When video cameras watch and screen: Privacy implications of pattern recognition technologies

Fanny Coudert
Interdisciplinary Center for Law & ICT (ICRI), K.U. Leuven, IBBT, Belgium

Abstract

Computer vision technologies based on pattern recognition software will soon allow identifying human behaviour that deviates from a pre-defined normality. Such applications are foreseen, amongst others, to be used in public places with purposes of crime prevention, especially in the context of the fight against terrorism. This technology increases the level of automation of video surveillance, changing the main nature of surveillance. The balance of power between the citizen and the State is altered, calling for a new balancing of interests. The automation of risk detection moreover raises the issue of the protection against partially automated decision-making. This paper will deal with the challenges raised by proactive video surveillance technologies to the way how privacy and security have been balanced so far. Attention will moreover be brought to the new safeguards that should be devised to protect the citizens from increased scrutiny and growing automation of the decision-making process.

© 2010 Fanny Coudert. Published by Elsevier Ltd. All rights reserved.

1. Introduction: from reactive to proactive surveillance

Computer vision, the ‘science of machines that see’, will soon make it possible to identify human behaviour that deviates from a pre-defined normality. Such is for instance the object of the research contest TRECVID (Text REtrieval Conference – VISio retrieval evaluation) organized every year since 2001 by the National Institute of Standards and Technology, a non-regulatory federal agency within the U.S. Department of Commerce, with additional support from the US government. The 2009 contest invited researchers from all over the world to compete for the design of the most accurate algorithms to detect events (patterns) such as ‘a person running’, a ‘person embracing other’, ‘a person taking photos’, based on video tapes provided by Gatwick airport surveillance cameras. In sum, normal events of a person’s life will be identified and screened by a machine against pre-defined patterns of ‘normal’ behaviours. In the long run, cameras located in public places can therefore be expected not only to record and monitor the everyday life of citizens but also to scrutinize their behaviour with purposes of crime prevention. Other uses include applications that monitor workers’ movements in order to improve workflow in factories (see e.g. the EU project SCOVIS), or applications that monitor customers’ gait in supermarkets to decide upon the best advertisement to be displayed (Schreurs et al., 2008).

Such powerful technologies change the nature of video surveillance (The Constitution Project, 2006) which evolves from a reactive to a proactive technology: video surveillance systems are now designed to identify risk factors in order to enable the operator to act upon the situation before the risk happens. Pre-defined (but evolving) patterns are used to monitor a target group and identify anomalies, based on complex probabilistic calculations. The ‘forecasting of the imaged human behaviour’ was already identified by the Working Party 29 in 2004 as ‘leading inconsiderately to dynamic-preventive surveillance — as opposed to the conventional static surveillance,
which is aimed mostly at documenting specific events and their authors’ (WP29, 2004).

The deployment of such invasive technologies raises the question of their impact on fundamental rights and eventually on the society as a whole. Risks of discrimination were already identified by the Working Party 29 (WP29, 2004). However, problems arise not only because ‘the more sophisticated a group profile becomes, due to the availability of ever more (relevant) data, the more it inclines towards a personalized profile and the more subtly it will discriminate between members and non-members’ (Schreurs et al., 2008) but also because proactive video monitoring exacerbates the risks linked to video surveillance as already identified and commented in several policy documents (WP29, 2004; Butarelli, 2000), such as the often described chilling effect on the way people behave, and because it raises new threats linked to the progressive automation of the decision-making process.

Protection against threats stemming from the use of new technologies is most commonly expected to be dealt with by data protection laws which however often appear ill-suited to provide an adequate protection. This paper intends to analyse not only which kind of protection can, but also should, be expected from the data protection framework to regulate proactive video surveillance monitoring with purposes of public safety. The new threats raised by the use of such technologies will be identified, before focusing on two specific issues, the balancing of interests at stake and the regulation of partially automated decision.

2. New surveillance tools, new privacy threats

2.1. Computer vision: towards automated surveillance

As a scientific discipline, computer vision is concerned with the extraction of added-value information from images captured by devices such as video cameras or any type of scanning system. The field for applications of computer vision systems is extremely broad but this paper will only focus on the applications aimed at detecting events (e.g. for people counting or visual surveillance including detection of abnormal behaviours, object recognition and tracking). These applications rely on pattern recognition software that extracts from raw data (images) observations to be classified or described based on a priori knowledge or on statistical information. The identification of abnormal behaviour by the system triggers an alarm, bringing the attention of the operator to specific events or starting the recording of a sequence. Integration of video surveillance with other systems and functions such as access control, alarm systems, building management, traffic management, allows the design of refined pre-configurable alarms and improves decision-making of operators (The Constitution Project, 2006).

Computer vision systems are being designed with the intent to improve video surveillance systems’ efficiency (the goal is more easily achieved) and efficacy (more of the goal is achieved). It facilitates the tracking of objects, such as cars or suspects, amongst the cameras of the network(s), the identification of suspicious behaviours or the detection of emergency situations. The spread of video camera networks has made it more difficult to monitor all incoming video feeds: computer vision provides the necessary help to operators in charge of watching multiple monitors. In words of Pane (2007), “computers never lose attention, so video analytics [computer vision] remedies the problem.” But more than the attention required to the operator, it is the ability to analyse the images which is at stake (Coudert and Dumortier, 2008). Computer vision is, according to IBM (2007), “designed to enable real-time decision-making and post event correlation of people and activities.” It enables “situation awareness of the location, identity and activity of objects in a monitored space including license plate recognition and face capture.” The city of Chicago has for instance acquired a video surveillance system that could be programmed to recognize and warn authorities of suspicious behaviour, such as a backpack left in a park or the same truck circling a high-rise several times. Chicago’s police have promised to grow the system until the city is covered from one end to the other. The interest of the city in the deployment of such comprehensive video surveillance network is motivated by the further linking up of the law-enforcement aspects with emergency services through a Central control room. The system uses a live Geographic Information System to match camera location to reported incident location, allowing the nearest cameras to immediately turning to picture the scene (Murakami Wood, 2009). The Golden Shield project in Shenzhen (China) went one step further: 20,000 smart cameras with face-recognition software were installed to monitor the 12, 6 million inhabitants of the city of Shenzhen (Bradsher, 2007). Further steps include linking the video surveillance system to the information stored in public databases about the persons identified.

Such applications, assuming that ‘the technologies used are sufficiently advanced and not prone to (too many) errors’ (Custers and Hildebrandt, 2009), thus appears in many aspects extremely valuable. However, as shown by the Golden Shield project their use is not free from consequences for fundamental freedoms.

2.2. Emerging threats from proactive video surveillance technologies

The development of proactive surveillance tools enables more privacy-intrusive practices. This is particularly obvious in the field of public security where such systems foster targeted surveillance, investigation or use of search powers. Security practices are evolving from reaction to crimes, i.e. focused on the gathering of conclusive evidence of wrongdoing ‘beyond reasonable doubt’ to put before a criminal court (Institute for Prospective Technological Studies, 2003), to proactive surveillance that targets the criminal and not the crime (Noris, 2007). A phenomenon of ‘technologization’ of security practices (Ceyhan, 2005) can be observed elsewhere. In that context, ‘technology appears as the most scientific solution for anticipating dangers and future threats’ (Ceyhan, 2005). Technology improves dramatically the efficiency of policing practices, allowing an increase in scale that would have been impossible using human observers (Bowyer, 2004). This is mainly because ‘automation allows for permanent surveillance’, promoting and
refining the methods of control, exposure, surveillance, normalization and manipulation (Gutwirth, 2002).

The impact on fundamental rights is twofold. On the one hand, the risks traditionally associated with video surveillance, such as the impact on the freedom of movement which implies the right to move without constantly being traced (WP29, 2004) or the chilling effect on behaviours in the persons being monitored (Butarelli, 2000), are exacerbated. Not only are individuals’ movement observed but they are also checked against pre-defined patterns of behaviours. Any deviation from ‘socially’ accepted behaviour (as defined when designing the pattern recognition’s software) automatically triggers the sending of an alarm to the operator who will decide the subsequent course of action to be followed. This could mean requiring the system to track the person or to send an agent to proceed to a closer examination of his or her conduct, maybe through an interrogation. In that context, everybody becomes a suspect. Proactive technologies are not specific to video surveillance but are part of a more general trend in the field of public safety and law enforcement. The screening of travelers offers another example. In words of the Commissioner for Human Rights of the Council of Europe (2008), ‘in the context of the fight against terrorism, this means individuals are at risk of being targeted for being suspected ‘extremists’ or for being suspected of being ‘opposed to our constitutional legal order’, even if they have not (yet) committed any criminal (let alone terrorist) offence.’ The Institute for Prospective Technological Studies (2005) identified, the progressive undermining of trust of the citizen in the State as one likely societal impact in the long turn. According to this Institute, “part of this trust is inherent in the concept of being considered innocent until proved guilty and in enjoying personal privacy and anonymity” (Institute for Prospective Technological Studies, 2005).

On the other hand, an increased use of computer vision systems renders individuals more exposed to automatic individual decisions. It facilitates tracking or behaviour analysis that can be by itself subject to specific safeguards, e.g. the obtaining of a warrant when performed by police for law-enforcement purposes, or that can result in harmful consequences for the individuals, e.g. discriminatory practices.

A fear which was already expressed in the debates surrounding the drafting of the Data Protection Directive was that ‘the result produced by the machine, using more and more sophisticated software, and even expert systems, has an apparently objective and incontrovertible character to which a human decision-maker may attach too much weight, thus abdicating his own responsibilities’ (European Commission, 1990). Bygrave (2001) refers in that sense to the ‘automatic acceptance of the validity of the decisions reached and a concomitant reduction in the investigatory and decisional responsibilities of humans.’ This leads to an implicit assumption as to the infallibility of the machine and to the fact that ‘the reasoning linking the premises and conclusions for these predictive judgments will be grounded in reality.’ Furthermore, in the words of Steinbock (2005), contrary to human judgment, ‘computer analysis has no way to evaluate the probable accuracy of the data on which it relies.’ It is also more difficult to evaluate than human assessment. In the case of event detection/pattern recognition, even if the machines ‘only’ send an alarm informing of an abnormal behaviour, the mere fact that the machine identifies an event as of risk implies that a judgment is being made about the conduct or person being observed.

In that regard, the presumption of innocence and the right to due process are increasingly invoked as means of protection of citizens against profiling technologies. However, a substantial obstacle emerges when considering that the actual configuration of the right under Article 6 ECHR is only envisaged in criminal proceedings: “the presumption only protects persons who are labeled ‘suspects’ in order to bring them before a criminal court.” (De Hert, 2005).

The increased automation of the decision-making process used for selection moreover threatens individuals’ autonomy (Custers and Hildebrandt, 2009) about behavioural biometrics profiling tools. Individuals are increasingly being judged by others, based on information that is made available through statistical analysis. Even if the impact at individual level may vary from situation to situation, the impact on society as a whole is identified as matter of concern, ‘certainly when used by government institutions to decide and act’ (Custers and Hildebrandt, 2009). In addition, risks of ‘de-individualisation’, where people are treated and judged on group characteristics not always valid for them as individuals, should be a matter of concern (Custers and Hildebrandt, 2009).

3. Balancing privacy with security in proactive video surveillance

Video surveillance activities can generally not be based on prior consent of data subjects, either because it involves an undetermined number of people or because it would undermine the main purpose of the processing. This is particularly the case for video surveillance systems implemented with security purposes. In words of Balboni (2005), this “would mean that the consent of potential thieves who want to break into a building or to rob a bank would be needed.” Video surveillance thus often implies a prior balancing of interests carried out by policy-maker when specific laws are enacted (e.g. France, Belgium, Spain) or by data protection authorities when prior authorization is required (e.g. in Italy) or when specific guidelines are issued (e.g. Spain, Italy). This section discusses the terms of the debate, analysing the interests at stake.

3.1. Balancing privacy with security, a zero-sum game?

Security and privacy are often presented as the two faces of the same coin continuously influenced by external factors. In words of the Institute for Prospective Technological Studies (2003), “if for some reason the perceived need for individual and collective security increases, emphasis on the maintenance of privacy tends to decrease.” Since 9/11, emphasis has however been put on the increase of security through the use of new technologies often without proper prior debate about their societal implications, particularly in terms of fundamental rights. Privacy is often presented as a mere obstacle to the implementation of more efficient security practices.

Deciding whether to deploy a certain technology, the goals this technology is expected to achieve or the legitimate
conditions of use, should undergo prior societal debate where the impact upon fundamental rights can be carefully assessed. Taking the example of the introduction of video surveillance and face-recognition systems into public places, Bowyer (2004) identifies three questions that should be answered before deciding their deployment, namely: "1) when or whether a sophisticated high-tech application works well enough to be worth deploying, 2) which elements of privacy are essential and which are inessential, and 3) what level of increased safety can come through the introduction of this technology."

To answer these questions, the metaphor of balancing of interests is often used. This has however been criticized by several scholars, all pointing out the fact that it inevitably leads to a "zero-sum game", incapable of providing satisfying solutions (see e.g. Hayes, 2006). If more privacy means lesser security and more security means less privacy, no wonder that the fear induced (and largely relayed by the Media) by terrorist attacks and the constant public messages feeding the feeling of insecurity leads the majority of citizens to be willing to sacrifice their freedom. The full consequences will only be fully appreciated when it is definitively and irremediably lost, for the (illusory) feeling that their lives and belongings are protected. The debate will thus consist in assessing how much ‘liberty’ could be lost and how much security is consequently gained. In the words of Bowyer (2004), "the full depth and meaning of Benjamin Franklin’s warning about trading liberty for security is not always appreciated. He posted the trade-off as one giving up "essential liberty" in order to obtain "a little temporary safety". Thus we can expect that much of the disagreement in this area comes down to whether the increase in safety is judged to be little or much, and temporary or permanent."

In order to give privacy back the fundamental role it should play in a democratic constitutional states, some scholars have stressed the importance of recalling the meaning of the right to privacy, i.e. the values it intends to protect, namely the right to dignity (Rouvroy, 2008; Dumortier, 2007) or to freedom (Gutwirth, 2002; De Hert and Gutwirth, 2006). Some even argue that such an important fundamental value should be insensitive to balancing against security (Dumortier, 2007). Security is presented here as an important public interest that has not yet been elevated to the rank of fundamental right. According to this reasoning, security could not be considered as part of a balancing exercise, as balancing implies competing interests of equal value.

3.2. What hides behind the concept of security?

The first question that arises is what gives security its legitimacy in a democratic constitutional state. The interests of national security, public safety, law enforcement could justify the derogation to the right to privacy (Article 8.2 ECHR). Security, understood as protection of the individual’s life and safety by the State, is moreover enshrined in the right to life (Article 2 ECHR). As a way of example, in Osman (28 October 1998), the European Court of Human Rights noted that Article 2 of the ECHR (right to liberty) may in well defined circumstances imply a positive obligation on the authorities to take preventive operational measures to protect an individual whose life is at risk from the criminal acts of another individual.

The answer lies in the theory of the Rule of Law that shapes the constitutional democratic state. At the heart of this State model is the idea of limitation of power by the protection of individual freedoms and the definition of a restrictive domain of competences to the State. The theory of the Rule of Law finds its origin in mistrust towards the State whose power will be tightened and framed to ensure it does not become oppressive (Chevallier, 1994).

The State is then entrusted with tasks critical to society, which only the former is able to carry out, such as the maintenance of law and order through appropriate security policies. To that end it is given the monopoly of force, regulated by laws and tied to specific ends (maximising the exercise of individual freedoms) that give its actions the required legitimacy. The structuring of the legal order is no more than a mean to ensure this limitation of power through Law (Chevallier, 1994). The State is thus given the primary mission to ensure the protection of fundamental rights, i.e. the right to liberty that may imply the use of force where necessary through security policies.

This has led Daugman to qualify the dichotomy between security and liberty as a false dichotomy because “under the ‘General Will’ theory (Rousseau’s formulation of the Social Contract), citizens collectively benefit from the existence of police forces, border controls and other arms of the state” (Kabatoff and Daugman, 2008). This analysis however does not reflect the pivotal role of human rights in a democratic constitutional state in framing the use of power. Not only is the power of the State limited by fundamental rights that allow individuals to oppose such power, but this power finds its main justification in the guarantee of such rights (Chevallier, 1994).

3.3. Privacy as counterweight in imbalanced power relationships

The approach of Gutwirth to privacy in terms of power relationship provides a better insight into the role of human rights in protecting individuals from excessive State power. According to Gutwirth (2002) “the democratic constitutional state is deeply involved in the issue of power distribution (...). It aims to keep the balance of power as much as possible within an acceptable proportionality.” Human rights and the Rule of Law are seen in this context as ensuring the “autonomy, freedom, and self-determination of an individual and they protect an individual against the ambitions of the authorities, legal entities, and other citizens.” The Law plays a role of preventing, “through mediation, power relations from becoming absolute.” Fundamental rights such as the right to privacy, enable the Law to fulfill its task.

Privacy is understood by Gutwirth (2002) as a claim to freedom. Privacy becomes the guardian of the weak party in the power relationship, allowing him or her to resist that power. In that regard, privacy imposes a balancing of power and resistance in all power relationships: the destruction of privacy is seen as an instrument of power. According to this author, a rule of thumb could be ‘the bigger the imbalance of power, the bigger the protection of privacy.’ Gutwirth analyses the balance of interests as a balance of powers where the Law should be entrusted with the task of protecting the weak party, the citizen, by giving him or her the means to resist such imbalanced use of power.

Proportionality is expected to play a key role in this balancing exercise. However, the mere balancing act is
presented as insufficient. Instead Gutwirth prefers to refer to privacy as counterweight to the power of the State (and other relevant stakeholders). It follows that ‘the emancipatory use of privacy should go beyond the fact that legislators, judges, and administrators give it sufficient consideration. They also have to run a permanent catch-up operation to make sure that privacy can play its full role as counterweight in the face of new, threatening developments.’ Policy-makers should then assess the impact of the technology on the ability of the citizen to resist and remain free from unfair or excessive use of power, taking into account the public interest (obligation) in maintaining public order as entrusted to the State.

4. Data protection law as tool of protection against proactive video monitoring

The regulation of video surveillance monitoring has been mainly approached from the perspective of data protection laws. The right to privacy is however worded in such general terms that it is often difficult to indicate clearly how new technologies should be deployed or developed (Kindt and Hildebrandt, 2009). Data protection, on the contrary, is applicable whenever personal data are processed, providing a somewhat objective tool to protect individuals and as a result, giving more legal certainty than privacy law (Schreurs et al., 2008). Privacy and data protection have always been intertwined, being necessary to define the different role they play in the regulation of new technologies. This analysis will shed some light on what can and should be expected from data protection laws when regulating proactive video monitoring.

4.1. Protecting privacy through data protection laws

The need to adopt a constitutional approach to data protection legislation rather than focusing on a legalistic narrow view in the application of the data protection legislation is increasingly stressed by the doctrine (Brown and Korff, 2004), particularly since the right to data protection has been emancipated from the right to privacy by the European Charter of Fundamental Rights. This implies to define the role this right plays in a democratic constitutional state in protecting fundamental freedom from threats arising from the use of new technologies.

In that sense, the approach developed by De Hert and Gutwirth (2006) based on the concepts of ‘transparency’ and ‘opacity tools’ in a democratic constitutional state, sheds some light on the way the right to privacy and the right to data protection interact in the regulation (and thus in the legitimisation) of new technologies. Opacity tools will function negatively to define which uses of technology should be banned. On the contrary, transparency tools will regulate the legitimate uses of such technologies, implementing procedural safeguards to ensure that these safeguards are respected.

Whereas the right to privacy mainly functions negatively in that it ensures the non-interference in private matters of the individual, acting in that sense as an ‘opacity tool’, data protection laws act instead as a set of ‘transparency tools’, i.e. ‘they regulate rather than prohibit personal data processing’ (De Hert and Gutwirth, 2006). It follows that when faced with an intrusive technology, the right to privacy (and other relevant fundamental rights) will serve as reference to define whether the technology should be allowed and under what circumstances. By comparison the right to data protection will come into the play only secondarily, to regulate these ‘socially acceptable uses’, i.e. to minimise the impact of the technology on the fundamental rights endangered. This however means that the policy choices made when regulating personal data processing imply prior choices as to the definition of the ‘legitimate’ uses of a given new technology. The main act of regulating personal data processing activities, such as the use of proactive video surveillance systems, therefore defines the socially acceptable uses of such technology. Regulating proactive uses of video surveillance technology through data protection laws thus means first and foremost, balancing privacy with security.

The previous developments shed a new light on the questions identified by Bowyer (2004). When dealing with a new technology such as proactive surveillance, which makes use of pattern recognition software, not only should the maturity of the technology be taken into account (when or whether a sophisticated high-tech application works well enough to be worth deploying), but also the way this technology affects the balance in power and reduces the ability of citizens to remain free from State interferences should be assessed (which elements of privacy are essential and which are inessential), as well as which uses of such technology should be deemed legitimate and subject to which conditions (what level of increased safety can come through the introduction of this technology). Data protection legislation will thus have a key role to play in this configuration as it will define the legitimate uses which can be made of this technology, giving data subjects the procedural means to resist to this new established power.

4.2. Assessing the proportionality of the video data processing

The principle of proportionality is the key for the definition and regulation of the legitimate uses of video surveillance systems. The proportionality test, according to the criteria established by the European Court of Human Rights under Article 8 ECHR (right to privacy), means that video surveillance systems should not only be able to achieve the goals foreseen (adequacy test) but also be strictly necessary (necessity test) and finally provide sufficient benefits for the public interest to compensate the harm caused to other competing values (proportionality test stricto sensu). The strict application of the proportionality principle is expected to prevent the emergence of pervasive surveillance which could result in an increased vulnerability of individuals. Furthermore, additional criteria can be extracted from the Council of Europe Recommendation R(87) 15 regulating the use of personal data processing in the police sector which for instance requires the existence of a real danger for the processing of personal data by police (Principle 5.1). This should prevent the installation of video surveillance systems in quiet neighborhoods where no violent act has been registered.

National laws have thus proceeded to define the purposes for which video surveillance cameras could be installed by public
authorities. Other measures have tended to minimise the impact on individuals’ privacy by reducing storage period, strictly defining the areas that could be filmed (data minimisation principle), or improving the transparency of such processing by the mandatory use of information notices and ensuring that data subjects could exercise their rights of access.

As regards the limitation of purposes, the deployment of video surveillance systems should first be limited to cases where alternative means and/or security measures prove clearly insufficient or inapplicable in view of the purposes of the processing. The Data Protection Authority of the Madrid Region (Spain) (2007) has for instance imposed on public authorities a duty to assess the needs grounding the use of video surveillance systems prior to their installation. Privacy impact assessments are thus required before the video surveillance system is implemented. Similarly, although less formal, the Italian guidelines on video surveillance (Il Garante, 2004) recommend that the data controller, before deploying a wide surveillance device, assesses “from an objective viewpoint and in selective manner, whether the planned implementation is actually proportionate in concrete to the purposes sought, which must be lawful.”

The Italian guidelines further develop the criteria that should be used to evaluate the necessity of video surveillance processing aiming at public safety. The use of video surveillance systems should be limited to situations where there is “actual, proportionate requirements concerning prevention or suppression of concrete, specific dangers as impending on a good — this is the case, for instance, of premises exposed to actual dangers or events that can reasonably produce prejudicial effects.” This for instance leads this authority to conclude that “it is unlawful to perform pervasive video surveillance of whole areas in a city — perhaps imaged in full and without intermission in the absence of adequate requirements — if the conditions referred to above are not fulfilled (…)”. This also excludes minor offences from the scope of surveillance such as prohibition against smoking or littering, walking on grass, posting bills, taking pictures, and any other activities such as depositing garbage in the appropriate bins. Similar approaches were followed in other countries, such as France or Spain.

However, recent developments point towards a loosening in the concept of ‘real danger’ or ‘suppression of a specific criminal offence’. Such concepts are progressively broadened so as to include the processing of data related to innocent people with the purpose of identifying potential criminals of ‘serious crimes’. As a way, for example, in France, the Act of 23 January 2006 for the fight against terrorism has expanded the lists of motives that could base the use of video surveillance systems so as to include the prevention of terrorism. Law-enforcement authorities have moreover been authorized to access images outside judicial proceedings. Public authorities are allowed to install video surveillance systems for the “prevention of terrorism”. Places and premises open to the public can also be subject to video surveillance when the place is likely to be exposed to terrorism acts. Additional safeguards advocated by the CNIL, the French data protection authority, to counterbalance these new powers were however not taken into account. This included limiting the authorization to perform video surveillance for the purposes of the fight against terrorism to a pre-defined period of time; to introduce mandatory independent assessments of the efficacy of the system in order to assess their legitimacy; and to strengthen the information provided to the persons being monitored (CNIL, 2006).

Furthermore, these Acts and guidelines only deal with ‘static’ video monitoring without taking into account the specific nature of proactive video surveillance. Whenever national laws have tended to define the purposes of video surveillance systems, it is likely that the introduction of a technology that improves the efficiency and the efficacy of the surveillance (therefore improving the ability of such technology to meet its goal), will comply with the requirements defined by national legislation. Data minimisation requirements, i.e. that mandates limitations on the collection of personal data to the ones strictly necessary and adequate to achieve the purposes of the processing, could however limit in some way the deployment of proactive video monitoring. However, chances are high that such requirements would be bypassed by imperatives of efficiency. Whenever prior control or authorization by data protection authorities is required (such as in Italy), these authorities will be given the opportunity to balance the proportionality of the video surveillance system and will be able to introduce additional and more adapted safeguards with hopefully more success than the CNIL. It however seems unavoidable to proceed to a new balancing of interests, defining the legitimate uses of proactive video monitoring with purposes of public safety and to devise new safeguards. Such safeguards should necessarily include privacy impact assessments as to assess the efficiency of the system on a regular basis. Strict definition of the uses and the persons authorized to use such functionalities should also be defined. The rights of information and of access should finally be strengthened as to empower data subjects to check the lawfulness and fairness of the processing.

4.3. Which protection against partially automated decisions?

Another major issue emerges as proactive video monitoring relies on pattern recognition, partially automating the surveillance performed. The machine becomes the one selecting the events or persons to monitor. This aspect has been only partially dealt with by the Data Protection Directive (Directive 95/46/EC) that is moreover not applicable to processing with purposes of crime prevention. The Directive has however provided a first (and embryonic) protection against automated decision-making processing activities that proves useful for the analysis.

Proactive video monitoring makes use of profiling technologies. Profiling is “the process of ‘discovering’ correlations between data in databases that can be used to identify and represent a subject and/or the application of profiles (sets of correlated data) to individuate and represent a subject or to identify a subject as a member of a group or category” (Schreurs et al., 2008). Group profiling consists in identifying persons that meet the pre-defined ‘group’ characteristics. Legal aspects of group profiling have received little attention so far from the doctrine and have been dealt with in the context of ambient intelligence. Schreurs et al. (2008) have shown that group profiling can affect individuals in a number of ways, even when the raw data are anonymous, especially in terms of increased automation of decision-taking.
The authors point out a series of gaps in the protection that current legislation could not fill. Most problematical points arise when determining to what extent data protection legislation applies to group profiling and how such legislation should apply in order to ensure a high level of protection.

In proactive video monitoring, profiles are applied to identifiable persons, the WP29 having long asserted that individuals monitored by video surveillance systems were ‘identifiable’ persons, triggering the application of the data protection framework (WP29, 2004). The question thus rather resides in how data protection legislation can protect citizens from new vulnerabilities generated by the use of such systems.

The growing automation of decision-making raises a series of concerns. As mentioned above, whereas the whole processing leading to the selection of which individual to monitor is not automated (a human person still makes the decision of the course of action to be followed once the system has identified a ‘risk factor’) the detection of ‘abnormal behaviours’ and thus of selection of facts to further investigate, monitor and track is left to a machine. The aforementioned belief in the infallibility of the machine leads to a state of affairs where the machine gains influence over the operator who is unlikely to take action against the diagnostic of the machine.

In that sense, Article 15 of the Data Protection Directive has regulated automated decision stating that: “every person has the right not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.” Bygrave (2001) has however soon warned against the insufficiencies of such article: difficulties arise as to defining when decisions will produce legal effects or when decisions “significantly affect” data subjects or in which cases a decision can be said to be based solely on automated data processing. This last requirement, limiting the scope of protection to wholly automated decision-making process, often leads in practice to the inapplicability of the protection as human intervention is rarely entirely suppressed.

The case of proactive monitoring raises the interesting question of the regulation of partly-automated decision-making processes and the protection against the influence of the machine upon the man.

Furthermore, Article 15.2 authorizes automated decision-making whenever provided for by a law, bringing us back to the considerations of the prior section on the balancing of interests. These questions appear particularly pressing as proactive video surveillance applications give public authorities enormous powers of control. This appears more obvious when considering the use of pattern recognition software together with face-recognition technology that can link an alarm with information stored in public databases. Whereas this scenario is worthy of a science-fiction movie, the deployment of smart cameras making use of face-recognition software in Shenzhen (China) is concomitant to the launching of an electronic resident card. These are fitted with a microchip containing information, not only about the citizen’s name and address, but also work history, educational background, religion, police records and medical insurance status. The fact that this card was about to be distributed to Chinese citizens, gives this scenario the ring of truth. As stressed by Schreurs et al. (2008), “the use of extensive data profiles of individuals by powerful public and private institutions indeed deprives the individual of the capacity to influence decision-making processes within those institutions, should decisions be taken on the sole basis of his data shadows.”

Recommendations from Schreurs et al. (2008) to improve the safeguards implemented by the data protection framework in the field of ambient intelligence focus on ensuring that: 1) individuals (should) have the right to object to profiling in certain situations and that 2) whenever the construction or the application of profiles takes place, they should have the right to know who, when and why the data relating to them are processed. In the field of security, this is however not enough. Additional safeguards limiting the power of the State and ensuring its accountability should be devised and incorporated into the data protection framework before foreseeing the deployment of such privacy-intrusive technologies. The more intrusive a technology appear, the more restrictive its use should be.

5. Conclusion: towards an improved protection against proactive video monitoring

Warnings against the risk of citizens losing trust in the State because of the introduction of new technologies that increasingly turn innocent people into suspects (Institute for Prospective Technological Studies, 2003) and increase the surveillance of the society as a whole, show that careful societal debates cannot be avoided before privacy-invasive technologies are deployed. Proactive video surveillance technologies are one example of such technologies. The role of privacy as a counterweight to State power should be restated through stringent regulation of privacy-invasive practices. In that sense, socially acceptable uses should be defined through the data protection framework, implementing strict safeguards to re-establish the balance of power.

Actual safeguards prove insufficient to provide a satisfactory protection against proactive monitoring. Proactive surveillance exacerbates the traditional risks identified in matters of video surveillance, requiring a new balancing of interests. It moreover creates new threats mainly linked to a progressive automation of the decision-making process that is not currently dealt with by the data protection framework. Whereas it appears necessary to enact specific regulation because of the changes proactive video monitoring trigger in the main nature of video surveillance, it also appears urgent to start regulating the increased automation of surveillance practices. The machine is now the one selecting which behaviours should be tagged as ‘suspect’ or ‘dangerous’. Increase in the scale of the surveillance and in the difficulties in detecting possible errors in the design and functioning of the software, calls to devise new (data protection) safeguards that would limit the power of the State and ensure its accountability.

As suggested by Kindt and Hildebrandt (2009), individuals should be given the possibility to access the logic behind pattern recognition. This appears however not sufficient because on the one hand, the individual often lacks the required technical knowledge to fully understand such logic and on the other hand the inherent opacity of the processing will often form a powerful barrier to the exercise of such right. It is therefore necessary to accompany such processing with strict privacy impact
assessments that would permit analysis of the opportunity, efficiency and efficacy of the processing, as well as to strictly define the authorities that can make use of such technologies and the cases where their use is deemed legitimate.

Fanny Coudert (fanny.coudert@law.kuleuven.be) Interdisciplinary Center for Law & ICT (ICRI) K.U. Leuven, Belgium, & IBBT (Interdisciplinary Institute for Broadband Technology).

Acknowledgements

This paper is based on research in the 7th framework EU project SCOVIS. This paper and the research in SCOVIS is supported and funded by the EU Commission. However, the paper is merely representing the author’s view and is not binding SCOVIS partners or the European Commission.

References


Butarelli G. Report to the Council of Europe on protection of personal data with regard to surveillance and guiding principles for the protection of individuals with regard to the collection and processing of data by means of video surveillance; 2000.


Ceyhan A. Technologie et se´ curite´ : une gouvernance libe´ rale dans un contexte d’incertitudes. Cultures et Conflits 2005;64.


Data Protection Authority of the Madrid Region [Agencia de Proteccion de datos de la Comunidad de Madrid]. Sobre el tratamiento de datos personales a través de sistemas de cámaras o videocámaras en el ámbito de los Órganos y Administraciones Públicas de la Comunidad de Madrid [Instruction 1/2007, of 16 May, on the processing of personal data through video surveillance systems within Public bodies and authorities of Madrid Community]; 2007.


Hayes B. There is no “balance” between security and civil liberties – just less of each. In: Essays for civil liberties and democracy in Europe. Essay, no. 12; 2006, ECLN.org; 2006.


Institute for Prospective Technological Studies. Biometrics at the frontiers: assessing the impact on society; 2005.


