available at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Towards a new generation of CCTV networks: Erosion of data protection safeguards?

Fanny Coudert

Katholieke Universiteit Leuven – IBBT, Belgium

Keywords:
CCTV networks
Data protection
Privacy
Video surveillance
Information sharing

ABSTRACT

CCTV networks are progressively being replaced by more flexible and adaptable video surveillance systems based on internet protocol (IP) technologies. The use of wireless IP systems allows for the emergence of flexible networks and for their customization, while at the same time video analytics is easing the retrieval of the most relevant information. These technological advances, however, bring with them threats of a new kind for fundamental freedoms that cannot always be properly assessed by current legal safeguards. This paper analyses the ability of current data protection laws in providing an adequate answer to these new risks.

1. Introduction: moving towards an interconnected society

During the last decade, an increased centralisation of databases, networks and systems has taken place at both a regional and national level. Suffice is to mention the introduction into the European legal framework of the principle of availability,[1] which "entails that information needed for the fight against crime should cross the internal borders of the EU without obstacles".[2] The principle as applied to DNA data was implemented by the Prüm Treaty,[3] which encourages Member States of the EU to create new databases on a national scale, through an obligation to create and keep DNA analysis files for the investigation of criminal offences.[4] As way of example, the UK DNA database, the largest in the world, already contains details of about 4.5 million people, including information on every person arrested, convicted or not, and on 900,000 children.[5]

As a consequence, the reuse of information for a completely different purpose to the one for which it was collected is becoming more common. This is illustrated by the processing of so-called "passenger name record data" (PNR data) collected for the provision of a transportation service, and then further communicated to public authorities for public safety purposes; or by the mandatory retention obligation for internet service providers (ISPs) to store traffic data

[1] The Hague Programme: strengthening freedom, security and justice in the European Union, 13 December 2004, Council of the European Union, 16054/04 (JAI 559).

[2] European Data Protection Supervisor. Opinion on the proposal for a Council Framework Decision on the exchange of information under the principle of availability, COM (2005) 490 final, 17 May 2006.

[3] Convention between the Kingdom of Belgium, the Federal Republic of Germany, the Kingdom of Spain, the French Republic, the Grand Duchy of Luxemburg, the Kingdom of the Netherlands and the Republic of Austria on the stepping up of cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal migration, signed by the contracting parties in Prüm (Germany) on the 27 May 2005. This Convention was integrated into the EU framework by the Council decision on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, 17 April 2007, doc. 7273/1/07, European Council meeting of 12–13 June 2007.

[4] Kosta E, Coudert F, Dumortier J. Data protection in the third pillar: in the aftermath of the ECJ decision on PNR data and the data retention directive. International Review of Law, Computers and Technology November 2007;21(3):343–58.

[5] The United Kingdom Parliament, Home Affairs, Third report; 24 May 2007.

0267-3649/$ – see front matter
doi:10.1016/j.clsr.2009.02.003

(i.e., data processed for the purpose of the conveyance of a communication on an electronic communications network, such as IP addresses) for a period up to 18 months, on the sole basis of the future and uncertain need to pursue criminal activities.[6]

These trends are not however exclusively seen from the public sector acting on the basis of public safety needs, they are also commonly observed in the private sector as well. The marketing sector, for instance, intensively uses extremely large databases that process personal data obtained from multifold sources. This has prompted NGO LIBERTY to observe that:

> *The commercial use of data is a massive growth industry. Tesco's Crucible database is reputed to have constructed a profile of every person in the UK regardless of whether they have shopped there. The information contained in it will then be sold to other companies. An increasing number of companies exist solely to sell data accumulated elsewhere.*[7]

The sheer growth and impact of mass databases are also linked to the development of powerful data mining and matching tools that allow for the exploitation of these databases by the extracting of information with added value, such as personal profiles or risk tendencies. Data mining tools are described as the ''means by which innocuous mass data is processed to allow an indication of characteristics or tendencies that might be used to justify some further and more intrusive step such as targeted surveillance, investigation or use of search powers''.[8]

Video surveillance does not escape from this phenomenon. CCTV networks have spread throughout urban area in response to public safety concerns, as a deterrent to crime and for evidence gathering purposes. Other important public interests such as traffic monitoring and private interests mainly focused on security have also motivated the large deployment of such systems, interweaving a web of video cameras that monitors everyday life of millions of citizens.

The efficiency of these networks, i.e. their ability to achieve the goals they were set for, has been however seriously challenged, in particular for crime prevention or deterrence.[9] This has led to serious concerns amongst privacy advocates who are contesting the legitimacy of such networks. Privacy International, for example, filed a complaint with the Ontario Information and Privacy Commissioner's Office regarding the plans to install 12,000 cameras across Toronto's transportation network of buses, streetcars, and subways on the basis that several international criminal studies had shown that video surveillance networks were failing to act as deterrent.[10]

Technological efforts are thus focusing on the more effective use of the information gathered by video surveillance cameras. The European Project DYVINE (DYnamic VIsual NEtworks)[11] offers an interesting example of these technological advances. This project aims at implementing a dynamically configurable video surveillance network that would give accurate and focused information on the status of incoming catastrophes. More particularly, it seeks to provide Civil Protection bodies with enhanced crisis management tools. The system would link, on a permanent basis, all the video surveillance networks owned by a local authority to each other. Such a linked network could moreover be connected to other networks (including private ones) ''on demand'', wherever it appears necessary for the effective management of the catastrophe. The possibility to integrate smart mobile cameras will moreover allow for the dynamic and adaptable configuration of specific alarms according to the needs of the situation. These features are complemented by the use of an advanced software module enabling the fusion of overlapping video data, the correlation of heterogeneous information and the tracking of persons and objects in large areas. It could moreover support artificial intelligence tools such as face-recognition software or human behaviour analysis to detect abnormal events.

The use of video analytics tools puts into play another dimension of the advances made by technology. Video surveillance systems do not only extend their scope of action by their integration, but also via their linkage to external databases in order to enrich the information initially collected. This creates a multitude of possibilities in terms of individual tracking and behaviour analysis. The Golden Shield project, for instance, participating from China's response to the ''war on terror'', has been described as an ''all encompassing surveillance network – a gigantic online database – incorporating speech and face recognition, closed-circuit television, smart cards, credit records and internet surveillance''.[12] As an example of how truly encompassing this network would be, in August 2007, the press unveiled that

[6] Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC. Official Journal 15 March 2006;L105:54–63.

[7] Liberty. Overlooked: surveillance and personal privacy in modern Britain; October 2007. Available online at: http://www.liberty-human-rights.org.uk/issues/3-privacy/pdfs/liberty-privacy-report.pdf.

[8] Ibid.

[9] See, for example, Heilmann E, Mornet M-N. L'impact de la vidéosurveillance sur les désordres urbains: le cas de la Grande Bretagne. Cahiers de la Sécurité Intérieure, 46, 4th trimestre; 2001. p. 197–211, or more recently, the studies mentioned by Privacy International at: http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-558046.

[10] Privacy International. PI files complaint about expansion of CCTV on Toronto transit network; 25 October 2007. Available online at: http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-558046. The Ontario Information and Privacy Commissioner's Office did however not follow the arguments raised by Privacy International based on the fact that video surveillance systems were not installed and used only for purposes of crime deterrence but also for risk management, public safety, detection and prosecution of crimes. See, Ontario Information and Privacy Commissioner's Office, Privacy and Video Surveillance in Mass Transit Systems: A Special Investigation Report, Privacy Investigation Report MC07/68, 3 March 2008.

[11] More information can be found at: www.dyvine.org.

[12] See for instance, Bradsher K. Big brother gets high-tech help in Shenzhen. International Herald Tribune 12 August 2007. Available online at: http://www.iht.com/article/2007/08/12/asia/china.1-113312.php.

20,000 smart cameras with face-recognition software were to be installed to monitor the 12.6 million inhabitants of the city of Shenzhen, and that electronic residence cards fitted with a microchip containing information on not only the citizen's name and address, but also work history, educational background, religion, police records or medical insurance status were about to be distributed to Chinese citizens.[13] The images captured by the CCTV network could thus actually be checked against this database to identify criminals and to increase control over the population's activities.

These technological advances challenge many EU regulations, mainly concerning data protection, which were not designed to deal with the issues stemming from the creation of an interconnected society. The benefits foreseen by these new technological developments are not contested. However, their impact on individual liberties should not simply be ignored because of apparent overriding public or private interests.

This paper will focus on the ability of current data protection laws in providing an adequate answer to these new risks. Even if data protection laws were originally created to provide safeguards against the interconnection of public databases, there were designed in substantially different technological context. This has led some scholars to argue that recent technological advances render the protection inefficient, calling for substantial changes in the legislative approach. This paper will first recall the rationale of data protection legislation and the nature of the claims made against their efficiency to, in a second part, analyze the threats posed to their application and offer some keys for adequately dealing with them.

2. The efficiency of data protection safeguards put into question

Before discussing the core principles contained in the data protection legislation and how new technologies challenge their application, it first appears necessary to recall what the right to privacy, as protected by data protection legislation, is meant to protect.

2.1. *The rationale of privacy protection*

2.1.1. *The right to privacy*

The simplest modern legal definition of privacy came from the 19th century American lawyer Judge Cooley who defined it as "the right to be let alone".[14] Privacy is thus a relatively recent right which has progressively found a place in western legislation, first introduced as a subjective right in torts law before acquiring a constitutional status in some jurisdictions.[15]

The right to privacy is, however, more than a mere protection against the intrusion of third parties: it aims above all to build the citizen's personality, and to provide him or her with the possibility to realize his or her full potential in society. It thus consists in a *right to be different*, which should ultimately "allow society to stay alive and to protect innovating way of thinking and living".[16] In that sense, Dr. Metcalfe noted that:

> *Personal liberty is ultimately part of the common good […] we benefit not merely as individuals in having privacy, we benefit as a society: because people do things in their private space, in their private time, and the benefits from that flow on to the society as a whole.*[17]

This, however, does not mean that privacy and the freedom it protects are absolute or inviolable values. On the contrary, as pointed out by S. Gutwirth and P. De Hert:

> *Privacy is relational, contextual and per se a social notion which only acquires substance when it clashes with other private or public interests. The friction, tension areas and conflicts create the need for a careful balancing of the rights and interests that give privacy its meaning and relevance.*[18]

Other legitimate competing interests such as public safety could thus justify limited and proportionate interferences with the right to privacy.

2.1.2. *From privacy to data protection*

Data protection legislations have marked a milestone in the evolution of the protection of privacy.[19] Data protection does not merely concern the "the right to be left alone", but also "informational self-determination" (i.e., the "right to control

[13] Ibid.

[14] Cooley on Torts, 2nd ed.; 1888. p. 29. The expression has been largely echoed after the article of Warren and Brandeis. The right to privacy. Harvard Law Review 1890;4:193.

[15] Many constitutions in Europe explicitly recognize the right of privacy and private communications. These include Belgium (Articles 22, 29), Finland (Section 10), Greece (Articles 9, 9A, 19), Netherlands (Articles 10, 12, 13), Portugal (Articles 26, 34, 35), and Spain (Article 18). See Privacy and human rights 2003, 158, 230, 257, 362, 407, 469, 474 (Electronic Privacy Information Center & Privacy International ed., 2003).

[16] Rouvray A. Repenser le sens du droit à la protection de la vie privée dans la société de surveillance: une urgence démocratique. In: Proceedings of the Juritic seminar on La vidéo surveillance: quel équilibre entre sécurité et protection de la vie privée, Namur, Belgium, 18 January 2008. Simitis. p. 135 Bygrave.

[17] As quoted in House of Commons, Home Affairs Committee. A surveillance society? Fifth report of session 2007–08; 20 May 2008. p. 38.

[18] De Hert P, Gutwirth S. Privacy, data protection and law enforcement. Opacity of the individual and transparency of the power. In: Claes E, Duff A, Gutwirth S, editors. Privacy and the criminal law; 2006.

[19] Rodota S. Data protection as fundamental right. In: Synopsis of the presentation at the international conference re-inventing data protection? Brussels, 12–13 October 2007.

the way others use the information concerning us''),[20] as recognized by a landmark decision of the German Constitutional Court in 1983. Whereas the right to privacy mainly functions negatively in that it ensures the non-interference in private matters of the individual,[18] data protection laws are not prohibitive in substance and intend instead to put the individual in control over his or her own information.[21] As contend S. Gutwirth and P. De Hert, data protection safeguards thus act in this sense as a set of ''transparency tools'', in so far they were enacted ''to channel power, to promote meaningful public accountability, and to provide data subjects with an opportunity to contest inaccurate or abusive record holding practices''.[22]

Data protection laws aim to protect the individual's rights with regard to the processing of his or her personal data. These laws have not been implemented to exclusively protect the right to privacy, but also to prevent interference with an individual's rights from the use of automated systems.[23] The Council of Europe has acknowledged in that sense that:

> *The exercise of the freedom to process information may, under certain conditions, adversely affect the enjoyment of other fundamental rights (for example privacy, non-discrimination, fair trial) or other legitimate personal interests (for example employment, consumer credit)*,[24]

Likewise, Recital 2 of the Data Protection Directive stipulates that ''data processing systems are designed to serve man'', and that they must ''respect their fundamental rights and freedoms''.[25] National laws have followed this approach. For instance, the first article of the French Data Protection Act[26] states ''that Information technology should be at the service of every citizen [...]. It shall not violate human identity, human rights, privacy, or individual or public liberties''.

To that effect, it is worth noting that in the specific field of video surveillance, concerns arise in that ''being seen without seeing'' may influence a person's conduct and activity, and thus his or her freedom. In this regard, the impact of both hidden cameras and their ''visibility'' on the feeling of being watched might lead to ''submissive'' behaviour on the citizen's part.[27] Data protection safeguards are thus meant to also protect, in this specific case, more than the mere right to privacy.

Data protection has thus acquired a broader scope of protection than privacy. Furthermore, where the object of the protection of the right to privacy is clearly the individual's private sphere – an undefined and evolving legal concept – the data protection right focuses on the (il)licit use of personal data.

2.2. *The efficiency of data protection legislation put into question*

The efficiency of data protection legislations has been challenged by recent developments in technology, as described above, and by the pressing need for the protection of competing interests such as public safety; privacy often appears as a hurdle in the way to greater efficiency in the private sector, or greater security in the field of public safety.

Data protection systems are often seen to be struggling to adapt to the new times and to provide adequate safeguards to ensure the protection of fundamental rights against emerging risks. In this sense, several scholars have voiced the opinion that the increasing lack of efficiency of the protection granted by these legislations, more particularly with regard to the difficulties to adequately enforce its provisions, should call for a shift in the approach. For instance, M. Hildebrandt has stressed that ''if we turn back to the fair information principles and think of the unobtrusive and ubiquitous computing technologies that are already embedded in our environment, the principles seem written for another – less complex – age''. She further argues that:

> *If unlimited collection of data is technologically possible and profitable while effective control is an illusion; if the amount of data is such that no person would even have the time to keep track of the collection and storage of her personal data, its purpose and the identity of the data controller, let alone to correct, complete and update her data and/or to erase, rectify, complete or amend her data; if use of data collected for another purpose, or disclosure of data for other purposes is technologically possible and profitable while effective control is an illusion; [...] – if all*

[20] Examples of definitions of privacy in terms of information control are found in AF Westin. Privacy and freedom. New York: Atheneum; 1967; Lusky L. Invasion of privacy: a classification of concepts. Columbia Law Review 1972;72:693, 709; Slane B. Private world: news from the Office of the Privacy Commissioner. April 1996, no. 4.6.

[21] Mayer-Schoenberger V. Generational development of data protection in Europe. In: Agree PE, Rotenberg M, editors. Technology and privacy: the new landscape. MIT Press; 1998.

[22] Op. cit. note 18 ante.

[23] In fact, as pointed out by Bygrave LA in Data protection law: approaching its rationale, logic and limits. Kluwer Law International 2002:37: many European data protection statutes (both past and present) make no explicit reference to the safeguarding of privacy. Of these some refer instead to relative concepts such as the protection of 'personality' or protection of 'personal integrity'.

[24] Council of Europe. Convention for the protection of individuals with regard to automatic processing of personal data, ETS n°108, Strasbourg, 28 September 1981.

[25] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal 23 November 1995;L281:31–50.

[26] Act n°78-17 of 6 January 1978 on data processing, data files and individual liberties (amended by the act of 6 August 2004 relating to the protection of individuals with regard to the processing of personal data).

[27] Giovanni BUTTARELLI. 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.http://www.coe.int/t/e/legal_affairs/legal_cooperation/data_protection/documents/reports_and_studies_by_experts/Y-Report_Buttarelli_2000.asp#TopOfPage; 2000.

this, than we may be fooling ourselves in thinking that such legislation will make much of a difference.[28]

Instead, Hildebrandt advocates for the "building of legal and technological constraints that intelligently interact".[29]

However, before deciding to abandon data protection systems as seems to advocate Hildebrandt, it may be necessary to recall that the concrete application of data protection principles is not evident, and therefore any discussion concerning what the approach of data protection systems requires a prior and periodical debate. Data protection is active and evolving, pragmatic and imaginative, and therefore should be constantly reconsidered.[30] The question is thus whether the reconsideration of the current data protection framework should lead the system to disappear or to adapt to the evolving reality.

3. Facing new challenges: can data protection systems be adapted to (re-)gain efficiency?

New advances in video surveillance technologies give us the opportunity to test the robustness of the system implemented by data protection legislations, in particular of its three core principles: the principle of purpose specification, of proportionality and transparency.

3.1. *The principle of purpose specification in interconnected video surveillance networks*

The principle of finality implies that personal data should be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. The purpose specification principle participates from the principle of forseeability.[31] This means that personal data cannot be processed for purposes beyond the reasonable expectations of the data subject (further processing of personal data can only be slightly but never substantially different from the original processing).[32]

It intends to form closed compartments, isolating data processing pursuing a specific and defined purpose from others, and to prevent abusive linkage of data processing. Such linkages, as the ones foreseen in DYVINE-like systems, amplify the usual risks that data protection legislation tries to minimize, such as function creep or the loss of control by the data subject over the processing of his or her data. The sharing of information presents increased risks and the respect of data protection rules intend to make sure that the benefits of information sharing are delivered. As pointed out by the UK Information Commissioner:

The sharing of personal information [should] be justified on the basis that the benefits – supported by meaningful safeguards – clearly outweigh the risks of negative effects. Where sharing is justified all reasonable steps should be taken to keep any negative effects to a minimum.[33]

3.1.1. *The purpose principle in a context of increased sharing of information*

An increased number of situations require organizations to work together and to share large amount of information. The importance of a clear definition of the lawful sharing of information is illustrated by the difficulties encountered during the recovery phase of the London bombings of 7 July 2005. The UK government noted in the resilience lessons paper that the:

[l]imitation on the initial collection and subsequent sharing of data between the police and humanitarian support agencies hampered the connection of survivors to support services. The concern at the time was that the Data Protection Act might prevent the sharing of personal data without the explicit consent of those concerned. As a result there were delays in information reaching survivors about the support services available.[34]

DYVINE-like systems institutionalize massive sharing of information and thus raise the fundamental question of whether the principle of purpose specification is completely outdated by the advances of the technology, or whether it still plays a valuable role in protecting individuals. If the purpose specification cannot fulfill its original role of limiting the abusive sharing of information, could it be still considered as a valuable tool in protecting individuals' rights in interconnected networks in where there co-exist several processing of different natures?

It cannot be denied that this principle plays a fundamental role in data protection systems in so far as it permits the individualization of every data processing from a legal point of

[28] Hildebrandt M. Profiling and the identity of the European citizen. FIDIS Deliverable D.7.4 Implication of profiling practices on democracy and rule of law. Available online at: http://www.fidis.net/resources/deliverables/profiling/#c1762.

[29] Ibid.

[30] Mallet-Poujol N. Avant-propos. In: Traçage électronique et libertés. Problèmes politiques et sociaux n°925, ed. la Documentation française; June 2006.

[31] See in that sense, Opinion of the General Advocate J. Kokott, 18 July 2007, ECJ Case C-275-06, point 53: "It must therefore, in accordance with the requirement of foreseeability, be formulated with sufficient precision to enable the citizen to adjust his conduct accordingly. The requirement of foreseeability has found particular expression in data protection law in the criterion – expressly mentioned in Article 8(2) of the Charter – of purpose limitation. Pursuant to the specific embodiment of the purpose limitation criterion in Article 6(1) (b) of Directive 95/46, personal data may be collected only for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes."

[32] Bygrave LA. Data protection law: approaching its rationale, logic and limits. Kluwer Law International 2002.

[33] Thomas R, Dr. Walport M. Data sharing review, a consultation paper on the use and sharing of personal information in the public and private sectors; 12 December 2007.

[34] Quotation extracted from HM Government. Data protection and sharing – guidance for emergency planners and responders; February 2007. p. 5.

view. As such the principle remains one of the core elements on which data protection laws should build upon. It is, however, true that safeguards originally implemented in order to prevent abusive linkages of processing are being eroded by, firstly, the fact that it is easier and cheaper each time to connect databases; but also by the evolving perception of the risks implied by this interconnection. A redefinition of the socially acceptable risks stemming from interconnection may be required and thus safeguards better adapted to the new societal context should be devised.

Some initiatives have been promoted in the sense of an increased *a priori* control. For example, Privacy Impact Assessments that allow the data controller to identify and manage privacy risks are already being advocated by the UK Information Commissioner[35] and by the European Data Protection Supervisor within the specific field of RFID technology.[36] In addition, prior checks by data protection authorities of processing that are more sensitive in terms of fundamental rights may also be used to ensure a greater efficiency of the legislation (see Section 3.2 below).

3.2. *The principle of proportionality in the massive collection of images and cross-checking against pre-existing databases*

The principle of proportionality is a common and constant requirement for the assessment of the validity of any behaviour or measure that restricts fundamental rights. Thus, data processing, to be permitted in the face of the right to data protection, must not only be able to achieve the goals foreseen (adequacy test), but also must be strictly necessary (necessity test), and, finally, must provide sufficient benefits for the public interest to compensate for the harm caused to other competing values (proportionality test *stricto sensu*). The more severe the infringement of privacy, the more important the legitimate objective of the measure must be.[37]

The principle of proportionality applies not only to evaluating the purpose of the processing itself, but also to the adequacy of the data collected to that end and the means used to achieve it.[38] The principle has acquired a significant role in the balancing of interests, particularly when it comes to assessing the conformity of intrusive technologies (i.e., biometrics or video surveillance) to data protection safeguards. As indicated by P. Breyer:

> *The positive and the negative effects of the measure on individuals and society as a whole must be balanced against each other. This cannot be achieved by means of general considerations on the interests and rights in question, since it is impossible to establish an absolute order or ranking of interests and rights. Instead, it is necessary to determine how useful the measure will actually be, and what harmful effects it will actually have.*[39]

This assessment is highly variable and depends on the risk stemming from each processing. As recalled by the House of Commons in the UK, proportionality's importance in the context of law enforcement is when the individual lacks choice: public controllers should thus only ''deploy surveillance technology where it is of proven benefit in the fight against crime and where this benefit outweighs any detrimental effect on individual liberty''.[40]

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.[41] In that sense, the integration of video surveillance networks follows a logic of mass surveillance (i.e., they create ''situations in which the privacy of many individuals is affected by wide-ranging or universal schemes''[42]), even though they can be equally utilized for the purpose of targeted surveillance (i.e., that ''involves the use of specific powers created through legislation used against a particular individual or individuals''[43]). Furthermore, the integration of video analytics tools that could require the linkage of video processing to other databases such as, for example, photographic databases of individuals, for the use of face-recognition software, should be strictly in conformity with the proportionality principle. Bystanders do not expect to have their face analysed, nor does it appear proportionate to scan the whole population on a day-to-day basis to identify ''usual'' criminals, or even to check on their activities.

The assessment of the proportionality of these pervasive surveillance systems before their implementation and extensive use appears to be crucial in so far that mass surveillance techniques are ''by their nature light touch and wide impact''.[44] The detrimental effects on individual freedoms are not usually directly felt by the individual on a day-to-day basis. Rather, they raise societal choices of how to balance the interests at stake. Therefore, when accurately applied, the principle of proportionality acts as an *a priori*

[35] Information Commissioner Office. Privacy Impact Assessment handbook and surveillance society conference website. http://www.ico.gov.uk/about_us/news_and_views/current_topics/Surveillance_society_conference.aspx.

[36] European Data Protection Supervisor. Opinion on the communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Radio Frequency Identification (RFID) in Europe: steps towards a policy framework, COM (2007) 96, 20 December 2007.

[37] Liberty. Overlooked: surveillance and personal privacy in modern Britain; October 2007. Available online at: http://www.liberty-human-rights.org.uk/issues/3-privacy/pdfs/liberty-privacy-report.pdf.

[38] See in that sense Dumortier F. La vidéosurveillance sous l'angle de la proportionnalité: premières réflexions au sujet de la loi réglant l'installation et l'utilisation de cameras de surveillance. Revue du Droit des Technologies de l'Information 2007;29:311–50.

[39] Breyer P. Telecommunications data retention and human rights: the compatibility of blanket traffic data retention with the ECHR. European Law Journal May 2005;11(3):365–75.

[40] Op. cit. note 17 ante.

[41] See Spanish Data Protection Authority, Report 486/2006. Uso de camáras para análizar hábitos de consumo.

[42] Liberty. Overlooked: surveillance and personal privacy in modern Britain; October 2007. Available online at: http://www.liberty-human-rights.org.uk/issues/3-privacy/pdfs/liberty-privacy-report.pdf.

[43] Ibid.

[44] Ibid.

guide-rail, which could limit the deployment of disproportionate systems.

This, however, raises the question of *who* should make such assessments of proportionality, and who should decide on what balance of rights should be made. With regard to video surveillance, the UK Privacy Commissioner and other European data protection authorities, such as the Data Protection Authority of the Madrid Region (Spain), have advocated that an obligation to carry out Privacy Impact Assessments should be put upon controllers. This would allow for the identification and management of privacy risks at an early stage. Follow-up assessments can then be made by such organizations to assess whether the sharing of information is having the desired effect, for example in terms of reducing crime or providing a more efficient service to the public.[45]

However, due to the magnitude of the data that can be collected by integrated video surveillance networks, additional safeguards to protect fundamental rights should be installed. Data protection authorities should therefore be involved in the difficult task of evaluating the proportionality of such processing. To that effect, the Data Protection Directive enables Member States of the EU to subject certain processing operations that are likely to present specific risks to the rights and freedoms of data subjects to prior checking (Article 20). Such a move would allow the relevant authorities to define the boundaries within which such processing could operate, based on the application of the principle of proportionality. This would reinforce the role of data protection authorities whose primary mission is, as recalled by the European Data Protection Supervisor, ''to ensure compliance and to promote effective protection. It is only through these concepts that data protection rules and principles can become a reality in practice''.[46]

3.2.1. *Proportionality of the personal data to be collected*

Another question arises with regard to the amount of data that should be collected. According to the data minimization principle, the collection of personal data should be limited to what is necessary to achieve the purpose for which the data are gathered and further processed. However, video analytics and the use of pre-configurable alarms despite requiring the processing of vast amount of data may limit at least the amount of information to be displayed to the operator to relevant events. The operator would thus not have to watch endless hours of footage, but only the images displayed by the system when a suspicious event or behaviour is detected. The impact of video surveillance systems on fundamental rights may thus be reduced.

This solution, which is also advocated by the UK Royal Academy of Engineering is, however, a double-edged sword. Video analytics are offering powerful tools in terms of event detection, ranging from the mere detection of a fire or traffic jam to the detection of ''abnormal'' behaviours, or of individual tracking, which are far more problematical in terms of fundamental rights. Such event detection would imply the further scanning of millions of individuals without prior notice or expectation. As stressed by the UK Royal Academy of Engineering:

> *The development of surveillance systems has changed what can be gleaned from observations of individuals. As well as recording the presence of and recognising individuals, surveillance systems now offer the possibility of evaluating and making inferences about a person's actions and intentions, drawing on stereotypes and profiling methods.*[47]

The proportionality of intelligent video tools such as video analytics and alarms should therefore be assessed on a case-by-case basis.

3.3. *The principle of transparency in increasingly opaque systems*

3.3.1. *Transparency put at risk*

Finally, the principle of transparency concerns the empowerment of data subjects to exercise control over the processing of personal data relating to them. This principle follows from one of the main objectives of data protection legislation, namely to make the data subject an active participant in his or her own protection. This principle compels controllers to provide the data subjects with sufficient information on the processing being carried out. This information will empower the data subjects to exercise their personal scrutiny upon the processing, through exercising their right of access, modification and deletion. Much data protection legislation seeks to ensure that an individual is able to participate in, and have a measure of influence over, the processing of data concerning him or her by other individuals and organizations.

This principle has, according to some scholars, become totally inefficient in the interconnected society. The objective of data protection systems to render the processing transparent to the data subject is endangered by the increased opacity of private and public institutions. This has led to a state of affairs, denounced by scholars, in which:

> *Individuals become each time more transparent and heteronomous in the construction of their personality, whereas private and public institutions become each time more opaque and invest in ''autonomy'' and ''automatisms'' in the construction of the mode of intelligibility, interpretation and reaction towards individuals.*[48]

This is clearly the case in the field of video surveillance, and particularly with DYVINE-like systems, because the data

[45] Information Commissioners Office. Privacy Impact Assessment handbook and surveillance society conference website. http://www.ico.gov.uk/about_us/news_and_views/current_topics/Surveillance_society_conference.aspx.

[46] Hustinx P. The role of data protection authorities. In: Speech at the international conference on re-inventing data protection, Brussels, 12–13 October 2007. Available online at: http://edps.europa.eu/EDPSWEB/edps/lang/en/pid/23.

[47] The Royal Academy of Engineering. Dilemmas of privacy and surveillance. Challenges of technical changes; March 2007. Available online at: http://www.raeng.org.uk/policy/reports/pdf/dilemmas_of_privacy_and_surveillance_report.pdf.

[48] Gutwirth S, De Hert P. Privacy and data protection in a democratic state. FIDIS Deliverable D.7.4 Implication of profiling practices on democracy and rule of law. Available online at: http://www.fidis.net/resources/deliverables/profiling/#c1762.

subject is not only forced to accept being monitored on a permanent basis (which threatens "to destroy the 'public privacy' previously enjoyed by anonymous citizens in a public space"[49]) but also to have his or her images further processed and shared with third parties without prior notice. As pointed out by the UK Royal Academy of Engineering:

> *This limits the extent of the freedom of citizens to go about their lawful business without being observed and monitored. It also extends the capacity for agencies and institutions to subject a section of the public realm to surveillance for their own purposes.*[50]

Further evidence of this growing opacity may be found in the recent developments of video analytics as it facilitates the use of automatic individual decisions. Up to now, Article 15 of the Data Protection Directive has provided certain protections against such decisions and empowers data subjects to object to it. This right applies to situations in which the decision is solely based on automated decision processing and is intended to evaluate certain personal aspects of the person who is targeted by the decision. According to L.A. Bygrave, the Directive will assist in situations "in which a person fails to actively exercise influence on the outcome of a particular decision-making process".[51] Article 15 of the Directive, however, does not compel the controller to review the criterion used for the processing, nor is it applicable to the law enforcement field, where video analytics is mainly applied.

Such concerns raise the possibility of a society in which the citizen is under permanent control. If this were the case, the obligation required by data protection laws to inform individuals through an information notice seems barely sufficient to really empower the data subject to recover the control over the processing of his or her images, and to exercise, for instance, his or her right of access, or to object to the processing of his or her data.

3.3.2. *Ensuring transparency in opaque systems*

To remedy the lack of transparency of video surveillance systems, a "community safety channel" showing images from surveillance cameras has been made available to residents of Shoreditch, East London. Any suspicious behaviour seen on the channel can be immediately reported to the police via the television set.[52] This system is presented by the UK Royal Academy of Engineers as a means to convert the "watched" into "watchers".[53] According to the Academy:

> *Public webcam images need not be private, but could be available to all who would use public spaces chosen for surveillance. […] Natural forms of surveillance are preferred by the public, and therefore an effective surveillance system needs to be more like the natural surveillance created when an area is monitored by community members, or known figures such as local police officers.*[54]

The Academy identifies several benefits of this programme, such as the enjoyment of "peace of mind" offered by the presence of video surveillance cameras: "if one could see for oneself that there were no worrying activities – or if there were, one could avoid and report them". Other benefits include the permitting of "reciprocal checks on the social behaviour of other drivers", without the discomfort often brought about by surveillance because "the sense of paranoia that a surveillance camera can create in even a perfectly law-abiding citizen might be mitigated if one knew for certain exactly what it could see".[55]

It is, however, difficult to see how this solution could provide a greater transparency of video surveillance systems. On the contrary, it seems that it would definitively annihilate the relative anonymity bystanders may enjoy in big cities, and is reminiscent of previous form of social control carried out by the community itself. This could thus undermine the few remaining sphere of privacy in public areas, and, in the worst case, could give way to new forms of "voyeurism".

Other measures that further encourage transparency should be envisioned. These measures must not only empower citizens to play a significant role in the processing of their data but, must also ensure that the controller is accountable. S. Simitis for instance believes that "only the greatest possible transparency under the rule of law […] ensures that the danger of slipping into a surveillance state can be countered".[56] This is in part because trust, intimately linked with transparency, is essential to a democratic society. As argued by Liberty:

> *Where surveillance put[s] the privacy of an individual at risk, the broader relationship between the citizen and state is also at stake [insofar as] there would be a society where the dignity of the individual has been compromised; intimacy between people, confidence between people and trust in big institutions, whether it is the Health Service or the Government, would be lost.*[57]

Other forms of *a priori* control over the processing, such as prior checks conducted by data protection authorities (see Section 3.1 above), may form a first step in making them more transparent and thus creating trust. However, trust can

[49] The Royal Academy of Engineering. Dilemmas of privacy and surveillance. Challenges of technical changes; March 2007. Available online at: http://www.raeng.org.uk/policy/reports/pdf/dilemmas_of_privacy_and_surveillance_report.pdf.

[50] Ibid.

[51] Bygrave LA. Minding the machine: Article 15 of the EC data protection directive and automated profiling. Computer Law & Security Report 2001;17:17–24.

[52] Weaver M. Residents given access to live CCTV footage. The Guardian Wednesday January 11, 2006.

[53] The Royal Academy of Engineering. Dilemmas of privacy and surveillance. Challenges of technical changes; March 2007. Available online at: http://www.raeng.org.uk/policy/reports/pdf/dilemmas_of_privacy_and_surveillance_report.pdf.

[54] Ibid.

[55] Ibid.

[56] As quoted by the Foundation for Information Policy Research. "UK Information Commissioner study project: privacy and law enforcement, Paper n°4: the legal framework, an analysis of the constitutional European approach to issues of data protection and law enforcement"; February 2004. p. 59.

[57] Liberty. Overlooked: surveillance and personal privacy in modern Britain; October 2007. Available online at: http://www.liberty-human-rights.org.uk/issues/3-privacy/pdfs/liberty-privacy-report.pdf.

only be achieved by ensuring that the ''watchers are watched'', e.g. by empowering trustworthy authorities to conduct investigations and to report on the findings. Data protection authorities are generally trusted by the public, and have proved to have sufficient independence and knowledge to carry out this role. In that sense, the CNIL, the French data protection authority, has recently pointed out that ''the question of the control of a video surveillance system by an independent authority, in other words, ''the control of the controllers'', from now on forms a fundamental requirement in modern democratic societies, that it is necessary to ground the legitimacy of developing surveillance systems by ensuring that the rights and liberties of individuals are taken into account and that safeguards are implemented.''[58]

4. Conclusion: are new safeguards needed?

The new generation of video surveillance networks raises significant challenges in terms of data protection. These challenges are not, however, only restricted to this specific field but seem to characterize most of the new technologies being recently developed. Some of the most problematic of these issues are identified when considering the principles of purpose specification, proportionality and transparency. In fact, as mentioned in this paper, it is now much easier and cheaper to link databases or systems in order to provide controllers with increased amount of data and to retrieve relevant information about one individual or situation thanks to sophisticated data mining techniques. The interest in such systems is thus growing, challenging by the same token on the one hand the principle of finality that ensures 'closed compartments' and facilitates the control over the processing, and on the other hand the principle of proportionality in the face of systems based on massive processing of personal data. Both phenomena give way to a transition from static and closed systems to dynamic and preventive systems, fundamentally opaque to data subjects. Individuals are thus not aware any more of the processing undergone by their personal data, weakening one of the pillars of data protection legislations.

These difficulties should however be understood as being part of a larger process of the ''unrelenting re-invention of privacy''.[59] The concrete application of data protection principles is not evident and it requires a prior and periodical debate which cannot be eluded.[60] Data protection legislations were in first place thought to face a change in the technological paradigm, and have evolved hand in hand with the technology they were supposed to regulate.[61] It may thus be time to make a further step in the definition of data protection principles in order to adapt them to the new technological paradigm. Several options are possible to achieve this objective.

Although some scholars have considered that data protection legislation is unable to achieve its aims and to bring any substantial benefit in the protection of individuals in front of the new technological paradigm, it is arguable that a better implementation of the broad provisions of the Data Protection Directive may constitute a first step towards improving the efficiency of the system. In that sense, the European Data Protection Supervisor has noted that ''in the short term, specific actions are needed to ensure full implementation of the Directive. That accomplished, and in the longer term, I see some important issues need to be addressed''.[62] This last statement refers more particularly to the issues linked to the interoperability of systems.

The adaptation of data protection safeguards should however not only take into account the technological shift but also the one in the public's perception of the associated risks of surveillance. This shift is particularly visible in the field of video surveillance: whereas ten years ago video surveillance was mainly identified with a new form of social control,[63] today's television advertisements promote personal video camera packages to monitor one's own premises or one's babies.

This shift, however, should not let one forget that:

> *Taking privacy seriously implies the making of normative choices: some intrusions are just too threatening for the fundamentals of the democratic constitutional state to be accepted even under a stringent regime of accountability. Other intrusions, however, can be felt to be acceptable and necessary in the light of other sometimes predominating interests.*[64]

The challenge may thus consist more in a ''re-thinking'' of the values to be protected under the cover of data protection legislation in an interconnected society, than in building a whole new framework of safeguards.

By the same token, the instruments of protection should be adapted. A specific focus should be put on the need for a greater involvement of a) controllers in the identification and management of privacy risks through, e.g., the use of tools such as Privacy Impact Assessments, and of b)

[58] CNIL. Press release, Vidéosurveillance: la CNIL demande un contrôle independent; 8 April 2008. Available online at: http://www.cnil.fr/index.php?id=2413.

[59] Rodota S. Data protection as fundamental right. In: Synopsis of the presentation at the international conference re-inventing data protection? Brussels, 12–13 October 2007.

[60] Mallet-Poujol N. Avant-propos. In: Traçage électronique et libertés. Problèmes politiques et sociaux n°925, ed. la Documentation française; June 2006.

[61] For the analysis of data protection legislations'evolution since 1970, see Mayer-Schönberg V. Generational development of data protection in Europe. In: Agree PE, Rotenberg M, editors. Technology and privacy: the new landscape. MIT Press; 1998.

[62] European Data Protection Supervisor. Press release, Data protection directive: EDPS wants full implementation before considering changes to the framework; 25 July 2007.

[63] See for instance Vitalis A. Être vu sans jamais voir: le regard omniprésent de la vidéosurveillance. Le Monde Diplomatique March 1998.

[64] Gutwirth S, De Hert P. Privacy and data protection in a democratic state. FIDIS Deliverable D.7.4 Implication of profiling practices on democracy and rule of law. Available online at: http://www.fidis.net/resources/deliverables/profiling/#c1762.

independent authorities such as data protection authorities in the *a priori* control of systems highly sensitive in terms of fundamental rights. However, the more pressing need lies with the redefinition of transparency instruments able to ensure a fair balance between 'watchers' and 'watched'. To that effect, new mechanisms should be devised that could both guarantee the accountability of controllers and generate sufficient trust for individuals.

Fanny Coudert (*fanny.coudert@law.kuleuven.be*) *Interdisciplinary Center for Law & ICT (ICRI), Katholieke Universiteit Leuven – IBBT, Belgium.*