# SIAM

# Security Impact Assessment Measures

WP 3

Impact analysis on criminal actions


## Deliverable D3.5

State of the art report on SMT impact on the global security level.

Report Title: CCTV and Smart CCTV effectiveness: a meta-level analysis'

The interdisciplinary Research Group on Law, Science, Technology and Society

Vrije Universiteit Brussel

1. Lucas Melgaço

2. Kristof Verfaillie

3. Mireille Hildebrandt

**Project number**
261826

**Call (part) identifier**
FP7-Security-2010-1

**Funding scheme**
Collaborative Project

# Table of Contents

# 1. Executive Summary

This deliverable contributes to the SIAM project by complementing the reports based on empirical research in work package 3 (impact analysis on criminal actions). The results of this report will contribute to the SIAM database and the Assessment Support Tool.

The main objective of this deliverable is to present and discuss the complexities involved in the assessment of the effectiveness of Security Measures and Technologies (SMTs) in reducing crime and in increasing security. Although there is an immense variety of SMTs currently operating, the analysis is limited to closed-circuit television (CCTV) and Smart CCTV because of the availability of relevant literature on these two technologies. For most of the other SMTs such literature is not accessible. This report focuses on texts which promote a meta-analysis of the effectiveness of video surveillance, that is, articles that compile previous research on effectiveness assessment or that promote methodological discussions about how to better evaluate its effectiveness.

The first chapter, “Rationalisation, complexity and effectiveness”, is a theoretical and abstract reflection about the assessment of effectiveness. It confronts the limits of rationalisation processes with the complexities of crime. The chapter also discusses the consequences of the current transition from a global focus on prevention to one on pre-emption. Pre-emption, which can be seen as an attempt to rationalise the unknown, an effort to predict the unpredictable, marks a new tendency in the way security has lately been pursued.

The following chapter, “Meta-analysis of the effectiveness of CCTV systems”, dissects a handful of reports on the evaluation of traditional CCTV systems. The chapter enumerates the main difficulties present in CCTV evaluation and depicts the mechanisms through which CCTV systems work. These mechanisms are classified in terms of their “past”, “present” and “future” functions, a reasoning that can largely be applied to other SMTs, particularly those that involve surveillance features.

The last chapter, “From traditional CCTV to Smart CCTV”, takes up the problem of automation and video analytics. It brings in a host of issues around complexity, discriminating between performance, evaluation, operation, policy concerns and political considerations. This chapter promotes a discussion about the performance of Facial Recognition Technologies (FRTs) and shows how the technology is – as yet – not effective enough to prevent crime in complex settings.

The report ends by showing that statements on the effectiveness or ineffectiveness of a certain SMT must be considered with caution, since such findings are contingent upon a variety of constraints, such as temporal, spatial, and political. This report also highlights that technical efficiency does not necessarily indicate crime-reducing effectiveness, since the latter involves a higher level of complexity. Controlled spaces, such as airports, train stations and especially parking lots, however, are easier to manage than open systems. Therefore, in less complex settings surveillance technologies seem to be more effective. Moreover, the less complex the context, the easier and more precise one can assess the effectiveness of SMTs.

## 2. Introduction

Assessing effectiveness in science is by definition a complex task. This is already a complicated effort in hard sciences like physics and biology and it can be ever more obscure when it comes to social sciences. In the criminology field, for example, discussions about whether a security measure is really effective in reducing crime have always existed, not infrequently raising more contradictions than certitudes. Such contradictions are in part due to the fact that sometimes reality can be just too complex to be translated into a statistical model. However, this does not mean that all attempts to measure effectiveness are worthless. Indeed, in some cases the discussion about effectiveness seems to be unavoidable since, as Tilley (1999) points out, evaluation and audit are imposed as major instruments of surveillance over publicly funded programmes.

The main objective of this report is to present and discuss the complexities involved in the assessment of the effectiveness of Security Measures and Technologies (SMTs) in reducing crime, particularly those technologies used in transportation contexts like airports, metro and train stations. Thus, the goal is not exactly to assert whether a particular SMT is effective or not, but to analyse the complexities involved in such a evaluation and to address some of the many variables that must be taken into account.

Thus, this report should not be taken as a state of the art on the effectiveness of SMTs. Firstly, because of the near impossibility of addressing all the available SMTs used in mass transportation. The SMTs in question include technologies as different as detection dogs to unmanned aerial vehicles. Moreover, criminal actions at airports and in public transport systems encompass from everyday crimes to terrorist attempts. Added to that it is the fact that new security technologies appear every day, many of them being still very recent and almost no academic work about their effectiveness has been published yet.

Among the different SMTs already in place in public mass transportation, closed-circuit television (CCTV) is one that has received more attention from scholars. Despite the difficulties of precisely defining CCTV (for example, not all systems classified under this label are necessarily “closed-circuit”; see IRISS (2012)), there is a significant amount of work dedicated to discuss the effectiveness of such systems, which justifies why this report is focused on this type of SMT. Less numerous but still significant are the publications on automated CCTV systems, which include Video Analytics and Facial Recognition features. Some of these publications will also be treated here.

The second reason why this report is not entirely a state of the art is because the literature discussed is not intended to be comprehensive. In the case of video surveillance, for example, the amount of research and the number of publications analysing effectiveness concerning specific case studies is considerable. This report does not intend to consider all of them but rather to focus on those texts that promote a meta-analysis of effectiveness, in other words, articles that bring together

previous research involving effectiveness assessment or that promote methodological discussions about how to better evaluate effectiveness.

The report is thus organized in three parts. The first part proposes a theoretical reflection about rationalisation, complexity and the challenges involved in the scientific discussions on effectiveness. The second part analyses the literature on the effectiveness of traditional video surveillance systems and highlights the multiple and complex variables that must be taken into account. The third part addresses a discussion about automation by using the example of Smart CCTV and includes an analysis about Facial Recognition applications. The conclusion shows how such a framework can be expanded to the analysis of the effectiveness of other SMTs used in public mass transportation, particularly those involving biometrics and profiling.

## 3. Rationalisation, complexity and effectiveness

The attempt to measure effectiveness can be understood as a rational practice. A way to reduce our ignorance in relation to reality, and achieve a certain mastery of it, is by the pursuit of *reason,* understood here as defined by Morin (2005, p. 94): "Reason reflects the desire to have a coherent vision of phenomena, objects and the universe. Reason has an undeniably logical aspect." Rationality would thus be the propensity to face the world from the aspect parting from reason. For Morin (2005, p.94) "rationality is a game, the perpetual dialogue between our spirit, that creates logical structures, implementing them to the world and which dialogues with this real world." Rationality refers to the desire to understand the world through a scientific spirit. As a consequence, rationalisation is the process of applying rationality to comprehend and the decoding of a given situation.

Ritzer (2011), through an interpretation of Weber's concept of rationalisation, suggests that a rational process involves four main principles: efficiency, calculability, predictability and control. The author uses McDonald's as an example to explain his thesis. According to Ritzer, efficiency refers to the optimal method for accomplishing a task. McDonald's drive-through system would be a clear instance of the fastest way to get from hungry to being full. The second principle, calculability, can be noticed in the procedures currently present in several McDonald's activities such as the quantification of stocks and the calculus of the time it takes to deliver a product. Predictability can be seen in the access customers have to similar products no matter which McDonald's they go to. Thus, predictability is related to routine and the standardization of procedures. It is related to the quest for the reduction of risks and unexpected situations. Finally, the existence of control in the McDonald's environment can be verified in actions like the standardization of employee's uniforms and in the close tracking of their tasks.

Considering rationalisation as a combination of efficiency, calculability, predictability and control can be useful to the analysis of the effectiveness of SMTs. Assessing effectiveness is, in itself, a rational procedure as it is an attempt to assert through rational parameters whether a security measure is effective or not.

Not only actions, but also spaces can be rationalised (Santos, 1996). The aforementioned example of McDonald's drive-through exemplifies how space is projected in a rational way to help costumers to go from a situation of hunger to that of fullness without much effort. The spatial configuration of the drive-through facilitates the quantification and control of both costumers and employees' actions in order to promote efficiency and predictability. In a similar reasoning, the quest for security can in certain circumstances also be understood as a form of rationalisation of space. Spaces may be designed or altered in order to reduce unpredictability and fear. Rationalisation of space for purposes of security can occur in different manners. For example, through the installation of surveillance cameras, body scanners, construction of barriers, demarcation of limits, walls, through constructions that regulate and restrict the movement of individuals and select those who have the privilege to attend a particular place. Video surveillance, for example, can be seen as an attempt to rationalise space as it includes the four principles suggested by Ritzer.

It permits calculability (the quantification of the number of persons or objects present in a scene), efficiency (police officers may be better deployed), control (intervention in actions that scape normality) and predictability (one may assume that actions taken in a monitored space tend to be more predictable).

However, there are cases where rationalisation can be taken to an extreme. Ritzer (2011) calls this "the irrationality of rationality", a notion similar to that of "rationalism" proposed by Morin (2005). While rationalisation is a process of decoding the world - a necessary simplification of reality by which it becomes tangible -, rationalism is the fact of aspiring to reduce reality to a purely rational system. When the simplification is excessive, it denies the complexity of reality, which could lead to biased interpretations. In this sense, rationalism would be the desire to imprison reality into a coherent system, leaving aside everything that eludes this logical scheme. Rationalism is thus an exaggeration of rationalisation (Melgaço, 2012).

Rationalism is not uncommon in science. This is particularly true when policy makers press scholars to simplify their advice in order to produce science-based decisions, even in cases where knowledge in uncertain. As Stirling (2010, p. 1029) points out,

> Expert advice is often thought most useful to policy when it is presented as a single 'definitive' interpretation. Even when experts acknowledge uncertainty, they tend to do so in ways that reduce unknowns to measurable 'risk'. In this way, policy-makers are encouraged to pursue (and claim) 'science-based' decisions.

On this subject Morin (2005, p. 11) says:

> While the simplifying thought disintegrates the complexity of the real, the complex thought comprises as much as possible the simplifying modes of thinking, but denies the mutilating, reductionist, one-dimensional and finally blinding consequences of a simplification that pretends to be the reflex of what is real in the reality.[i]

This reasoning proposed by Stirling and Morin can be transposed to the analysis of effectiveness made in this report. The challenge remains exactly in addressing assertive conclusions about the effectiveness of security measures without denying the complexity of such question. One of the issues concerning the assessment of effectiveness is related to the difficulties in considering all the possible variables. A simplistic reasoning can conclude, for example, that since the attacks on the Twin Towers on 9/11 in the United States no other event of the same magnitude has taken place and that would be due to global investments in counter-terrorists practices and technologies. However, the attacks might have ceased to take place even without the expenses on security measures. The motivations and rationale of a terrorist attack seem to be too complex to convey in a cause-effect scheme.

This justifies, in a certain sense, why Massumi (2007, p. 5) argues that we are moving from a prevention to a pre-emption paradigm. He explains what prevention is by saying:

> Preemption is not prevention. Although the goal of both is to neutralize threat, they fundamentally differ epistemologically and ontologically. Epistemologically, prevention assumes an ability to assess threats empirically and identify their causes. Once the causes are identified, appropriate curative methods are sought to avoid their realization. Prevention operates in an objectively knowable world in which uncertainty is a function of a lack of information, and in which events run a predictable, linear course from cause to effect.

Pre-emption, on the other hand, differs from prevention in that it acts on threats that have not yet fully formed or that have not even emerged yet, "(i)n other words, the threat is still indeterminately in potential" (Massumi, 2007, p. 13). Pre-emption appears, thus, as a challenge of rationalizing the unknown, an effort of predicting the unpredictable.

The recent investments in security initiatives, particularly those related to counter-terrorist actions, are strongly influenced by the principle of pre-emption. The former United States president George W. Bush, in a speech pronounced on June 2002 before the graduating class of the US Military Academy, affirmed (Massumi, 2007, p. 1):

> If we wait for threats to fully materialize, we will have waited too long. We must take the battle to the enemy, disrupt his plans and confront the worst threats before they emerge. In the world we have entered, the only path to safety is the path to action. And this nation will act.

The concept of pre-emption then brings even more complexity to the discussion about effectiveness. How can one assert that a certain technology is in fact effective against a still unknown threat?

When it comes to measuring effectiveness, how to include all the variables involved? How to avoid the lure of over-simplifying reality, which can lead to hasty conclusions? Goodwin (2002) presents a case study that, if one analyses it superficially, one could come to the possibly incorrect conclusion that the installation of CCTV failed to deter crime. "Across the six camera locations covered in the study, the number of crimes recorded by the police before the installation of CCTV was 205, and the number of crimes recorded by the police after the installation of CCTV was 213." (Justice Analytical Services, 2009 p. 11). A more in-depth analysis may, however, show that in fact the CCTV system increased the detection effect: more crimes were detected but not necessarily more crimes were committed. Farrington, Bennet and Welsh (2007) came up with similar findings in their work comparing police recorded crime statistics with victimisation survey data in Cambridge. They assert that in that case study CCTV surveillance led to the growth of crime detection rates.

Another example of rationalisation involving security measures is that of cost and benefit evaluation. Such evaluation involves calculability, control and predictability of expenses and, overall, efficient trade-off between costs and

benefits. However, the complexity of the question makes cost and benefit evaluation a very confusing issue. Previous reflections on the case of CCTV system can illustrate such a complexity[ii]. Armitage (2002, p. 3) highlights the multiple variables to be taken into account when evaluating the costs of CCTV systems:

> The cost of CCTV as a crime prevention measure includes not only the initial investment but also the ongoing maintenance and running costs. For this reason, any cost effectiveness analysis (as part of a post-installation evaluation or a pre-installation feasibility study) must account for these factors, in particular the staff time required to monitor the cameras.

Tilley (1998, p. 149) adds that: "There will rarely if ever be sufficient data to assess the full costs and benefits that can be directly attributable to CCTV. The potential choice of what to include as a cost and a benefit is so wide that robust and meaningful estimates will seldom be possible."

Groombridge (2008, p. 74) argues that the benefits of CCTV do not compensate the high costs. He declares: "My intention therefore is to argue from a radical perspective – that is broadly sceptical of CCTV – that the Home Office, and therefore the Treasury, has wasted enormous sums of tax payer's money on the deployment of CCTV." Paradoxically, a report from the Scottish Government (Justice Analytical Services, 2009, p. 26) seems to be more optimistic as it recognizes that CCTV footage may bring financial benefits when used as evidence in court:

> In light of the great expense of CCTV, its economic benefits, particularly in relation to the savings gained through early intervention and use of evidence in court, must be a focus of future research. In order to gain a true picture of the associated economic benefits, savings in these respects need to be balanced out against the cost of installing and maintaining CCTV in the first place.

Thus, if assessing effectiveness is already a tough task, doing it through a precise quantification of costs and benefits seems to be even more challenging.

It is equally difficult to translate abstract features like security, risk, and fear into mathematical terms. Security, as Ceyhan (1998) states, is a complex and abstract concept that involves both the absence of risks and the feeling of safety. Thus, how to measure security? Should one measure it in terms of mathematical risks? Moreover, how can one measure subjective features like the feeling of safety or fear? One of the few essays on "measuring" fear is the work of Ditton (2000). The author compared crime fear levels in Glasgow city before and after the installation of CCTV and concluded that CCTV "is not making the unsafe feel safe, it is making the already safe feel safer" (p. 702). Would it be possible to translate these findings into precise mathematical terms? Would it be possible to measure security in terms of the effectiveness of specific SMTs?

One should also keep in mind that statistics may "lie", as argues Huff (1954) in his book "How to lie with statistics". The author depicts how intentional and

unintentional common errors associated with the interpretation of statistics can lead to inaccurate conclusions. Statistics proving the effectiveness or the ineffectiveness of a certain SMT may, in fact, be the result of manipulated or wrongly interpreted data. In addition, Monmonier, in the book "How to lie with maps" (1996) adds that maps, often used by criminologists to show the geographical development of criminal patterns and to assert effectiveness, may similarly be object of manipulation. Criminology studies have also addressed the difficulties of dealing with statistics. Authors like Cicourel and Kitsuse (1963), Elliot (1995) and Maguire (2002) point out the complexities and inaccuracies involved in the practice of measuring and comparing crime rates.

In certain cases, evaluation reports have the ultimate goal of justifying costs. Consequently, they can serve as a political tool. It is not incorrect to affirm that in some occasions the final decision whether or not a certain SMT is effective ends up being a political question rather than a technical one. As Tilley defends: "Sadly, many really only want evaluations for self or political or organisational or civic aggrandisement, even when purporting to want an independent piece or work. They want the independent piece of work only if it comes up with the 'right' answer." (Tilley, 1998, p. 149). There are also cases where effectiveness is not even the main purpose of the installation of SMTs. Policy makers sometimes install SMTs aiming to promote the satisfaction of public demand for 'something to be done' about crime; a demand that, as presented by Reiner (2002), has been inflated by the continual representation of crime in the media discourse.

At this point it is important to distinguish efficiency from effectiveness. Some SMTs may be efficient in relation to a specific goal they were designed to achieve, without necessarily being effective in reducing crimes. While efficiency is related to performing a task in an optimal way, effectiveness makes reference to choosing the right tasks in order to achieve a goal. An iris scanner can be efficient in recognizing individuals but may not be effective in reducing terrorist attacks in an airport, for example.

Moreover, an approach that focuses too much on asserting the efficiency or the effectiveness of a certain technology may ignore undesirable consequences caused by the installation of such apparatus. For example, a scanner that allows an agent to see intimate details of a passenger body may be a highly efficient technology for the detection of explosives, but at the same time an intrusive initiative that raises clear questions about privacy rights.

## 4. Meta-analysis of the effectiveness of CCTV systems

The first experiments involving the use of CCTV systems go back to the 1950s. These systems were primarily applied to the management of public transportation and later cameras were installed in banks and commercial centres. The pioneer country to promote large investments in CCTV was the United Kingdom. In the 1970s, video surveillance cameras were installed in four major British underground train stations (Carli, 2008). It was only in the 1980s that CCTV was broadly expanded to the United States and other European countries. During the 1990s, CCTV technology developed significantly (IRISS, 2012) with the emergence of digital CCTV cameras and the association of CCTV with the Internet.

Scientific publications about the effectiveness of CCTV systems started to appear in the late 1970s. In 1979, Mayhew et al. (see also Burrows, 1979) published a study about the effectiveness of CCTV cameras as part of a security effort to reduce crime in some metro stations in London. The study found that cameras seem to be effective in reducing the number of robberies, a finding also shared by Webb and Laycock, in a later report published in 1992.

In 1999, Norris and Armstrong published "The Maximum Surveillance Society: The Rise of CCTV", one of the first books dedicated exclusively to the analysis of the spread of video surveillance. Already in the introduction, the authors make it clear they do not intend to present surveillance as merely a totalitarian initiative. There are cases where surveillance conducted by the state (like knowing citizens' addresses, income, and health conditions) is necessary to guarantee the protection of the individual. On the other hand, as exposed by the authors, video surveillance can reinforce prejudices by focusing differentially on the young, the male, the black and the slovenly people.

One of the strengths of Norris and Armstrong's book is the fact that the authors carried out an empirical study of more than 600 hours of observation in three different areas in the United Kingdom. The authors collected qualitative and quantitative data of different agents involved and concluded that CCTV cameras are not as effective in assisting the detection of criminal activities as normally suggested by their proponents.

The compilation "Surveillance, Closed-Circuit Television and Control" edited by Norris, Moran and Armstrong (1998) must also be highlighted. Four chapters of the book are dedicated exclusively to the evaluation of CCTV. "Evaluating the Effectiveness of CCTV Schemes", by Nick Tilley, stands out because of its meta-analytical approach. According to the author, the text aspires "to help those with responsibilities for CCTV evaluations better to think through the logic and rationale of their work; and to highlight a number of technical problems that need to be addressed in evaluating the effectiveness of CCTV schemes." (p. 139).

Anyone trying to assess the effectiveness of CCTV systems, or any other SMT, must have in mind the complexity of the task. Tilley (1998, p. 142-143) highlights such complexity by enumerating a range of difficulties present in CCTV evaluation procedures. These procedures were adapted and reinterpreted by us as follows:

i) *Pseudo-random fluctuations in crime rates*. In small areas crime can 'naturally' fluctuate independently of specific crime prevention efforts.
ii) *Regression to the mean*. Crime prevention efforts are normally put in place after periods of a high crime rate. However, crime rate may naturally regress to a normal rate, therefore to the mean, even without any particular intervention.
iii) *Floor effects*. In contexts where crime rate is normally low, it is very difficult to detect downwards effects as a result of CCTV.
iv) *Changes in background crime rates*. The fluctuation crime rate of the studied area must be compared to the development of crime in the surrounding area.
v) *Other changes in the area covered by CCTV*. Researchers must take into account other changes that might have happened in the studied area and analyse how it may affect crime patterns or influence the effectiveness of CCTV systems.
vi) *Changes in patterns of crime reporting and recording*. CCTV can lead to the increase of reporting crimes that would otherwise pass unnoticed.
vii) *CCTV as part of a package of crime prevention measures*. The installation of a CCTV system is normally accompanied by other measures that may multiply the effectiveness of video surveillance technologies.
viii) *Displacement*. In the case of CCTV actually being effective, crimes can simply migrate to other less monitored areas or criminals can change the time, method and type of crime. (see also Waples, Gill and Fisher, 2009).
ix) *Diffusion of benefits*. As offenders are not fully aware of the CCTV coverage they can change their behaviour even when acting in areas outside the scope of the CCTV scheme.

When utilized for security purposes, surveillance cameras can be broadly classified according to three principal mechanisms, which can be explained in terms of the "past", "present" and "future" functions of the criminal activity (Melgaço, 2012). In relation to "past", cameras have the intention to record events and serve as a data bank for investigation and later identification of the criminal. The images can also be used in court as evidence. In the relation to the "present" function, the camera has the aim to serve as an extension of the eyes of the police or private security guards. The agent behind the cameras identifies a suspected activity or a crime already in the process of being committed and acts in real time, preventing it from being accomplished. The third goal, which turns to "future" time, refers to the capacity of the camera to prevent a crime from occurring by inducing a sensation into the criminal that he is being continuously monitored.

Thus, a running camera, when connected to a system of data storage, responds to "past", "present" and "future" purposes as described. In other words, it permits investigation, detection and deterrence. However, a connected camera, that does not store images, only meets "present" and "future" functions. And finally, a false camera in which images are neither produced nor stored, has only a function in the "future", since its sole purpose is to induce the feeling of being monitored.

Owen et al (2006), in their evaluation of the benefits of CCTV systems in managing police resources, concluded that a considerable amount of police time could be saved during the investigation process as a consequence of the use of CCTV. Hence, it can be said that CCTV could be efficient in relation to the "past" function by allowing police time to be used more productively.

The "present" function, that of immediately detecting crime or reacting to suspicious behaviours, seems to be the one where cameras are less effective, particularly due to the increasing amount of data to be monitored by agents. However, as will be discussed later in this report, investments are being made in software dedicated to the automatic detection of persons and behaviours.

Concerning the complexity involved in the "future" function, a report conducted by the Police and Community Safety Directorate of the Scottish Government (Justice Analytical Services, 2009, p. 23) states: "The issue of crime deterrence as a potential outcome of CCTV is particularly difficult to evaluate as researchers are faced with the problem of assessing crime that may have been observed, had CCTV not been installed in the area." Smith (2004 p. 377) is equally sceptical about the deterrence effects of CCTV and believes that video surveillance is more effective as an investigative tool:

> I would argue that CCTV is generally ineffective as a crime prevention tool. This is because the cameras, in these examples, are clearly not producing "anticipatory conformity" in the population, deterring criminals, nor are they offering Big Brother protection to those under their gaze. Their use, in this type of scenario, is limited to the reconstruction of events for post crime police enquiries.

When it comes to violent crimes, the literature (Sivarajasingham, Shepherd and Matthews, 2003; Gill et al. 2006; Justice Analytical Services, 2009; Welsh and Farrington, 2002) shows little evidence of a deterrent effect, which is understandable due to the impulsive nature of this kind of crimes.

This framework of mechanisms by which a CCTV system works ("past", "present" and "future") can be expanded as done by Armitage, Smyth, and Pease (1999, p. 226). According to the authors the means by which CCTV may prevent crime include:

- Caught in the act: perpetrators will be detected and possibly removed or deterred.
- You've been framed: CCTV deters potential offenders who perceive an elevated risk of apprehension.
- Nosy Parker: CCTV may lead more people to feel able to frequent the surveilled places. This will increase the extent of natural surveillance by newcomers, which may deter potential offenders.
- Effective deployment: CCTV directs security personnel to ambiguous situations, which may head off their translation into crime.
- Publicity: CCTV could symbolize efforts to take crime seriously, and the perception of those efforts may energize law-abiding citizens and/or deter crime.

- Time for crime: CCTV may be perceived as reducing the time available to commit crime, preventing those crimes that require extended time and effort.
- Memory jogging: the presence of CCTV may induce people to take elementary security precautions, such as locking their car, by jogging their memory.
- Anticipated shaming: the presence of CCTV may induce people to take elementary security precautions for fear that they will be shamed by being shown on CCTV.
- Appeal to the cautious: cautious people migrate to the areas with CCTV to shop, leave their cars, and so on. Their caution and security mindedness reduce the risk.

Tilley (1998) also describes some of the mechanisms through which CCTV may work, but he formulates it differently. According to him, CCTV systems:

- Enable more effective deployment of security guards/police.
- Increase 'natural surveillance' through increased usage of area by people less fearful of crime.
- Increase confidence of members of the public to intervene, if they believe the situation is being observed and police back-up will follow.
- Increase potential offenders' fears that they will be seen, caught and shamed of punished, or moved on for misbehavior or unwanted behavior.
- Help catch offenders, who may then be removed.
- Remind people to be cautious in areas covered, for instance where signs tell them they are at risk.
- Deter people from using the area because they deem it dangerous if CCTV is needed.
- Provoke offenders to search for an alternative area/situation in which perceived risks of being seen are lessened.

Assessing the efficiency of cameras in fighting crime, Heilmann (2003) argues they are more effective under specific conditions. According to the author, for a monitoring program with cameras to be successful, one must consider: the use of resources with technology potently sufficient to detect targets, the complexity of urban space to be monitored, the correct definition of the targets and relevant goals and the combination of other preventive measures.

Cusson (2005) identified that cameras do not have the same impact on all types of crime, and that video surveillance has the best results: in the case of visible crimes, in which offenders do not dare to confront their victims; in places that do not allow criminals a quick escape; when the devices improve the capacity of identification and intervention; when the installation of cameras is publicized and when monitoring results in a constant intervention of security organs.

To date, a variety of case studies were conducted trying to assess the effectiveness of CCTV systems. However, only few studies approached the methodological difficulties of evaluating effectiveness, like in the case of Tilley (1998). Also rare are

comprehensive studies of the literature on the effectiveness of CCTV systems. In this report we will highlight four studies that conducted a meta-analysis of other case studies. The first is the research conducted by Welsh and Farrington (2002), who compiled a systematic review of the literature up to that date. Searching by the keywords "closed-circuit television", "CCTV," "cameras," "social control," "surveillance," and "formal surveillance", the authors came up with forty-nine evaluations to be analysed. Within this first survey they only included those evaluations that met the following quality criteria:

- CCTV was the main focus of the intervention;
- There was an outcome measure of crime;
- The evaluation design was of adequate or good methodological quality, with the minimum design involving before-and-after measures of crime in experimental and control areas;
- There was at least one experimental area and one reasonably comparable control area;
- The total number of crimes in each area before the intervention was at least twenty.

Out of the forty-nine previous evaluations, only twenty-two met the aforementioned criteria for inclusion. The other twenty-seven evaluations were excluded because of inconsistent methodologies. Ironically, they were not effective enough to be considered for Welsh and Farrington's effectiveness report. The main findings of this compilation of papers were that:

> CCTV had a significant desirable effect on crime, although the overall reduction in crime was a rather small 4 percent. All nine studies showing evidence of a desirable effect of CCTV on crime were carried out in the United Kingdom. Conversely, the other nine studies showing no evidence of any desirable effect of CCTV on crime included all five North American studies. CCTV was most effective in reducing crime in car parks. It had no effect on violent crimes but had a significant desirable effect on vehicle crimes. (p. 110)

Four out of the twenty-two analysed cases deal with transportation. The four researches were conducted in metro systems: one in the Montreal Metro by Grandmaison and Tremblay (1997) and three in the London Underground, being two by Webb and Laycock 1992) and one by Burrows (1979). According to Welsh and Farrington the results show conflicting evidence of effectiveness:

> [T]wo had a desirable effect, one had no effect, and one had an undesirable effect on crime. However, for the two effective programs in the London Underground, the use of other interventions makes it difficult to say with certainty that it was CCTV that produced the observed crime reductions, although in the program by Burrows (1979), CCTV was more than likely the cause. Only two of the studies measured diffusion of benefits or displacement, with one showing evidence of diffusion and the other displacement. (p. 124)

Welsh and Farrington highlight the complexity of assessing effectiveness of CCTV systems when other interventions like an increase in police patrol, improved lighting, installation of passenger alarms, notices and signs about CCTV are included. They argue that one-third of the twenty-two selected programs included interventions in addition to CCTV, which "makes it difficult to isolate the independent effects of the different components and the interactional effects of CCTV in combination with other measures."(p. 132). This reasoning can be expanded to other SMTs. It is common for an SMT to be installed together with other technologies or practices, which makes it sometimes difficult to isolate the effects of a single initiative.

Welsh and Farrington's results, however, should not be immediately applied to the present time since most of the studies they analysed were related to the technological and political context of the 1990s. Since then, video surveillance technologies have advanced drastically. Moreover, events like the bomb attacks on the London underground in 2005 and particularly the attacks on the New York twin towers in 2001 changed the way police, citizens and criminals deal with security technologies and that include CCTV systems.

Three other comprehensives studies appeared after that. In 2005, Gill and Spriggs published the results of a multi-evaluation of 14 English cities. One conclusion puts forward that in only two out of fourteen cases the installation of CCTV systems resulted in a reduced number of crimes. Moreover, in only one of the two successful cases, which incidentally is a car park case, there was a significant reduction in crime.

Gill and Spriggs also found that recorded crime rates increased in several target areas. This, as mentioned before, can lead to the wrong conclusion that CCTV failed to effectively deter crime, when in fact it is possible that CCTV led to the increase of crime detection. For this reason, Gill and Spriggs asserted that crime rates may be a poor measure of the effectiveness of CCTV interventions.

In 2007, Welsh and Farrington prepared a report for the Swedish National Council for Crime Prevention, which was later published as an article in 2009. The article is an update of their first research conducted at the beginning of that decade. Welsh and Farrington's meta-analysis findings were consistent with those of their initial review of 2002: "CCTV is most effective in reducing crime in car parks, is most effective in reducing vehicle crimes, and is more effective in reducing crime in the UK than in other countries." (2009, p. 736). Their evaluations also showed that CCTV schemes did not have a significant effect on crime in city and town centres, public housing and public transport.

In 2009, the Justice Analytical Services of the Scottish Government prepared a report which included only studies that had been conducted since the year 2000. The report reviewed the evidence of the effect of CCTV on crime by looking at these four parameters: crime deterrence effects; crime displacement effects; detection of crime; and the use of evidence in the investigations and prosecutions process (Justice Analytical Services, 2009). With the exception of crime displacement effects,

it can be said that the report comprises the aforementioned “past” (investigation), “present” (detection) and “future” (deterrence) functions of video surveillance.

Due to a lack of case studies on the effectiveness of CCTV conducted since the year 2000, the report used selection criteria that were less strict than those used by Welsh and Farrington (2002). The number of selected papers would have been too small if they had used stricter criteria. In order to be selected, studies had to include empirical efforts, CCTV had to be the main intervention included in the evaluation and they had to have come up with an outcome measure of crime (Justice Analytical Services, 2009, p. 6). Twelve studies were chosen, being five “quasi-experimental” crime intervention studies, four interview studies, two studies incorporating psychological experimental methods and theory and one observation study of behavioural adaptations to CCTV.

Amongst others, the Scottish report analysed the work by Griffiths (2003), which studied the effectiveness of a town centre CCTV system in Gillingham, UK. The study’s findings include that video surveillance seems to be more effective within the first year following the installation but such deterrence effects usually fade with time. One of the reasons for this being the fact that media play a role in publicizing the CCTV installation. Criminals aware of these security measures may feel constrained in committing a crime. A very similar finding is presented by Armitage (2002). She claims that the effectiveness of CCTV within London Underground stations was reduced after approximately one year and that other CCTV evaluations revealed that the initial reductions in crime following the installation of CCTV can diminish if publicity is not maintained. In other words, it can be said that while the “past” and the “present” functions of video surveillance may keep up the same degree of effectiveness over time, the “future” function has an expiry date.

The evaluation conducted by Sivarajasingham, Shepherd and Matthews (2003) was also highlighted by the Scottish report. This study addressed the aforementioned common confusion between real changes in crime rates, and increases in crime detection and recording. Furthermore, the authors focused on the effects of CCTV on violent crime and, different from previous research, suggested that CCTV may have a desirable effect on these type of crimes. Increased detection would lead to more punishment, which would deter criminals from committing violent acts (Justice Analytical Services, 2009).

Concerning the evaluation of CCTV effectiveness in violent crimes, the strategy adopted by Gill et al (2006) is noteworthy. The authors led focus group discussions with ten murderers, who were about five years into their sentence, and seven had committed the murder in a public place. “The aim of this study was therefore, to investigate whether the murderers involved in the focus groups would have been deterred by the presence of CCTV cameras at the time of committing their offence.” (Justice Analytical Services, 2009, p. 11). The results of this research are different from those found by Sivarajasingham, Shepherd and Matthews (2003). Gill et al found evidence that the murderers did not consider the presence of cameras as an important deterrent technology. Moreover, when the crimes were committed under the influence of alcohol, they ignored CCTV cameras even more.

According to Tilley, the existence of conflicting results in evaluations of the effectiveness of CCTV systems, like these presented by Sivarajasingham, Shepherd and Matthews (2003) and Gill et al (2006), was to be expected:

> So, though mixed findings from evaluation studies can often be expected simply because many pieces of work are technically flawed or technically different, they are also inevitable because measures will have differing impacts depending on the conditions in which they are introduced. This means that the frequently asked question, 'Does CCTV work?' admits and can admit of no consistent answer. It is, therefore, not a sensible, useful or intelligible question to address, notwithstanding the frequency with which it is asked or the money and effort spent trying to answer it. (Tilley, 1998, p. 144).

Thus, as said in the Scottish report: "The 'effectiveness' of CCTV must be considered in light of its intended purpose, as each individual project is installed to serve its own purpose." (Justice Analytical Services, 2009, p. 23).

Despite these conflictive findings, there seems to be at least one consensus: CCTV systems appear to be significantly effective in reducing crimes in less complex settings, such as parking lots (Webb and Laycock, 1992; Armitage, 2002; Griffiths, 2003; Carli, 2008; Welsh and Farrington, 2009). This finding is consistent with the reasoning outlined in the introduction of this report: the more complex a situation or a space is, the larger the number of variables to be considered; hence, more challenging the rationalisation process. In 1992, Webb and Laycock had already alerted that "CCTV does not seem very useful in large, complex and crowded environments to deal with more surreptitious behaviour such as pickpocketing or shoplifting." (1992, p. 23). Similar findings were produced by Ditton and Short (1999) in their study about the effectiveness of open street CCTV in two adjacent British town centres: Airdrie, a small town, and Glasgow, a large city. The authors indicated that CCTV seemed to be more effective in the first case. The Scottish report puts forward a similar reasoning when it says that "Recent research has resulted in evidence consistent with the repeated finding that CCTV may be more effective in deterring crime in smaller and less complex areas than large city centres." (Justice Analytical Services, 2009, p. 2). It can thus be said that the less complex a situation or a space is, the more effective an SMT may be in reducing crime, and the more precise the evaluation of such effectiveness will be.

Complex settings, on the other hand, present themselves as a challenge to rationalisation. The multiplicity of variables to be considered makes it complicated to translate them into terms of efficiency, calculability, predictability and control. Moreover, considering the three functions of CCTV – "past", "present" and "future" – the "present" function seems to be the least effective in complex settings. Detecting suspicious activity, and acting upon it before it becomes an accomplished crime, is an enormous challenge to guards and police officers acting in intricate contexts.

One way to increase effectiveness in relation to the "present" effect is by setting up CCTV control rooms, where agents can manage multiple cameras from and monitor

several screens at a time. Smith (2004) conducted field research in the CCTV control room of a British college. Within the findings of his ethnological research is what he named the “boredom factor”. In such a context, like a college, the occurrence of criminal activities is significantly low. The agents, thus, get bored and watch the screens with less attention and interest. Moreover, he found that “the operatives felt alienated from their job, due to the imprisoning confines of the CCTV control room, the long hours worked, the high expectation levels placed upon them and the low pay and lack of acclamation received from their employers” (p. 376). The result is the inefficiency of the system in flagging crime in real time.

Moreover, with the spread of CCTV cameras the number of images produced steadily grows. This means that more and more images are to be analysed. Besides the installation of CCTV control rooms, another response to this increasing flow of information has been the use of software that is able to automatically detect faces and suspicious activity. This topic will be discussed in the following part of this report.

## 5. From traditional CCTV to Smart CCTV

Both the increasing capacity of data recording and the widespread use of cameras have resulted in an immense volume of data at hand. It is important to highlight that although the spread of CCTV cameras has lead to an overload of data being gathered, it did not necessarily lead to an increase in information[iii]. A traditional CCTV camera merely produces a set of pixels, an amount of data to be interpreted and transformed into information. Footage is traditionally interpreted by human operators, who, by watching computer screens, decide whether or not an event is normal or abnormal. Humans, however, are exposed to failures due to reasons like those mentioned by Smith (2004). In response, software has been developed to enable facial recognition and automatic detection of suspicious activities and behaviour. As Adams and Ferryman (2012, p. 2) argue: "The rapid proliferation in the number of CCTV installations worldwide, in areas such as shopping centres, underground stations, and airports, has expedited the demand for automatic methods of processing their output." The demand for automated surveillance is also presented in the military context, where drones create large data bulks to be processed and analysed.

Usually called Smart CCTV, Intelligent CCTV, or Video Analytics, these automated systems differ significantly from traditional analogue video surveillance in respect to their possibilities. What makes them smart is the combination of images and software. Ferenbok and Clement (2012) highlight the following in their definition of video analytics:

> Video analytics (VA) is software that uses signal processing and pattern recognition techniques to automatically generate meaningful or semantic data from video images. Video analytics marks a paradigmatic shift in visual surveillance practices — in how information is purposed, and repurposed — and in the potential consequences for surveillance subjects.

Adams and Ferryman (2012, p. 3) put forward that "The overall capability to automatically analyse video images to extract objects, detect events, and to perform behavioural analysis, is referred to as video analytics."

Detection, tracking and classification of targets are the main tasks expected from video analytics engines. Detection refers to the identification of what physical objects exist in the surveillance area, tracking is the understanding of how they move and classification is related to the labelling of objects as human, vehicle, animal and to the interpretation as normal or abnormal objects or behaviours.

In video analytics, data can be interpreted from a single frame from one camera, across a video sequence from one camera, or in comparing different views of the same area from multiple cameras (Adams and Ferryman, 2012, p. 3). Data can also be interpreted from cameras in different areas, as in the case of transport applications where inferences on speed can be made through the identification of the same object in two different spots (Rios-Cabrera, Tuytelaars, and Van Gool, 2012).

As pointed out by Haering, Venetianer, and Lipton (2008, p. 281), the first applications of automated video surveillance systems were related to simple motion detection. Cameras could, for example, be set to start recording only and as soon as they detected movement. The usefulness of motion detection systems was, however, reduced due to the high false alarm rates caused by the movements of unimportant objects like shadows, foliage, or small animals.

The following step in the evolution of intelligent CCTV was the creation of object based video analysis. This type of analysis reduced the occurrence of false alarms by introducing sophisticated filtering capabilities. Alarms would sound only in the case of movement of specific types of objects.

The detection of object functions as follows: "Pixels deviating from the background model statistics are labeled as foreground. These pixels are grouped together into spatial blobs, then tracked, thus creating spatiotemporal objects" (Haering; Venetianer; Lipton, 2008, p. 281). The distinction between objects and background is also influenced by the quality of lighting of the area. The more complex the background and the worse the lightning, the less precise the identification of objects will be. As Adams and Ferryman (2012, p. 3) pointed out, object identification in small and indoor scenes tends to be simpler as ambient lighting is more controlled while applicability to dense, crowded environments is much more limited. Dee and Velastin (2008) assert that Smart CCTV engines perform with decreased performance in unstructured or changing environments such as public places.

Although one of the main expected applications of video analytics is the improvement of the "present" function of surveillance, Adams and Ferryman (2012) argue that most of its applications still do not operate in real time, being currently used for after-the-fact investigation. Ferenbok and Clement (2012) also address this discussion when they say the following:

> Video Analytics (VA) addresses at least two major limitations of the conventional analog CCTV model: live monitoring and retrospective searching. Watching video surveillance can be tedious and boring. Often there can be hours or days of video from multiple sources where very little of interest actually happens. The volume of information produced by multiple cameras running 24 hours seven days a week means that much of the information captured by analog CCTV cameras is not viewed in real-time or retained, and if recorded, remains effectively not viewed.

Significant effort, however, has been put into increasing the speed of object detection. Lately, a lot of attention has been going to automatic number plate recognition (ANPR) – also called License Plate Reader/License Plate Recognition (LPR) – as well as to the automatic detection of abandoned bags. As presented by Carli (2008), ANPR is a surveillance technology that uses optical character recognition of images to read license plates. When acting in real-time, ANPR can help the police chasing a vehicle, as well as for monitoring traffic activity. ANPR can thus be considered an example of rationalisation of spaces: streets equipped with CCTV cameras connected to ANPR systems are spaces that permit the quantification and

the control of traffic activity and an increase in the efficiency of police activities.

The development of faster real-time responses is particularly desirable in the detection of abandoned bags. The longer it takes to detect such objects, the higher the risks. The European Union recently concluded a project called SUBITO (www.subito-project.eu) "aimed at developing a surveillance system for robustly detecting abandoned bags in public spaces and to identify and track the owner" (Adams and Ferryman, 2012, p. 6). As highlighted by the project, detecting abandoned bags automatically is a complex task. An example of a criterion normally taken into account by the algorithms is when the supposed owner of a bag is, for a certain time, further than a given distance from the bag. However, it is possible that in a busy airport people move closely enough to a bag, which may confuse the system in classifying it as unattended. As Adams and Ferryman (2012, p. 6) point out: "For dealing with these more complex scenarios, it became necessary to derive a more complete activity analysis and the concept of social groups was introduced." The SUBITO project developed a framework to automatically understand the behaviour of groups, which helped to reduce the number of false alarms for abandoned bags.

The example of applying video analytics in detecting abandoned bags gives proof of the increasing capacity of software to translate social relations into computational language. Concepts like ownership of an object and belonging to a social group are only two of a variety of examples of social relations decoded in rational and mathematical models.

A similar process of digitisation and quantification is currently happening with the human body. Body features like the iris, face and hands are being translated into mathematical formulas in a process commonly named biometrics. In the case of Smart CCTV, the most evident biometrical application is in the use of cameras for facial recognition.

As explained by Carli (2008, p. 5), "Facial recognition technology is a computer application for automatically identifying or verifying a person from a digital image or video frame from a video source." One of the advantages of facial recognition technologies (FRTs) in comparison to other biometric systems is that, as pointed out by Introna and Wood (2004), they can operate anonymously in the background, while iris or hand scanners require a direct physical involvement from their targets. Moreover, FRTs are relatively inexpensive and can, in principle, take advantage of existent traditional CCTV systems, as FRTs are more software than hardware-based.

Video analytics is a still recent technology – the first experiments with facial recognition technologies date from the late 1990s – which explains why very few case studies have been published about their effectiveness in reducing crime. Even more rare are the meta-level studies about Smart CCTV effectiveness along the lines of the four reports on traditional CCTV mentioned before. Three of the few exceptions are the aforementioned work of Adams and Ferryman (2012), Dee and Velastin (2008) and the report produced by Introna and Nissenbaum (2009) on what could be called an evaluation of other evaluations on FRTs.

According to Introna and Nissenbaum, there already exist a considerable amount of publications on the technical side of FRTs and some studies on the social impact of these systems but no publication connecting both:

> On the one side, there is a huge technical literature on algorithm development, grand challenges, vendor tests, etc., that talks in detail about the technical capabilities and features of FRT but does not really connect well with the challenges of real world installations, actual user requirements, or the background considerations that are relevant to situations in which these systems are embedded (social expectations, conventions, goals, etc.). On the other side, there is what one might describe as the "soft" social science literature of policy makers, media scholars, ethicists, privacy advocates, etc., which talks quite generally about biometrics and FRT, outlining the potential socio-political dangers of the technology. This literature often fails to get into relevant technical details and often takes for granted that the goals of biometrics and FRT are both achievable and largely Orwellian. Bridging these two literatures—indeed, points of view—is very important as FRT increasingly moves from the research laboratory into the world of socio- political concerns and practices (Introna and Nissenbaum, 2009, p. 8)

Through an approach that is in line with Morin's aforementioned reflections on the idea of complexity, their report "attempts to straddle the technical and the socio-political points of view without oversimplifying either" (p. 8).

The authors analyse FRTs through five main parameters (pp. 3-5), of which the first three are of special interest to our discussion:

> 1. Performance: What types of tasks can current FRT successfully perform, and under what conditions?;
>
> 2. Evaluations: How are evaluations reported? How should results be interpreted? How might evaluation procedures be revised to produce more useful and transparent results?;
>
> 3. Operation: What decisions must be made when deciding to adopt, install, operate, and maintain FRT?;
>
> 4. Policy concerns: What policies should guide the implementation, operation, and maintenance of FRT?;
>
> 5. Moral and political considerations: What are the major moral and political issues that should be considered in the decision to adopt, implement, and operate FRT?

The literature analysed by Introna and Nissenbaum shows that in general FRT performance has proven effective in the case of relatively small populations in controlled environments. Consequently, facial recognition is much more efficient in applications of verification than identification. As the authors explain, verification

consists of matching an individual's face to a pre-existing image "on-file" associated with the claimed identity. Identification, on the other hand, refers to recognizing individuals who did not voluntarily offer their biometrics. The literature shows that in these more complex cases where FRTs are used to match an individual's face with any possible image "on-file", the performance results are much poorer.

There are two types of identification: closed-set and open-set. In closed-set identification, it is known in advance that the wanted individual's profile is already present in the database. Whilst in more complex open-set situations, it is not known in advance whether an individual is present or not in the gallery image. As Introna and Nissenbaum (2009, p. 12) stress:

> The outcome of these two identification problems will be interpreted differently. If there is no match in the closed-set identification then we know the system has made a mistake (i.e., identification has failed (a false negative)). However in the open-set problem we do not know whether the system made a mistake or whether the identity is simply not in the reference database in the first instance.

Most of real-world identification applications are open-set, which explains the poor performance of FRTs in more complex situations. As a consequence, the authors affirm: "the 'face in the crowd' scenario, in which a face is picked out from a crowd in an uncontrolled environment, is unlikely to become an operational reality for the foreseeable future." (Introna and Nissenbaum, 2009, p. 3)

The performance of verification and, especially, identification tasks depends on a series of factors. One of the most important aspects is the quality of the gallery image used to identify a certain individual. In the case of a verification task, the conditions of enrolment are ideal, as individuals opt to voluntarily offer their biometric information. In this case, the image captured by the camera is comparable to passport quality photographs. However, in identification cases this often is not the case since the gallery is composed of low quality images. Charlie Savage, in an article for the New York Times (Facial Scanning is Making Gains in Surveillance – August 21, 2013), proposes a similar reasoning:

> The automated matching of close-up photographs has improved greatly in recent years, and companies like Facebook have experimented with it using still pictures. But even with advances in computer power, the technical hurdles involving crowd scans from a distance have proved to be far more challenging. Despite occasional much-hyped tests, including one as far back as the 2001 Super Bowl, technical specialists say crowd scanning is still too slow and unreliable.

The literature analysed by Introna and Nissenbaum (2009, p. 3) showed that performance is also contingent of other factors like:

> *Environment:* The more similar the environments of the images to be compared (background, lighting conditions, camera distance, and thus

the size and orientation of the head), the better the FRT will perform.

*Image Age:* The less time that has elapsed between the images to be compared, the better the FRT will perform.

*Consistent Camera Use:* The more similar the optical characteristics of the camera used for the enrollment process and for obtaining the on-site image (light intensity, focal length, color balance, etc.), the better the FRT will perform.

*Gallery Size:* Given that the number of possible images that enter the gallery as near-identical mathematical representations (biometric doubles) increases as the size of the gallery increases, restricting the size of the gallery in "open set" identification applications (such as watch list applications) may help maintain the integrity of the system and increase overall performance.

In regard to performance, Introna and Nissenbaum (2009) also analysed the conditions that may limit the efficiency of FRT, in other words, "what makes it not work" (p. 38). The authors highlight that FRT effectiveness is a consequence of the performance of the whole operational system rather than of a particular technological issue. In addition, they point out that "The successful operation of a FRS [facial recognition system] in the identification mode is critically dependent on the key characteristics of the gallery database: image quality, size, and age." (p. 39). It is also important to take the quality of the probe image and the conditions of capture into account. Best FRT performance occurs when the conditions under which the probe photos were taken most closely resemble those of the gallery image. Moreover, the recognition algorithms should be carefully chosen since different algorithms can produce different results.

Concerning the evaluations of FRT, Introna and Nissenbaum divide them into three categories: technological, scenario and operational. Technological evaluations address the capabilities of algorithms to promote facial recognition under closely controlled conditions. Scenario evaluations deal with the capacity of the system to recognise faces in a specific scenario designed to emulate a real-world situation. Finally, operational evaluations are related to the application of FRT to real in-locus situations.

The authors analysed publications in these three different categories and came to the conclusion that the best results were found in technological evaluations. Thus, the more complex the settings are, like in real operational contexts, the less efficient an FRT is. It is not uncommon though for positive findings of technological evaluations to be used as a justification for investment in FRT in real operational situations. Introna and Nissenbaum (2009, p. 4) affirm that:

> Evaluation results must be read with careful attention to pre-existing correlations between the images used to develop and train the FRT algorithm and the images that are then used to evaluate the FRT algorithm and system. Tightly correlated training (or gallery) and

> evaluation data could artificially inflate the results of performance evaluations.

In regard to the operation of FRT, Introna and Nissenbaum highlight how delicate the balance is between the level of certainty to which a system works and the acceptance rates. There is a trade-off between False Acceptance Rates (FAR; the probability that a system incorrectly matches the captured biometric feature with the stored template, creating a false positive) and False Rejection Rates (FRR; the probability that the system fails to detect a match, creating a false negative). They explain (2009, p. 4):

> For instance, a system with a high threshold, which demands a high similarity score to establish credible recognition in the verification task, would decrease the number of individuals who slip past the system (false accept mistakes), but would also increase the number of individuals who would be incorrectly rejected (false reject mistakes). These trade-offs must be determined, with a clear sense of how to deal with the inevitable false rejections and acceptances.

When applying FRT to verification issues, it is common to set a high threshold for the system. In such a situation, it is crucial to guarantee a low quantity of false accept mistakes, even at the expense of a high number of false reject mistakes. However, when FRT is applied to identification procedures, a high rate of false alarms may tamper the applicability of such technologies. False alarms require extra resources for constant follow-up. Moreover, the repetition of constant false alarms may lead operators to ignore a real alarm.

Introna and Wood (2004), Introna and Nissenbaum (2009) and Adams and Ferryman (2012) draw attention to two scenario applications where facial recognition systems were abandoned due to their lack of utility. In Tampa Bay, in the US, this happened because the system generated a large number of false positive alarms. In the Palm Beach Airport case, a group of 15 volunteers were compared to a small database of only 250 images and the results of a mere 47% of correct identifications motivated the abandonment of the project.

False positive alarms are not just technical issues; they are also political. Operators may, for example, deal differently with a wrongly target individual, who is a member of a minority group. Moreover, as Introna and Wood (2004, p. 192) asserts “The operators may even override their own judgments as they may think that the system ‘sees something’ that they do not.” Situations like these could be labelled as cases of rationalism, where, as termed by Ritzer (2011), the process of rationalisation resulted in the “irrationality of rationality.”

Introna and Nissenbaum (2009) conclude their report by saying that the analysed evaluations suggest that FRT can be useful in verification task as long as certain conditions are met. However, so far their performance has still been very poor in process of identification, whether closed- or open-set. Adams and Ferryman (2012, p. 9) reinforce this idea by saying that the current automated surveillance systems operate with satisfactory performance in restricted domains in which algorithms

function well. “However, the overall vision is to develop systems which can respond to and act in the real world.” Thus, facial recognition systems, and more broadly video analytics, are technologies that are efficient in controlled settings but still very inefficient in real complex situations.

# 5. Conclusions

Anyone involved in assessing the effectiveness of Security Measure Technologies must keep in mind that this is not a simple task. As this report showed, the discussion about effectiveness is full of complexities of all sorts. Asserting the effectiveness of a technology in reducing crime is both a technical and a political task.

Although there is an immense variety of SMTs currently operating in mass transportation, the choice for CCTV and Smart CCTV was based on the availability of the bibliography on these two technologies. The number of case studies on the effectiveness of video surveillance systems abounds. This plentiful offer of references allowed authors like Welsh and Farrington (2002; 2007), Gill and Spriggs (2005), and Justice Analytical Services (2009) to produce comprehensive reports on the state of the art of such technology. In these four reports, the reference to the notion of complexity is evident. The work of Tilley (1998) must also be highlighted. Despite not being a compilation like the other reports, it addresses crucial methodological questions about the difficulties involved in assessing the effectiveness of video surveillance systems.

The inclusion of Smart CCTV in our analysis is justified by two reasons. Firstly, because Smart CCTV seems to be an unavoidable update to traditional CCTV systems. These systems are becoming more "intelligent" and automated each day. Not taking this development into account may thus result in an out-dated evaluation. Secondly, the logic behind the functioning of video analytics systems shares similarities to that currently put in place with other SMTs. The understanding of the reasons why facial recognition systems may fail can be used to help analysing other technologies like body scanners, for example.

There exist, however, fewer publications on Smart CCTV than on traditional CCTV. The number or existent case studies is considerably lower, and methodological and comprehensive state of the art reports are very rare. Nevertheless, the works of Adams and Ferryman (2012) and Dee and Velastin (2008) and particularly the report prepared by Introna and Nissenbaum (2009), were highlighted because of their comprehensive approach to the discussion and because of how they underscore the complexity of the question.

Reducing crime, measuring the reduction of crime, asserting that this reduction was due to the effects of a certain technology, and measuring such effects are four extremely complicated issues. The reality is so complex that a policy maker may be surprised by the fact that an SMT can actually augment crime instead of diminishing it. As Welsh and Farrington (2003, p. 111) explain: "The presence of CCTV may give people a false sense of security and cause them to stop taking precautions that they would have taken in the absence of this intervention, such as not wearing jewelry or walking in groups when out at night." Consequently, the rationalisation of the question through a cause-effect analysis will be insufficient to apprehend all the intricacies involved.

As presented, video surveillance, whether traditional or “smart”, functions through a series of mechanisms that can be classified into three main effects: “past”, “present” and “future”. The “past” effect, that is to say, the capacity of video surveillance to serve investigation purposes appeared as the one in which both CCTV and Smart CCTV are more effective in reducing crime. The growing digitisation of video surveillance and the increasing capacity of saving data has lead to what Mayer-Schönberger (2009) named the almost impossibility of forgetting in the digital age. This phenomenon improved the “past” effect of video surveillance since the amount of information recorded and stored in CCTV databases grows each day. In regards to the “present” function, that of detecting crimes in real time and acting upon it, CCTV seems to be very ineffective, whilst Smart CCTV showed better results. Concerning the “future” aspect, that is, deterrence, video surveillance appeared more effective in the first year after the installation of cameras. However, such effectiveness tends to decrease over time.

Another important finding extracted from the report analysis is that the concept of effectiveness is often used as a political discourse. In fact, there are cases where technical assessments of the efficiency of certain SMTs are confounded with their real effectiveness in reducing crime. This is currently the case with facial recognition systems, the technological evaluations of which – that is, the capabilities of algorithms to promote facial recognition under closely controlled conditions – are mistaken for its real operational capabilities. In other words, the positive findings about the efficiency of facial recognition engines are used as a justification for implementing this technology in real operational situations of combating crime. Efficiency is, thus, mistaken for effectiveness.

Some findings regarding the functioning of facial recognition technologies (FRTs) can be expanded to biometrics as a whole. Whether it is a fingerprint, iris or body scanner, the logic involved in the trade-off between false acceptance rate (FAR) and false rejection rate (FRR) is always present. The decision on the FAR and FRR depends on the application under consideration and has important social and political implications.

The analysis of the effectiveness of FRT also pointed out the importance of databases. The main goal of an FRT is to match faces with profiles on an image gallery. As shown, effectiveness is a function of the quality of this gallery. The quality of such database depends on the time lapse between the gallery image and the captured probe image. Consequently, it can be said that FRT efficiency decreases with time, which draws attention to the importance of keeping a database always updated.

Finally, the most important finding of this meta-level analysis goes back to the discussion about complexity mentioned at the outset. The majority of the analysed bibliography mentioned that video surveillance, whether traditional or smart, is more effective in simpler and controlled settings, while performance declines as the context gets more complex. Traditional CCTV seems to be effective in the investigation, detection, and deterrence of crime in parking lots. These are very simple contexts where the number of involved variables is reduced.

Smart CCTV uses the same logic. The literature showed that FRT tends to be much more efficient in verification than identification procedures, which is explained by the fact that the former is more controlled while the latter involves a higher number of variables. Introna and Nissenbaum (2009, p. 24) also indicate the connection between complexity, the number of involved variables and effectiveness of FRT by saying:

> To conclude this discussion, we can imagine a very plausible scenario where we have a large database, less than ideal images due to factors such as variable illumination, outdoor conditions, poor camera angle, etc., and relatively old gallery images. Under these conditions, performance would be very low, unless one were to set the FMR [false match rate] to a much higher lever, which would increase the risk that a high number of individuals would be unnecessarily subjected to scrutiny.

The relationship between complexity and effectiveness can be expanded to a general analysis of SMTs in public mass transportation. An airport, for example, can be considered a more controlled setting than a train station. In an airport, the public is selected and space is rationalised through the implementation of checkpoints used to quantify and control the flux of passengers. On the other hand, a train station looks more like an open system where the input of variables is more complex compared to an airport. According to this reasoning, it is expected that SMTs implemented in airports would be more effective than those installed in more complex and unpredictable contexts.

In conclusion, the assessment of the effectiveness of CCTV and Smart CCTV in reducing crime must inevitably take into account all the complexities involved in such question. Therefore, this is not a mere cause-effect question to be answered by technicians but a multifaceted issue to be addressed by a combination of different specialties.

# 7. Bibliography


Ackoff, R. L. (1989) "From Data to Wisdom", Journal of Applied Systems Analysis, Volume 16, 3-9.

Adams, A. A. and Ferryman, J. M. (2012). The Future of Video Analytics for Surveillance and its Ethical Implications (November 12). Security Journal, Forthcoming. Available at: http://ssrn.com/abstract=2174255. Accessed October 8, 2013.

Armitage, R. (2002) To CCTV or not to CCTV?: A review of current research into the effectiveness of CCTV systems in reducing crime. Nacro Briefing Note. Available at http://epic.org/privacy/surveillance/spotlight/0505/nacro02.pdf. Accessed October 8, 2013.

Armitage, R., Smyth, G., and Pease, K. (1999). Burnley CCTV evaluation. In K. Painter and N. Tilley (eds.), Surveillance of Public Space: CCTV, Street Lighting and Crime Prevention: Vol. 10. Crime Prevention Studies, pp. 225-50. Monsey, NY: Criminal Justice Press.

Burrows, J. N. (1979). The impact of closed circuit television on crime in the London Underground. In Crime in public view, Home Office Research Study no. 49, edited by Patricia Mayhew, Ronald V. G. Clarke, John N. Burrows, J. Michael Hough, and Simon W. C. Winchester. London: HMSO.

Carli, V. (2008) Assessing CCTV as an effective safety and management tool for crime-solving, prevention and reduction. Comparative Analyses Report. Montreal: International Centre for the Prevention of Crime. Available at: http://www.crime-prevention-intl.org/fileadmin/user_upload/Publications/La_videosurveillance_est-elle_un_outil_de_securite_et_de_gestion_efficace_FR.pdf. Accessed October 8, 2013.

Ceyhan, A. (1998) Analyser la sécurité: Dillon, Waever, Williams et les autres. Cultures and Conflits, 31-32. Available at: http://conflits.revues.org/index541.html. Accessed October 8, 2013.

Cicourel, A. V. and Kitsuse, J. I. (1963): A Note on the Use of Social Statistics. Social Problems, 11, 131-139.

Cusson, M. (2005). La surveillance et la télésurveillance: sont-elles efficaces? Revue internationale de criminologie et de police technique et scientifique, vol. 58, no 2, avril-juin 2005, 131-150. Available at: http://classiques.uqac.ca/contemporains/cusson_maurice/surveillances_et_telesurveillances/surveillances_et_telesurveillances.pdf. Accessed October 8, 2013.

Dee, H. M. and Velastin, S. A. (2008). How Close Are We To Solving the Problem of Automated Visual Surveillance? A Review of Real-World Surveillance, Scientific Progress and Evaluative Mechanisms. Machine Vision and Applications, 19(5-6), 329-343. Available at: http://www.comp.leeds.ac.uk/hannah/papers/mva07.pdf. Accessed October 8, 2013.

Ditton, J. (2000). Crime and the city: Public attitudes towards open-street CCTV in Glasgow. British Journal of Criminology, 40, pp. 692 – 709.

Ditton, J. and E. Short (1999) Yes, it works, no it doesn't: Comparing the effects of open-street CCTV in two adjacent Scottish Town Centres, Crime Prevention Studies, 10, pp. 201-223. Available at: http://www.popcenter.org/library/crimeprevention/volume_10/08-Ditto_Short.pdf. Accessed October 8, 2013.

Elliot, D. S. (1995). Lies, Damn Lies and Arrest Statistics. The Sutherland Award Presentation. The American Society of Criminology Meetings. Boston, MA. Available at: http://www.colorado.edu/cspv/publications/papers/CSPV-015.pdf. Accessed October 8, 2013.

Ferenbok, J. and Clement, A. (2012). Hidden Changes: from CCTV to "Smart" video surveillance. In: A. Doyle, R. Lippert and D. Lyon, (Eds). Eyes Everywhere: The Global Growth of Camera Surveillance. Routledge.

Gill, M.; Spriggs, A.; Little, R.; and Collins, K. (2006). What do murderers think about the effectiveness of CCTV? Journal of Security Education, 2, (1), 11 – 17.

Gill, M. and Spriggs, A. (2005), Assessing the impact of CCTV, Home Office Research Study, no. 292, London: Home Office. Grandmaison, Rachel, and Pierre Tremblay. (1997). Évaluation des Effets de la Télé—Surveillance sur la Criminalité Commise dans 13 Stations du Métro de Montréal. Criminologie 30:93-110.

Griffiths, M. (2003). Town centre CCTV: An examination of crime reduction in Gillingham, Kent. Reading, UK: University of Reading. Available at: http://www.popcenter.org/Responses/video_surveillance/PDFs/Griffith_nd.pdf. Accessed October 8, 2013.

Groombridge, N. (2008), Stars of CCTV? How the Home Office wasted millions – a radical 'Treasury/Audit Commission' view, Surveillance and Society, 5(1), 73-80.

Haering, N., Venetianer, P., and Lipton, A. (2008) The evolution of video surveillance: an overview. Machine Vision and Applications 19, 279–290.

Heilmann, E. (2003). La vidéosurveillance, une réponse à la criminalité?. Criminologie, vol. 36, n. 1, 89-102. Available at http://www.erudit.org/revue/crimino/2003/v36/n1/006554ar.html. Accessed October 8, 2013.

Huff, D. (1954) How to Lie with Statistics. New York: Norton.

Introna, L. D. and Wood, D. (2004). Picturing Algorithmic Surveillance: The Politics of Facial Recognition Systems. Surveillance and Society. CCTV Special (eds. Norris, McCahill and Wood) 2(2/3): 177-198. Available at: http://www.surveillance-and-society.org/cctv.htm. Accessed October 8, 2013.

Introna, L. D. and Nissenbaum, H. (2009). Facial Recognition Technology: A Survey of Policy and Implementation Issues. July, 22. Center for Catastrophe Preparedness and Response, New York University. Available at http://www.nyu.edu/ccpr/pubs/Niss_04.08.09.pdf. Accessed October 8, 2013.

IRISS (2012). Surveillance, Fighting Crime and Violence. Report of the project Increasing Resilience in Surveillance Societies. Available at: http://irissproject.eu/wp-content/uploads/2012/02/IRISS_D1_MASTER_DOCUMENT_17Dec20121.pdf. Accessed October 8, 2013.

Justice Analytical Services (2009), The Effectiveness of Public Space CCTV: A review of recent published evidence regarding the impact of CCTV on crime, Police and Community Safety Directorate, Edinburgh: The Scottish Government. Available at: http://www.scotland.gov.uk/Resource/Doc/294462/0090979.pdf. Accessed October 8, 2013.

Maguire, M. (2002). Criminal Statistics: The 'Data Explosion' and its Implications in M. Maguire, R. Morgan and R. Reiner (eds.). The Oxford Handbook of Criminology, Third Edition. Oxford: Oxford University Press.

Mayhew, P., Clarke, R. V. G., Burrows, J. N., Hough, J.M. and Winchester, S. W. C. (1979) Crime in public view. Home Office Research study 49. London: HMSO

Massumi, B. (2007). Potential Politics and the Primacy of Preemption. Theory and Event 10:2. Available at: http://muse.jhu.edu/login?auth=0andtype=summaryandurl=/journals/theory_and_event/v010/10.2massumi.html. Accessed October 8, 2013.

Mayer-Schönberger, V. (2009). Delete: The Virtue of Forgetting in the Digital Age. Princeton: Princeton University Press.

Melgaço, L. (2012). Estudantes sobre controle: a racionalização do espaço escolar através do uso de câmeras de vigilância. O Social em Questão, year XIV, n. 27, 193-212. Available at: http://osocialemquestao.ser.puc-rio.br/media/OSocial27_Se%C3%A7%C3%A3o_Livre_Melga%C3%A7o1.pdf. Accessed October 8, 2013.

Monmonier, M. (1996) How to lie With Maps. 2nd ed. Chicago and London: University of Chicago Press.

Morin, E. (2005). Introduction à la pensée complexe. Lonrai-França: Éditions du Seuil.

Norris, C. and Armstrong, G. (1999). The maximum surveillance society: The rise of CCTV. Oxford, UK: Berg.

Owen, K. et al. (2006), A short evaluation of the (economic) benefits of the Milton Keynes CCTV system in managing police resources, Leicester: Perpetuity Research and Consultancy International (PRCI) Ltd.

Reiner, R. (2002) Media made criminality: The representation of crime in the mass media. In: Reiner, Robert, Maguire, Mike and Morgan, Rod, (eds.) The Oxford Handbook of Criminology. Oxford University Press, Oxford, UK, 302-340.

Rios-Cabrera, R., Tuytelaars, T., and Van Gool, L. (2012). Efficient multi-camera vehicle detection, tracking, and identification in a tunnel surveillance application. Computer Vision and Image Understanding 116, 742–753.

Sivarajasingham, V.; Shephard, J.P.; and Matthews, K. (2003). Effect of urban closed circuit television on assault injury and violence detection. Injury Prevention, 9, (4), 312 – 316.

Smith, G. (2004). Behind the Screens: Examining Constructions of Deviance and Informal Practices among CCTV Control Room Operators in the UK, Surveillance and Society, 2(2/3): 376-395. Available at: http://www.surveillance-and-society.org/articles2(2)/screens.pdf. Accessed October 8, 2013.

Stirling, A. (2010). Keep it complex. Nature, 468, 1029–1031. 23 December.

Waples, S., Gill, M. and Fisher, P. (2009), Does CCTV displace crime?, Criminology and Criminal Justice, 9(2): 207-224.

Webb, B. and Laycock, G. (1992). Reducing crime on the London Underground: An evaluation of three pilot projects. Crime Prevention Unit Series paper no. 30. London: Home Office. Available at: http://www.popcenter.org/library/scp/pdf/189-Webb_and_Laycock.pdf. Accessed October 8, 2013.

Welsh, B. C. and Farrington, D. P. (2009). Public Area CCTV and Crime Prevention: An Updated Systematic Review and Meta-Analysis. Justice Quarterly 26(4), 716-745.

Welsh, B. C. and Farrington, D. P. (2007). Closed-circuit television surveillance and crime prevention: A systematic review. Stockholm: National Council for Crime Prevention.

Welsh, B. C. and Farrington, D. P. (2002). Effects of Closed-Circuit Television on Crime. The ANNALS of the American Academy of Political and Social Science 2003 587: 110-135.

[i] "Alors que la pensée simplifiante désintègre la complexité du réel, la pensée complexe intègre le plus possible les modes simplifiants de penser, mais refuse les conséquences mutilantes, réductrices, unidimensionnalisantes et finalement aveuglantes d'une simplification qui se prend pour le reflet de ce qu'il y a de réel dans la réalité." (Morin, 2005, p. 11).

[ii] For an analysis of costs and benefits of other surveillance technologies see IRISS (2012).

[iii] For the distinction between data, information, knowledge and wisdom, see Ackoff (1989).