available at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

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

Keywords:
Pattern recognition technology
Surveillance
Video cameras
Privacy and security
Data protection
Automated decision-making

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.

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 – VIDeo 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,*

☆ First presented at the 4th International Conference on Legal Security and Privacy issues in IT Law (LSPI), Malta, 3–5 November 2009.

0267-3649/$ – see front matter © 2010 Fanny Coudert. Published by Elsevier Ltd. All rights reserved.
doi:10.1016/j.clsr.2010.03.007

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 how 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 loose 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