

Chapter XII

Surveillance in the 21st Century: Integration of Law and Technology

Pieter Kleve

Erasmus University, The Netherlands

Richard V. De Mulder

Erasmus University, The Netherlands

Kees van Noortwijk

Erasmus University, The Netherlands

ABSTRACT

In this chapter, some current technologies for monitoring and surveillance as well as some legal considerations regarding the application of these technologies will be discussed. The application of monitoring technology has developed from the monitoring of mere technical processes and environmental processes to the monitoring of physiological “processes” and now even of everyday human behaviour. Before discussing legal considerations, an explanation of this development is given and it is placed within a broader social perspective. This leads to an examination of the development of technology that made it possible for monitoring technologies to evolve as they did, and an analysis of norms and values resulting in a conceptual model for evaluating law in the “information society”. An overview of technologies for monitoring and surveillance will be presented. From this overview it will become clear that the use of this type of technology is growing fast. At the same time, questions arise regarding its permissibility in the light of legal and constitutional rights, such as the right to privacy. These questions are then addressed in the context of the wider social developments. Finally, it is concluded that with the increasing importance and use of surveillance technology, “monitoring the surveillers” will become essential as well.

INTRODUCTION

Technology for surveillance and monitoring has, in today's society, become commonplace. In the Netherlands, for example, certain so-called 'sniffing poles' have been installed. These measure the level of air pollution and when a certain limit is reached a warning system is activated. As a consequence of the disastrous tsunami in December 2004, a tsunami warning system has been installed in the Indian Ocean. Hospitals use technology to monitor the state of the human body and our financial obligations are monitored by computers that send us reminders and final demands if the payment has not been made on time.

Monitoring technology is used to supervise both social and physical processes, and to monitor individual behaviour. This technology is constantly being refined. For example, speeding, as an offence that forms a risk to public health, has for some time been dealt with by technology. The standard approach has been to have a camera that takes a photograph of the car once a certain maximum speed has been exceeded. Having established the level of the speeding, a fine is then sent to the car owner. However, in this set up the camera can only register the offence if it takes place where the camera is located; speeding either before or after the location of the camera cannot be registered. To remedy that deficiency, a new form of surveillance has made its appearance: it is now possible to follow the car along a section of the road. A camera located at one place on the road registers the speed of the car at that point and a camera placed a number of miles farther down the road registers the speed there. A computer then calculates the average speed of the car along that stretch of road between the two cameras. If the average speed is too high, a fine will be sent. For the road user, this development means that it is pointless just to slow down at the location of the first camera; speed must be kept down for the whole stretch of road between the two cameras. (It should perhaps be pointed out that this technology

will not catch the driver who only speeds for a very short time on that section of road.)

In the above example, there are legitimate legal grounds for the use of surveillance technology; the law has already laid down what constitutes the maximum speed and the carrying out of the procedure is the responsibility of the state. This surveillance technology has led to a certain conditioning of driving behaviour. However, even though we have become familiar with the use of road cameras, that does not mean that their existence is accepted by all road users. It could be that we consider that driving above the speed limit on that particular road, or section of the road, is not dangerous, or that we have a good excuse for speeding. When the check-points were manned by police officers, a sympathetic officer might have been prepared to accept a good story; a camera is not.

Road cameras have stimulated some drivers to find means of evasion. One such technique is the radar detection device, which warns of the vicinity of radar controlled speed measurement equipment. That has led some authorities to demand that such detection devices be made illegal (and consequently some manufacturers have developed detection devices that do not fall within the category of 'illegal radar detection devices'). What this shows is that a rule of law does not, of itself, produce compliancy. Individuals will act in their own self-interest, as they see it (cf. Jensen & Meckling (1994) pp. 4-19). This action/ reaction phenomenon draws attention to the relationship between a rule of law and the enforcement of that rule of law. The enforcement of a rule of law is of great importance. The use of technology may promote compliance with the law, although that is not always necessarily the case.

Surveillance by camera is, of course, not confined to traffic situations. The use of camera surveillance is common in shopping centres, petrol stations and industrial areas, to name just a few examples. Moreover, camera surveillance is on the increase. If you wish to visit a company,

19 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

www.igi-global.com/chapter/surveillance-21st-century/29365

Related Content

A Cyber Crime Investigation Model Based on Case Characteristics

Zhi Jun Liu (2020). *Digital Forensics and Forensic Investigations: Breakthroughs in Research and Practice* (pp. 164-172).

www.irma-international.org/chapter/a-cyber-crime-investigation-model-based-on-case-characteristics/252687

Two Methods for Active Detection and Prevention of Sophisticated ARP-Poisoning Man-in-the-Middle Attacks on Switched Ethernet LANs

Kenan Kalajdzic, Ahmed Patel and Mona Taghavi (2011). *International Journal of Digital Crime and Forensics* (pp. 50-60).

www.irma-international.org/article/two-methods-active-detection-prevention/58408

Virtual Sample Generation and Ensemble Learning Based Image Source Identification With Small Training Samples

Shiqi Wu, Bo Wang, Jianxiang Zhao, Mengnan Zhao, Kun Zhong and Yanqing Guo (2021). *International Journal of Digital Crime and Forensics* (pp. 34-46).

www.irma-international.org/article/virtual-sample-generation-and-ensemble-learning-based-image-source-identification-with-small-training-samples/277091

Monitor and Detect Suspicious Transactions With Database Forensic Analysis

Harmeet Kaur Khanuja and Dattatraya Adane (2020). *Digital Forensics and Forensic Investigations: Breakthroughs in Research and Practice* (pp. 402-426).

www.irma-international.org/chapter/monitor-and-detect-suspicious-transactions-with-database-forensic-analysis/252703

Collision Analysis and Improvement of a Parallel Hash Function based on Chaotic Maps with Changeable Parameters

Min Long and Hao Wang (2013). *International Journal of Digital Crime and Forensics* (pp. 23-34).

www.irma-international.org/article/collision-analysis-and-improvement-of-a-parallel-hash-function-based-on-chaotic-maps-with-changeable-parameters/83487