often strongly overestimated by the responsible parties. In the end, this leads to the "recognition" of a person as behaving "unacceptably" or any other process of "meaning extraction" **not being critically questioned in the light of human weighing and the social assumptions applicable to the respective context**. Instead, the technological assessment is all too often simply taken as a "given fact", leading to a **significant risk of mistreatment**.

[8] See, for example, Graham and Wood (2003, p. 236).

To conclude, modern video surveillance technology in particular induces the risks of

- significantly reducing privacy of the observed,
- fostering conformism instead of individualism,
- leading to strong inequalities in matters of informational power between observer and observed through integration of multiple sources of information and their collection over long periods,
- automated analysis being performed on the basis of potentially defective or inappropriate algorithms without critical human reflection in the light of the application context's social givens, and of
- results of automated analysis being taken "as an objective fact" instead of "as a hint", potentially inducing significant mistreatment.

Even if the voluminous literature on surveillance, technology and their ethical implications discusses innumerable further aspects emerging from domains such as workplace surveillance (e.g., Hansen 2004), urban planning (e.g., Koskela 2000) or Gender Studies (e.g., Monahan 2009), these are the most important ethical aspects of video surveillance that serve as the basis of discussion for the remainder of this deliverable.

Moreover, it has been pointed out that the ethical impact of surveillance technology significantly depends on the concrete application scenario and context. As one and the same technology can prove ethically questionable as well as welcome depending on its application context, generic considerations about ethical implications of a given technology as such can never be exhaustive and must always be complemented by a context-specific assessment. This will be done throughout the establishment of the demonstrator based on the table of the "compass questions" and reported on in the final ethics report due in M 12 (D 2.8).

2.2 Ethical problems concerning (semi-) automated traffic management services

Different from the intended evaluation demonstrator of cloud-enabled video-surveillance, the subject of the second demonstrator holds – at least at first sight – no obvious ethical challenges going beyond those already discussed above. Of course, (semi-) automated traffic management services could also include surveillance equipment monitoring the current traffic situation, for example. This would in turn induce all the risks already mentioned above, including the generation of **movement profiles** based on recorded individuals or number plate recognition.

Beyond video surveillance, comparable problems could in the future also emerge from advanced models of **Car-2-X-communication being integrated with traffic control systems.** Within such systems, there exists an inherent risk that single and explicitly identifiable vehicles (and, thereby, their users) are subject to **tracking and monitoring**. An early form of such mechanisms which could very well also be integrated into a traffic control system are congestion detection mechanisms based on the density and movement speed of mobile phones like the one already employed by Google: Based on a multitude of Android mobile phones repeatedly sending their location data to a centralized platform, it is possible to derive a current traffic situation in potentially higher accuracy than with specialized sensors being installed near to the roads and nearly without any specific investment necessary. While this provides a technically interesting option for gathering current information about traffic flow, it is obvious that such a model induces the significant risk of the movement of individual persons being tracked without their consent and/or knowledge – at least as soon as these information are not strictly **anonymized or pseudonymized**. Were such technologies integrated in future traffic control systems without strong anonymization techniques, this would significantly strengthen a whole group of risks emanating from public bodies being able to track and locate individuals in real time as well as in retrospect. Such aspects would, however, already be covered either by existing data protection

laws or by the ethical considerations on video surveillance laid out above and would therefore not call for specific considerations about the second demonstrator here.[9]

Beyond aspects that are reasonably attributed to the fields of data protection and video surveillance, the first aspect of (semi-) automated traffic management that could be extracted as being of possible ethical relevance from existing literature refers to the risk of **social discrimination / unequal treatment** based on rules that are ethically questionable. Graham and Wood (2003, p. 238f), for example, mention London's so-called "*congestion charge*" as well as "*private premium highways*" being erected in Toronto, Los Angeles, etc. as examples of traffic infrastructure that are practically accessible only to a selected portion of all drivers (those who can afford to regularly pay for using certain roads, for example). An example pointing in the opposite direction is that of so-called "*high-occupancy highway lanes*" which are well-known in the US and may only be used by cars with a minimum of two, three, or even four occupants, thereby introducing an incentive not to use cars alone and thus not to contribute to traffic congestion more than necessary. Generally speaking, both directions of differential treatment raise questions of ethical acceptability.

Furthermore, ethical questions also arise from the possibility of **enforcing the respective rule sets automatically through technology**. If, for instance, a (semi-) automated traffic management system would block any driver not able to pay an extra fee or not equipped with specific technical devices from entering a city centre during certain "high-congestion times" by means of physical barriers (comparable to the toll stations present on some European highways), this would induce the risk of **exceptions** which would traditionally have been unquestionably accepted **not being possible anymore** due to the usual **strict mode of technology-based enforcement**. As long as no alternative path that allows "overriding" of technical constraints exists, this would raise severe ethical questions regarding, for example, system behaviour in unforeseen cases of emergency.

Besides the risks of technology-based differentiation, and of unquestionably accepted rule-breaking made impossible because of absolute technological enforcement, no ethical challenges specific to the demonstration use case of traffic control could be identified that go beyond surveillance aspects already covered in section 2.1. Depending on the concrete design for the evaluation demonstrator, the first-mentioned aspects will have to be kept in mind and, if applicable, to be addressed appropriately throughout the evaluation phase to prevent ethically questionable uses of the demonstration system. The latter aspects from the domain of data protection in the strict sense as well as from the broader area of surveillance, in turn, will in all likelihood play a key role for the concrete demonstrator and will therefore be addressed comparably to that of the video-surveillance demonstrator, i.e., by means of sound legal assessment and on the basis' of Marx's compass questions. Finally, the close cooperation with responsible data protection authorities reported on in D 2.4 also ensures at least the most relevant ethical and data protection issues to be properly accounted for.

3 Characteristics of Cloud Computing with Potential Ethical Impact

After the generic ethical aspects relevant for the concrete evaluation demonstrators planned in SECCRIT have been laid out so far, we now come to the main subject of the project and its potential ethical impact, namely cloud computing. As outlined in the DoW, these considerations will – besides also ensuring that all project activities are in line with established ethical values – provide "first high-level considerations that shall serve as a starting point for discussing the further development of the regulatory framework relevant for cloud computing." Furthermore, some first

[9] It is, however, also clear that the approach of ethical assessment on the basis of the "compass questions" developed by Marx (1998) should also be applied to this demonstrator.

"concretizing deliberations regarding the transformation into the relevant regulatory framework" are to be derived. This will be done in the subsequent sections.

The identification of concrete characteristics of cloud computing that have potential ethical impact is subject to two main constraints: First, the whole field of cloud computing is – as compared to other technological domains – still in its infancy and especially lacks broad and consolidated coverage in the socio-technical domain. Different from, for example, surveillance technology, there is thus no well-established body of scientific discussion, categorization or classification of ethical aspects having to be considered in the context of cloud computing. Even if taking into account some early findings that are currently emerging in this regard, the following considerations are therefore necessarily of explorative nature, too.

Second, cloud computing is also subject to the well-known problem of general-purpose technologies being hardly assessable in matters of their expectable implications, including those of ethical relevance. Technologies like cloud computing, which basically do not carry an inherent "target application" but can rather be employed for a broad variety of ethically welcome or objectionable purposes, are particularly subject to the control dilemma prominently described by Collingridge (1980): as long as a certain technology is in its infancy, its (social) implications can hardly be assessed reliably. On the other hand, once the technology is mature enough for making reliable estimations on its implications, it is usually too late to actually influence development in order to achieve (socially) welcome outcomes. As ethical considerations do, like legal ones, always require a concrete application scenario (or "a case") for being meaningful, ethical considerations about new technologies are usually conducted on the basis of prognostic scenarios ("*scenario-based technology assessment*"). This, however, turns out to be of limited explanatory value with regard to general-purpose-technologies due to the prognosis- and control-dilemma, leading to the problem of (social) implications of general purpose technologies being hardly assessable at all in a reliable manner (Weber 2010). Nonetheless, a structured analysis of the most significant characteristics of a certain technology may at least allow for an identification of *possibly* expectable implications – albeit with the risk of significantly overestimating some aspects and overlooking others.

In the light of these two constraints, we will in the following identify *possible* problems of ethical relevance that could – given the technological characteristics of cloud computing – be induced by a switch from traditional computing models to cloud-based ones. In so doing, we will explicitly exclude aspects that are already covered in deliverable D 2.2 on legal fundamentals. In particular, this refers to concrete questions of data protection law which are already subject to current legislation. Instead, we will concentrate – in line with the intentions from the DoW –on higher-level aspects that will presumably cause problems not adequately addressed by the current regulatory status quo.

In the subsequent sections, these generic considerations will then be projected onto the scenario-specific deliberations already outlined above in order to generate more concrete ideas on the social implications of cloud computing being used within ethically relevant applications.

3.1 Loss of Control

The first foreseeable potential problem of ethical relevance induced by cloud computing emanates from the fact that the outsourcing of computing resources leads to a shift of control over these resources. Whereas data, processes etc. had formerly been residing on a local infrastructure, under cloud computing they will have relocated to the cloud provider. This necessarily implies at least a partial loss of control over them as the cloud user can exert control only via well-defined interfaces defined by the cloud provider. The cloud provider, in turn, is at least basically able to take notice of, or – depending on the concrete technical givens – even

manipulate data as well as processes without being observed.[10] In the end, it is basically the cloud provider that has the ultimate control over data and processes and, in addition, ultimately determines the further (technical and non-technical) conditions under which data processing takes place.

The risk of control loss becomes even more significant in cases of interconnection between multiple cloud service providers. The ongoing trend towards end-user services being composed from other services provided by different cloud providers leads to the apparent problem of actual responsibility for the ultimate outcome being vaguely distributed across a multitude of involved parties.

Given this possible shift of control, forcing the cloud user to be the only one accountable for any kind of malfunction or misbehaviour by its contract partner (as is basically done by the current legal framework) raises concerns of appropriateness and fairness. Especially for cases of possible intrusion by non-authorized third parties, or of possible failures or, indeed, corruption[11], it would surely be important to prove what exactly went wrong. This is particularly true for cases with services from different providers being integrated with each other where, without technical mechanisms of proof, it would be impossible to attribute unwanted outcomes to the party that actually caused it. Ultimately we want to avoid unfair risk distributions and, in consequence, economically inefficient outcomes.

The potential loss of control, however, also induces ethical risk in areas much more closely bound to the individual. Whitman (2004), for example, points out that at least the European understanding of "privacy" for large parts refers to the individual's "rights to control your public image, rights to guarantee that people see you the way you want to be seen." With regard to personal data as covered by European data protection laws, this implies the need for exerting control over data that can unquestionably influence this "image" that is well-covered in the term of "informational self-determination": Any person is then basically in control over data that might influence the image that others have about her or him. Of course, this individual control following pure self-determination is already limited in traditional models of data usage and is – within well-defined boundaries defined by data protection laws – to a large extent exerted by the respective holder of the data (in legal terms, the controller). But within this traditional model, the data subject also has a couple of rights against the controller; and the controller, in turn, has a couple of responsibilities and must follow several comparably strict obligations to ensure that the individual has the largest possible control over the ultimate handling of data that forms her or his "person image".

In the case of cloud computing and especially in those cases involving the complex interconnection of services provided by different parties[12], this control over data that influences the person's image tends to decrease significantly. Instead of actually being in control the data subject will therefore increasingly have to rely on other mechanisms like "trust" regarding the question of whether their data falls into the wrong hands. The "right to control one's public image" thereby could become significantly harder, if not impossible, to be actually exerted for the individual. In order to prevent such a technology-deterministic fading of enforceability of fundamental rights, mechanisms should be developed that render the aforementioned "trust" back into actual control over the dissemination of personal data.

In any case, the generic risk of control loss can be identified as one possible source of changed socio-technical givens introduced by an increased use of cloud computing. This change risks the emergence of new ethical challenges, whereas questions about fairness and about the possibility

[10] Notably, this also includes the risk of the cloud provider secretly exploiting the respective data for own purposes. See, for instance, Cavoukian (2008).
[11] See Paquette, jaeger and Wilson (2010).
[12] See also Timmermans, Stahl, Ikonen and Bozdag (2010, p. 5).

of controlling the use and dissemination of personal data will presumably be of particular relevance.

3.2 Lack of transparency

Closely coupled with possible loss of control is the risk that processes of data handling increasingly lack transparency because of cloud computing. Transparency, as understood here, refers to the ability to know and retrace what actually happens within a system or service being used. Cloud computing, however, often assumes that services are used as "functioning black boxes" that exempt the user – be it a private person or an organization – from having to care about the internal details.

This reduction, or loss, of transparency again has potential implications with regard to the above-mentioned European understanding of privacy. If an individual cannot know and retrace how her or his personal data will be handled, it becomes nearly impossible to exert control over this data handling. Generally speaking, the same problem also applies to organizations using cloud services. Without possibilities to assess the internals of a used service, it can hardly be ensured that obligations of any kind (legal, business, corporate ethics, …) are met in practice.

Again, mechanisms must therefore be developed in the future that do, at least to a certain extent, re-establish transparency of used services on demand. In particular, such mechanisms must ensure that the cloud user can check what is actually happening to certain data transferred to the cloud and if the cloud is actually performing as intended. Key requirements for such mechanisms are the establishment of transparency about how the data will be handled and the exposure of different responsibilities, especially for cases with multiple actors being involved in a certain process (see above discussion on "loss of control"). This goes in the direction of one of the core challenges of the SECCRIT project as evidence and data protection have opposing goals when recorded actions cannot be revealed to any person, unless data protection regulations are totally ignored and therefore violated. Consequently, it seems plausible to distinguish between recording and exposing transparency information, whereas simultaneously evidence and data protection law must be adhered to.

3.3 Transfer across cultural and legislative boundaries

As cloud services can be located in any part of the world, cloud computing increases the risk of data being exposed to different cultural settings.[13] This raises the risk of an individual's data not being treated in conformance with his/her own cultural and ethical values, but rather in the light of the social context in which the storage or processing is taking place. In a comparable way, this is also true for the legislative setting, where individuals can no longer rely on the national legal framework with which they are familiar, but rather bear the risk of their data being handled on the basis of regulations that they do not know and probably would not accept if they were aware of them.[14]

In both variants, the trend towards increased data transfers across cultural and legislative boundaries heightens the risk of significant incompatibilities between what is expected or deemed acceptable by the individual with respect to data and what is actually done with that data. From an ethical perspective, this can be of particular relevance with regard to privacy, as the respective cultural conceptions significantly differ across the world.[15] The same risk could, however, also exist with regard to other domains shaped by cultural or legal differences whenever data is transferred across the respective boundaries.

[13] See, for example, Timmermans, Stahl, Ikonen and Bozdab (2010, p. 5).

[14] In this regard, the current conflict between Europe and the US about data transfer obligations for US corporations and even their European subsidiaries is an example with high relevance in the context of cloud computing.

[15] See, for example, Capurro (2005) or again Whitman (2004).

Particularly with regard to the legal framework, the transfer across boundaries not only bears the risk of individuals' rights being significantly limited[16] but also of these individuals not being able to exert their rights properly. This could, for example, be due to changes of the parties that the respective individual would have to approach, due to specific requirements having to be met in order to make a request eligible, due to language barriers, etc.

The question of how data (and, in the future, processes) crossing cultural and legislative boundaries at massive scale could be properly addressed has to remain open at this point. Of course, we may consider approaches such as "unifying legal frameworks", but when discussing this option it has to be kept in mind that legal frameworks are always rooted in the respective cultures in which they are to be "operated". Alternatively, one could consider "extraterritorial islands" where a cloud service within one cultural or legislative framework is, under certain preconditions, operated in accordance with cultural values and legal regulations from another one. The latter would reflect the current approach of Europe, which tries to ensure that European data protection law is to be applied to "European personal data" even when stored and/or processed in cloud services outside of Europe. It is, however, obvious that raises conflicts because it would logically result in two different legal frameworks being applicable to one and the same piece of data or processing instance.

For now, the identification of the expectable conflict arising from increased transfer across cultural and legislative boundaries must suffice. The question how it can effectively be dealt with shall, however, be further addressed throughout the remainder of the project.

3.4 Inherent Risk of Monopolies and Lock-Ins

Finally, one more aspect of cloud computing that bears certain indirect ethical risks will be discussed in brief, namely the inherent tendency of cloud computing services to develop so-called natural monopolies and the related risk of significant vendor lock-ins. Generally speaking, cloud services feature typical characteristics of information goods / network goods as depicted, for instance, by Shapiro and Varian (1998).

First, cloud services are subject to significant economies of scale; the provision of the first unit (an hour of computing time or a gigabyte of storage being offered through a sophisticated service interface, one user served with a complex SaaS application etc.) induces high initial development costs, while once the first unit has been provided, the costs for providing another unit are significantly lower or even negligible. This cost structure usually leads to a single vendor being able to serve a whole market at lower costs than would be the case with a multitude of competing vendors and therefore stimulating the emergence of monopolies.

Second, cloud services can usually be seen as so-called network goods which are characterized by providing a value to any single user that increases with additional users joining the network. This value-increase can emanate from more possibilities for interaction with other members being present, from more complementary goods being available, or from a higher availability of specific qualification on the market, etc. Especially with regard to complementary goods and specific skills, it is plausible to assume this network effect to be present with regard to IaaS, PaaS and SaaS cloud services. In addition, SaaS cloud services will presumably also feature benefits from more possibilities for communication and data exchange among different users. These network effects also provoke market monopolization.

And third, cloud services can also be characterized as being subject to lock-in effects. These basically arise whenever a certain specific good or service is integrated into a customer's

[16] Again, just think about the current conflict between the US and Europe and, in particular, the obvious fail of the so-called „Safe Harbor Regulations", which were explicitly intended to build a bridge between two fundamentally different cultures and legislations in matters of data protection.

processes in way that would make it so expensive for the customer to switch to an alternative supplier that it is economically rational to stick with the current one even if the alternative offer came at zero costs. As can be prominently seen in the market for office software, a dominant vendor can of course consciously design his product in a way that heightens these switching costs and thereby strengthens its dominant position. The risk of this also happening in the context of cloud services is obvious: IaaS and PaaS providers could make arrangements that prevent customers from easily migrating virtual machines, data or application logic to another provider while SaaS providers could make their products incompatible to other ones in a multitude of further ways. In the end, all three characteristics supply the emergence of monopolistic structures and work against a functioning market in the traditional sense.[17]

Even if this effect should at first sight be subject to considerations on traditional market regulation, it could also have ethical relevance. Within a monopolistic market, the dominant player enjoys significant bargaining power that can be (mis)used to force customers to accept terms of use, prices or other contractual conditions that are clearly detrimental to them. In lack of realistic alternatives, this could also lead to ethically relevant "decisions" being made under the constraint of no viable alternative being available. Bearing in mind that cloud services are often realized on the basis of other cloud services, this monopoly power of one player may furthermore also extend to relations between the customers of the single player and their customers, respectively. In such situations, the concept of "individual consent", which is, for example, often referred to in the domain of data protection, is clearly of only limited value. Similarly, concepts like "privacy as competitive advantage"[18] – even if discussable in other contexts – would under such market conditions hardly change anything. Instead, ways must be found that ensure compliance with ethical values (to which "choice" might also belong) within monopolistic markets, too.

Finally, the monopolistic character of cloud computing could also lead to ethical risks on the societal level: Given that the cloud market is driven by economic mechanisms that foster monopolistic structures, there is the certain risk that more and more services of various sorts are realized on the basis of the fundamental services provided by one single player. This could then lead to a single player posing a "systemic risk" – a factor that is so omnipresent and so interwoven into so many aspects of daily life that it becomes indispensable for societies as a whole. Again, this holds tremendous extortion potential which might, for instance, also be exploited in matters of not accepting "overly strict" regulatory restrictions regarding data protection, security, etc. Even if questions of market regulation are unquestionably far beyond the subject of SECCRIT, this potential shall be kept in mind throughout future considerations on the further development of the existing regulatory framework relevant to SECCRIT topics.

4 "Cloudification" of SECCRIT Use-Cases and Derived Safeguards for Project Implementation

In a third step of the "triangulation approach" laid out in section 1, we now have to discuss which specific ethical problems could potentially result from the "cloudification" of the use-cases employed in SECCRIT. In order to identify these possible issues, we interweave both dimensions – the ethical aspects specific to the two use cases as identified in section 2, and the ethically relevant characteristics of cloud computing as laid out in section 3 – with each other, and we examine where the concurrence of two effects either considerably strengthens an already identified risk or even changes its nature significantly. Due to the fact that ethical assessments strongly depend on the concrete application context and in line with the above-mentioned problems regarding the impact assessment of general purpose technologies, we will structure these considerations along the two use-cases. Basically, we thus look for the changes implied by

[17] See also Gentzoglanis (2012).
[18] See, e.g., Hoeren (2000).

the ethically relevant characteristics of cloud computing upon the ethical problems already identified for the use-cases.

In so doing, we will also lay out how the respective risks – cloud specific as well as the generic ones identified in section 2 – will be addressed throughout the remainder of SECCRIT in order to ensure that all activities within the project are not only in line with legal requirements but also with ethical imperatives.

4.1 "Cloudification" of Video Surveillance

As the first ethically relevant aspect of video surveillance, we identified the risk of the privacy of those under observation being significantly reduced, that is, the risk of hardly any behaviour being definitively unobserved, depending on the space under consideration (a prison, the workplace, semi-public or public spaces, …). With strict regard to this risk, the identified characteristics of cloud computing (control loss, lack or loss of transparency, cross-cultural and cross-legislation transfer, risk of monopolies and lock-in) have no relevant impact. The amount of conduct being potentially observed solely depends on the extent to which the space under consideration is covered by surveillance equipment and not on the mechanisms and technologies employed for handling and analysing the respective recordings.

The risk of significant privacy-reduction being implied by video surveillance in general must, however, also be addressed throughout the project and, in particular, throughout the establishment and operation of the video surveillance demonstrator. This leads us to the following safeguards:

- **SG2 – No surveillance of private or public spaces: In order to prevent privacy invasions, no evaluation activities will be conducted based on the surveillance of (semi-) public or even private spaces.**
- **SG3 – Experimental environments: Evaluations and tests of the secure cloud technologies that are to be developed in the project will, with regard to video surveillance, only be conducted on the basis of experimental environments that are explicitly set up for the project.**
- **SG4 – Explicit Consent (Video): Evaluations and tests will, with regard to video surveillance, only be conducted on the basis of recordings that are specifically produced for this purpose with explicit, well-informed and written consent of the persons being recorded.**

Through these safeguards, we prevent any ethical conflicts with regard to privacy invasion from emerging through the evaluation of our to-be-developed technologies applied to the scenario of video surveillance. Furthermore, this also ensures legal compliance of the respective evaluation activities.

With regard to the second ethically relevant aspect of video surveillance – the risk of fostering conformism – the above-mentioned explanations on the absence of specific consequences of cloudification similarly apply. The risk emanates from the individual's knowledge of (possibly) being observed and not from a specific way of data being handled or analysed. The above-mentioned safeguards therefore also ensure that conformism-related risks do not arise from the evaluation use-case being implemented.

Different from the first two aspects, there is a risk of ever-increasing inequalities of informational power between the observer and the observed because of the possible integration of multiple sources, as already described by Marx (2002) under the term of "*new surveillance*". This is

affected by the cloud-specific aspects of ethical relevance as identified in section 3. In particular, the risk of "control loss" could have a reinforcing effect on the inequalities of informational power, as cloud-technologies make the integration of a multitude of different data sources, the sharing of such data and their long-time storage even cheaper (and thus, more likely) while they at the same time decrease the observed individuals' possibilities for exerting influence on what is actually done with recordings showing them. Furthermore, this potential loss of control is not only confined to the observed but might also apply those parties that operate surveillance systems on the basis of cloud technologies. For example, a security firm monitoring a critical infrastructure like a subway station by means of a cloud-based surveillance system, can (without further technologies being used) not be sure that video recordings are not passed on to other parties by the cloud provider.[19]

Even if the technologies that are to be developed within SECCRIT explicitly counteract the risks associated with this control loss, through the establishment of advanced mechanisms for data flow control, for the generation of reliable digital evidence, etc., it cannot be guaranteed that these mechanisms are already well-functioning and complete during the evaluation phase. The outlined risk must therefore be addressed properly. In order to prevent potentially adverse and uncontrolled transfer, integration, analysis, etc. of video recordings, we will thus only use well-controlled cloud environments that are separated from the public Internet through strong state-of-the-art security mechanisms for our demonstrators. These well-controlled cloud environments are provided by one of the project partners (Amaris) and exclusively hosted in Europe. Different from other well-known cloud providers, we thereby employ more sophisticated and effective separation and security mechanisms and prevent any onward transfer of the respective data to third countries.

- **SG5 – Controlled cloud: Evaluations will only be conducted within well-controlled cloud environments separated from the public Internet through strong state-of-the-art security mechanisms and hosted within the European Union.**

The risks arising from the characteristic of lack of transparency also tends to reinforce the risk of significant inequalities of informational power as the observed individuals not only cannot influence which parties are able to access video recordings showing them, but they cannot even know who actually has this access. And depending on the concrete system design, even the operator of a cloud-based video surveillance system might not be aware where the respective data will be stored or processed. Without this knowledge, however, any attempt to fill the idea of "informational self-determination" with life is doomed. Again, the technologies that are to be developed within the project shall mitigate this lack of transparency faced by the different parties today[20], but it cannot be guaranteed that these are already in full function during the evaluation phase. The confinement to a well-controlled and well-protected cloud setting together with the explicit, well-informed and written consent introduced above should, however, counteract ethical risks that would otherwise possibly have emerged in matters of (lack of) transparency.

A potential impact of cloud-specific risks on the risk of automated analysis being performed on the basis of potentially defective or inappropriate algorithms could emerge from the context of transfer across cultural and legislative boundaries. If, for example, a cloud-based analysis service

[19] Besides the ethical dimension, this would also be problematic from the legal perspective as in this case, *the security firm* would have to ensure that data is handled correctly and not passed on to unauthorized parties. Such considerations are, however, subject to the legal deliverables D 2.2 and D 2.7 and shall therefore not be discussed in detail here.

[20] And again, there are also strong legal motivations for doing so which shall not be discussed in detail here. See, for instance, the sections of „transparency", „user rights" or on the provision of digital evidence in deliverable D 2.2.

should in the future be used ad-hoc within something like a “service based video surveillance system”, this would pose a significantly higher risk of the employed analysis service not matching the social expectations of the observed (and possibly also those of the observers) than it can be assumed within consciously designed and well-conceived integrated systems. Such models are, however, far beyond the scope of the SECCRIT and will therefore not be employed within the evaluation demonstrator. Instead, the confinement to a well-controlled and well-protected cloud setting exclusively hosted within the European Union will prevent this risk from actually gaining relevance at all.

Regarding the risks of cloud computing posing the inherent risk of natural monopolies and lock-in-effects in turn, no expectable interferences with other risks could be identified for the video surveillance demonstrator. Also, no specific safeguards could be identified as being necessary for preventing negative effects of this rather general risk throughout the project. Nonetheless, this potential risk exists and shall therefore be kept in mind during further activities. In particular, this will be done whenever it is reflected on the further development of the existing regulatory framework in Task T 2.4.

As already stated in SG1, we will furthermore conduct ethical assessments of the demonstrators during their establishment based on the table of “compass-questions” in order to prevent potential negative impacts that were missed in the analysis so far. During this assessment, the risk of results from technological analysis being inappropriately taken as objective fact will also be covered, even if the risk of “mistreatment” being done on the basis of such a misinterpretation is rather limited within our evaluation setting.

A tabular overview on how the different risks and their identified interdependencies are counteracted within the project will be given below. Before doing so, we must, however, also analyse the potential risks arising from the “cloudification” of (semi-) automated traffic management in the same way we already did for the “video surveillance” use-case.

4.2 “Cloudification” of (semi-) automated Traffic Management

Concerning the (semi-) automated Traffic Management scenario, we identified the potential risks of possibly tracking individuals and establishing movement profiles of the observed persons by recording faces of those individuals or the number plates of their cars. The identified cloud-characteristics of losing control, lack of transparency, cross-cultural and cross-legislation transfer, risk of monopolies and lock-in have partially a direct impact on these risks.

This is especially the case for the loss of control, lack of transparency and cross-legislation transfer. In contrast to the video surveillance scenario, where we can build our own “experimental environment”, we are for this evaluation demonstrator forced to take recourse on the infrastructure of the city of Valencia. It is therefore not possible to make our assessment without really observing a “real” and not a simulated volume of traffic in order to manage it properly as required within the SECCRIT project.

In order to nonetheless avoid privacy invasions as well as the generation of movement profiles, social discrimination and further risks already identified in the context of video surveillance, it is therefore absolutely necessary that individuals cannot be identified within our demonstrator setting – neither on the basis of their faces or other characteristics nor through by other means like cars.

- **SG6 – Obviate identification: It is technically ensured that faces, number plates and other features possibly allowing the identification and tracking of individuals are made unrecognizable whenever visual data (video, still images) is used in the**

traffic control demonstrator – be it through blurring or through a respective reduction of image resolution.

Beyond this, as cited in the section on the cloudification of video surveillance, the use of a **well-controlled cloud environment** for the storage and processing of the data (**SG5**) is correspondingly required.

Regarding a possible integration of Car-2-X communication technologies into the demonstrator, corresponding mechanisms for preventing the tracking of individuals and any possible discrimination are necessary, too. This can be done by means of strong technical mechanisms of anonymization or pseudonymization. As, however, identification of individuals could nonetheless be possible directly after data gathering and before their anonymization, well-informed and written individual consent is still to be obtained for any possible integration of Car-2-X data into the demonstrator.

- **SG7 – Anonymization/Pseudonymization: Whenever advanced technologies of Car-2-X communication are to be integrated into the traffic control demonstrator, the respective data will only be used in anonymized or pseudonymized form, preventing any attribution of data to individuals.**
- **SG8 – Explicit Consent (C2X): Any potential integration of data from Car-2-X communication and similar systems is only done if the respective individuals have given their (well-informed and written) consent in advance.**

The risk of cross-cultural and cross-legislation transfer will again be addressed by employing a well-controlled secure cloud environment exclusively hosted within the European Union (**SG5**), so that it will not gain any practical relevance for the traffic control demonstrator, too.

Potential problems with regard to monopolies and lock-ins will not be addressed specifically as they are not a threat for the concrete scenarios of the SECCRIT project, but rather shall be kept in mind during future deliberations on the development of the regulatory framework.

Concerning the selection of "*who is permitted to drive at a certain time*" this risk of discrimination/unequal treatment (congestion charges, extra lanes) emerges from the (semi-) automated traffic system itself and is not significantly affected by "cloudification". Even if the respective data and processes are relocated to external servers, this would lead to a problem only if the data makes it possible to draw conclusions about the individual from it which could then form as a basis for discriminations. For our demonstrator, these risks are, however, counteracted through the employment of alteration mechanisms (**SG6, SG7**) which are aimed at avoiding conclusions about individuals as well as through the strict confinement to well-controlled cloud environments specifically set up for the project (**SG5**).

Last, but not least, the automatic enforcing of rule sets through technology is also emanating from the (semi-) automated traffic management itself without significant cloud-specific aspects. The only imaginable impact of cloudification could arise from the cloud provider arbitrarily manipulating the technology to the disadvantage of the road user. Due to the well-controlled cloud environments used in the demonstrator (**SG5**), this risk will, however, play no significant role within the SECCRIT project.

4.3 Consolidated Overview

In order to provide a consolidated overview of the identified ethical risks, their potential interrelations with particular relevance and the safeguards that are to be employed throughout the project, the following table summarizes the findings obtained and the implications developed in

this document. Whenever no specific risks were identified for a certain combination, this is marked as “n/a”.

	General	Control Loss	Intransparency	Transfer across boundaries	Monopolies and lock-ins
General	n/a	SG5	SG5	DPA involvement (see D 2.4)	Continuous consideration during further development of regulation
CCTV					
Reduced Privacy	SG1, SG2, SG3,SG4	SG2, SG3, SG4, SG5	SG2, SG3, SG4, SG5	SG5	n/a
Conformism	SG1, SG2, SG3, SG4	n/a	n/a	n/a	n/a
Inequalities of informational power	SG1, SG2, SG3	SG3, SG4, SG5	SG3, SG4, SG5	SG5	n/a
Defective / inappropriate analytical algorithms	SG1	SG5	SG5	SG5	n/a
Results mistaken “as objective facts”	SG1	n/a	n/a	SG5	n/a
Traffic Control					
Movement profiles / tracking	SG1, SG6, SG7	SG5, SG6, SG7	SG5, SG6, SG7	SG5	n/a
Social discrimination / unequal treatment	SG1, SG6, SG7	SG5, SG6, SG7	SG5, SG6, SG7	SG5	n/a
Automated enforcement / no exceptions	SG1	SG5	SG5	SG5	n/a

The safeguards developed herein and referred to in the above table are:

- **SG1 – Compass Questions: The "compass questions" reproduced in section 0 will be applied in the design and implementation of the demonstrators.**
- **SG2 – No surveillance of private or public spaces: In order to prevent privacy invasions, no evaluation activities will be conducted based on the surveillance of (semi-) public or even private spaces.**
- **SG3 – Experimental environments: Evaluations and tests of the secure cloud technologies that are to be developed in the project will with regard to video surveillance only be conducted on the basis of experimental environments that are explicitly set up for the project.**
- **SG4 – Explicit Consent (Video): Evaluations and tests will with regard to video surveillance only be conducted on the basis of recordings that are specifically produced for this purpose with explicit, well-informed and written consent of the persons being recorded.**
- **SG5 – Controlled cloud: Evaluations will only be conducted within well-controlled cloud environments separated from the public Internet through strong state-of-the-art security mechanisms and hosted within the European Union.**
- **SG6 – Obviate identification: It is technically ensured that faces, number plates and other features possibly allowing the identification and tracking of individuals are made unrecognizable whenever visual data (video, still images) is used in the traffic control demonstrator – be it through blurring or through a respective reduction of image resolution.**
- **SG7 – Anonymization/Pseudonymization: Whenever advanced technologies of Car-2-X communication are to be integrated into the traffic control demonstrator, the respective data will only be used in anonymized or pseudonymized form, preventing any attribution of these data to individuals.**
- **SG8 – Explicit Consent (C2X): Any potential integration of data from Car-2-X communication and similar systems is only done if the respective individuals have given their (well-informed and written) consent in advance.**

Based on these safeguards, we will ensure that ethical aspects are consciously taken into account and addressed properly during further activities within SECCRIT. The SECCRIT Security group will therefore be responsible that these safeguards are followed throughout the implementation phase. Once again, we note that this deliverable explicitly concentrates on ethical aspects that are not, not yet, or not yet sufficiently referred to within the legal and regulatory framework covered in other deliverables (in particular, D 2.2 and D.2.7). Furthermore, aspects relating to the interaction with relevant national data protection authorities are also covered in a separate deliverable (D 2.4) and therefore not covered herein, too. Altogether, these deliverables and the deliberations included here (and there) form the basis for ensuring that all activities of the project are in line with well-established societal values and will prevent avoidable adverse impacts as far as possible.

5 Conclusion

In summary, this deliverable has pointed out the ethical problems emerging from the risk of using new cloud technologies. Generic ethical aspects of the two demonstrators, CCTV and (semi-) automated traffic control, have been identified. Furthermore, the concept of cloud computing has been analysed in matters of ethically relevant characteristics. On this basis, the specific risks that potentially arise from “cloudification” within the areas of CCTV and (semi-) automated traffic have been identified. Through a “triangulation approach”, we have determined how the respective risks – cloud-specific as well as the generic ones identified – are to be addressed throughout the remainder of the SECCRIT project in order to make sure that all activities within the project are not only in line with legal requirements but also with ethical imperatives. For that purpose we have established an easy-to-use method that is to be employed throughout the remainder of the project, based on so-called “compass questions” and a suitable set of safeguards. By applying this method, ethical conflicts should, as far as possible, be prevented from emerging throughout the evaluation of our to-be-developed technologies as applied to the evaluation demonstrators.

6 Annex: Table of "Compass Questions"

TABLE 1: "COMPASS QUESTIONS" AS DEVELOPED BY MARX (1998)

A. The Means	
	1. Harm: Does the technique cause unwarranted physical or psychological harm?
	2. Boundary: Does the technique cross a personal boundary without permission (whether involving coercion or deception or a body, relational, or spatial border)?
	3. Trust: Does the technique violate assumptions that are made about how personal information will be treated, such as no secret recordings?
	4. Personal relationships: Is the tactic applied in a personal or impersonal setting?
	5. Invalidity: Does the technique produce invalid results?
B. The Data Collection Context	
	6. Awareness: Are individuals aware that personal information is being collected, who seeks it, and why?
	7. Consent: Do individuals consent to the data collection?
	8. Golden rule: Would those responsible for the surveillance (both the decision to apply it and its actual application) agree to be its subjects under the conditions in which they apply it to others?
	9. Minimization: Does a principle of minimization apply?
	10. Public decision-making: Was the decision to use a tactic arrived at through some public discussion and decision-making process?

	11. Human review: Is there human review of machine-generated results?
	12. Right of inspection: Are people aware of the findings and how they were created?
	13. Right to challenge and express a grievance: Are there procedures for challenging the results, or for entering alternative data or interpretations into the record?
	14. Redress and sanctions: If the individual has been treated unfairly and procedures violated, are there appropriate means of redress? Are there means for discovering violations and penalties to encourage responsible surveillant behaviour?
	15. Adequate data stewardship and protection: Can the security of the data be adequately protected?
	16. Equality-inequality regarding availability and application: (a) Is the means widely available or restricted to only the most wealthy, powerful, or technologically sophisticated? (b) Within a setting is the tactic broadly applied to all people or only to those less powerful or unable to resist? (c) If there are means of resisting the provision of personal information are these means equally available, or restricted to the most privileged?
	17. The symbolic meaning of a method: What does the use of a method communicate more generally?
	18. The creation of unwanted precedents: Is it likely to create precedents that will lead to its application in undesirable ways?
	19. Negative effects on surveillants and third parties: Are there negative effects on those beyond the subject and, if so, can they be adequately mediated?
C. Uses	
	20. Beneficiary: Does application of the tactic serve broad community goals, the goals of

	the object of surveillance, or the personal goals of the data collector?
	21. Proportionality: Is there an appropriate balance between the importance of the goal and the cost of the means?
	22. Alternative means: Are other, less costly means available?
	23. Consequences of inaction: Where the means are very costly, what are the consequences of taking no surveillance action?
	24. Protections: Are adequate steps taken to minimize costs and risk?
	25. Appropriate vs. inappropriate goals: Are the goals of the data collection legitimate?
	26. The goodness of fit between the means and the goal: Is there a clear link between the information collected and the goal sought?
	27. Information used for original vs. other unrelated purposes: Is the personal information used for the reasons offered for its collection and for which consent may have been given, and do the data stay with the original collector, or do they migrate elsewhere?
	28. Failure to share secondary gains from the information: Is the personal data collected used for profit without permission from, or benefit to, the person who provided it?
	29. Unfair disadvantage: Is the information used in such a way as to cause unwarranted harm or disadvantage to its subject?

References

Bentham, J. (1791): “Panopticon, or the Inspection House”, Dublin/London, T. Payne.

Capurro, R. (2005): “Privacy. An intercultural perspective”, Ethics and Information Technology 7(1), pp. 37-47.

Cavoukian, A. (2008): “Privacy in the clouds”, Identity in the Information Society 1(1), pp. 89-108.

Collingridge, D. (1980): “The Social Control of Technology”, New York, St. Martin‘s Press

Gentzoglanis, A. (2012): “Evolving Cloud Ecosystems: Risk, Competition and Regulation”, Communications & Strategies, 1(85), pp. 87-107.

Graham, S. and D. Wood (2003): “Digitizing surveillance: categorization, space inequality”, Critical Social Policy 23(2), pp. 228-248.

Hansen, S. (2004): “From ‘Common Observation’ to Behavioural Risk Management – Workplace Surveillance and Employee Assistance 1914-2003”, International Sociology 19(2), pp. 151-171.

Hoeren, T. (2000): “Datenschutz als Wettbewerbsvorteil – eine Fortsetzung früherer Überlegungen mit neuem Vorzeichen”, E-Privacy 2000, pp. 263-279, Vieweg&Teubner.

Kang, J. and D. Cuff (2005): “Pervasive Computing: Embedding the public sphere”, Washington & Lee Law Review 62, pp. 93-147.

Koskela, H. (2000): “’The gaze without eyes’: video surveillance and the changing nature of urban space”, Progress in Human Geography 24(2), pp. 243-265.

Marx, G. (1998): “Ethics for the New Surveillance”, The Information Society, 14, pp. 171-185, http://en.scribd.com/doc/22549509/

Marx, G. (2002): “What’s New About the ‘New Surveillance’? Classifying for Change and Continuity”, Surveillance & Society 1(1), pp. 9-29.

Monahan, T. (2009): “Dreams of Control at a Distance: Gender, Surveillance, and Social Control”, Cultural Studies – Critical Methodologies 9(2), pp. 286-305.

Paquette, S., P.T. Jaeger and S.C. Wilson (2010): “Identifying the security risks associated with governmental use of cloud computing”, Government Information Quarterly 27(3), pp. 245-253.

Roßnagel, A., M. Desoi, and G. Hornung (2012): “Noch einmal: Spannungsverhältnis zwischen Datenschutz und Ethik – Am Beispiel der smarten Videoüberwachung”, ZD 10/2012, pp. 459-461.

Shapiro, C. and Varian, H. (1998): “Information Rules: A Strategic Guide to the Network Economy”, Boston, Harvard Business Press.

Timmermans, J., V. Ikonen, B.C. Stahl and E. Bozdag (2010): “The Ethics of Cloud Computing: A Conceptual Review”, Proc. IEEE CloudCom 2010, pp. 614-620.

Weber, K. (2010): “Reichweite und Grenzen der Technikfolgenabschätzung”, In: Lingner, Lutterbeck, Pallas (ed.) “Die Zukunft der Räume”, pp. 53-65, Europäische Akademie Bad Neuenahr-Ahrweiler.

Whitman, J.Q. (2004): “The Two Western Cultures of Privacy: Dignity Versus Liberty”, Yale Law Journal 113, pp. 1151-1221.