Sorting Out Smart Surveillance

ABSTRACT

Surveillance is becoming ubiquitous in our society. We can also see the emergence of "smart" surveillance technologies and the assemblages (or combinations) of such technologies, supposedly to combat crime and terrorism, but in fact used for a variety of purposes, many of which are intrusive upon the privacy of law-abiding citizens. Following the dark days of 9/11, security and surveillance became paramount. More recently, in Europe, there has been a policy commitment to restore privacy to centre stage. This paper examines the legal tools available to ensure that privacy and personal data protection are respected in attempts to ensure the security of our society, and finds that improvements are needed in our legal and regulatory framework if privacy is indeed to be respected by law enforcement authorities and intelligence agencies. It then goes on to argue that privacy impact assessments should be used to sort out the necessity and proportionality of security and surveillance programmes and policies vis-à-vis privacy.

KEY WORDS

Smart surveillance, security, privacy, transborder data flows, privacy impact assessments

1 INTRODUCTION

The prevalence of surveillance in our society grows by leaps and bounds. Scarcely, a day goes by without a story in the media about some new surveillance activity that has just come to light. While the UK accounts for one quarter of all the CCTV cameras in the world and while people in London are captured by CCTV cameras up to 300 times a day, the diffusion of surveillance systems and technologies to other parts of Europe (and elsewhere, of course) gathers momentum. Surveillance today is not just manifested by surveillance cameras. Many other technologies such as radio frequency identification (RFID) tags and biometrics are being deployed. Roger Clarke coined the term "dataveillance" more than two decades ago in reference to the phenomenon of data being used to monitor and surveil citizens.[1] Furthermore, surveillance systems and technologies are no longer discrete. They are converging and being combined – the phrase surveillance assemblage is gaining currency to describe this activity[2] – to create even more powerful networked surveillance systems.

Surveillance systems and technologies are no longer confined to law enforcement authorities, intelligence agencies and the military – modern information technology has manifested surveillance as an everyday phenomenon. Surveillance technology monitors traffic on our roads and passengers on the Underground; government services use surveillance technology to check who is really entitled to social services; employers monitor employee keystrokes, e-mails, and phone calls; and Internet service providers inspect their customers' data traffic to target them with behavioural or personalised advertising. Thus, surveillance is not only bound to the notion of increasing security, but several surveillance practices and technologies have become commonplace in our daily activities, and they are, somehow, "banalised" by a routine use that scarcely takes into account the principles of necessity, purpose limitation and proportionality.[3] Some surveillance applications enjoy citizen support, while others are viewed as oppressive and spark resentment. In many cases, citizens have just

[1] Clarke, R., 'Information Technology and Dataveillance', *Communications of the ACM*, Vol. 31, No. 5, May 1988, pp. 498-512.

[2] The authors note contemporary activities in bringing surveillance systems together, whether for control, governance, security, profit or entertainment. Haggerty, K.D., and R.V. Ericson, 'The Surveillant Assemblage', *British Journal of Sociology*, Vol. 51, No. 4, 2000, pp. 605-22.

[3] By "banalisation", we mean making surveillance commonplace (banal), so that it becomes something we as a society do not care about. Banalised forms of surveillance enter our daily life without notice, so that they become a common part of our socio-political and economic relations, so that we become acclimatised or accustomed to surveillance in general, even if we are not always aware of the deployment of particularly intrusive forms of surveillance. The term is used to indicate the increasing pervasiveness of surveillance, right down to the level of the individual (parents monitoring their children's whereabouts or taking pictures of what their neighbours are doing). Some examples could be the capture, storage and processing of fingerprints of frequent costumers of sporting complexes, in order to ease their access to and use of facilities, or the processing of large amounts of personal data in social networks for running "small entertaining applications". In the field of law enforcement, it could be represented by the disproportionate retention of DNA in cases involving petty crimes. This idea partially resonates with the concepts of "soft surveillance", developed in Marx, G.T., "Soft Surveillance. The Growth of Mandatory Volunteerism in Collecting Personal Information", in T. Monahan (ed.), *Surveillance and Security. Technological Politics and Power in Everyday Life*, Routledge, New York, 2006, pp. 37-56. For more on banalisation, see Bellanova, R., P. De Hert, and S. Gutwirth, "Variations sur le thème de la banalisation de la surveillance", *Mouvements*, No. 62, 2010.

accepted what they cannot change even though they might have uncomfortable feelings about it (a phenomenon known as cognitive dissonance[4]).

This paper examines the recent developments in surveillance technologies and argues that today's "smart surveillance" approaches require explicit privacy assessments in order to sort out the necessity and proportionality of surveillance programmes and policies vis-à-vis privacy. After the dark days following 9/11 when security and surveillance became paramount, Europe has more recently seen a shift in the socio-political context towards a policy commitment that restores privacy to centre stage. We thus examine the legal tools available to ensure that privacy and personal data protection are respected in attempts to ensure the security and safety of our society, and find that improvements are needed in our legal and regulatory framework if privacy is indeed to be respected by law enforcement authorities and intelligence agencies.

2 SURVEILLANCE

First, we consider what surveillance means and how social scientists have viewed it. The term "surveillance" literally refers to a "close watch kept over someone or something".[5] In contemporary social and political sciences, surveillance refers to "the process of watching, monitoring, recording, and processing the behaviour of people, objects and events in order to govern activity".[6] Surveillance is one of the most challenging political questions of our age. At the centre, there is the issue of how surveillance should be conceptualised. One of the most famous answers was Michel Foucault's disciplinary model, exemplified by the *panopticon*. According to Jeremy Bentham, the *panopticon* or "the inspection-house" was a principle of construction "applicable to any sort of establishment, in which persons of any description are to be kept under inspection and in particular to penitentiary-houses, prisons, houses of industry, work-houses, poor-houses, manufactures, mad-houses, lazarettos, hospitals,

[4] Festinger, Leon, *A theory of cognitive dissonance*, Stanford University Press, Stanford, CA, 1957.

[5] As defined in the *Merriam-Webster Online Dictionary*. http://www.merriam-webster.com/dictionary/surveillance. The English word originates from the French verb "surveiller", which, literally translated, means "to watch over".

[6] Jenness, V., D.A. Smith and J. Stepan-Norris, "Taking a Look at Surveillance Studies", *Contemporary Sociology: A Journal of Reviews*, Vol. 36, No. 2, March 2007, pp. vii-viii.

and schools"[7]. The architectural model was a circular building in which a central observatory makes it possible to inspect all the activities at the perimeter. In the panopticon, those who are in the periphery cannot see their observers, and they can only assume that someone may be watching over them all of the time.

Michel Foucault described "Panopticism" as a system which aims "to induce in the inmate a state of conscious and permanent visibility that assures the automatic functioning of power".[8] According to Foucault, the panopticon was the model of the technology of power of the nineteenth century, of the apparatus through which people were replaced by "a collection of isolated individualities", easier to be controlled and disciplined. In Foucault's model, surveillance is connected with both observation and control. Its goal is the production of knowledge (observation and the birth of criminology as prison is described in *Discipline and Punish*) and of power (the control or, in the nineteenth century, the "disciplination" of behaviour).

Some scholars have raised objections to the theoretical vision implied by panopticism. English sociologist and former president of the London School of Economics, Anthony Giddens, argues that Foucault's paradigm tends to overestimate supervision and underestimate surveillance and collection of information and data.[9] Bauman has argued that panopticism would be inappropriate to describe mechanisms of societal control in post-modern societies, based as they are on "liquid identities, mass consumption and enjoyment imperatives".[10]

In the twentieth century, new ways of effective steering of behaviour in the open social field developed. Taking a cue from Foucault, and particularly his work on "bio-power"[11], this different and more actual power diagram was further explained by, among others, Stanley Cohen, Gilles Deleuze and Gary T. Marx. The latter two claim

[7] This is a quote from the full title of Bentham, Jeremy, *Panopticon*, 1787, a copy of which can be found at http://cartome.org/panopticon2.htm.

[8] Foucault, M., *Discipline and Punish: The Birth of the Prison*, Vintage Books, New York, 1995, p. 195.

[9] Giddens, A., "Surveillance and the capitalist state", in *A Contemporary Critique of Historical Materialism*, Macmillan, London, 1981, pp. 169-176.

[10] Bauman, Z., *Globalization: The Human Consequences*, Polity Press, Cambridge, 1998.

[11] Foucault, M., *Histoire de la sexualité 1. La volonté de savoir*, Gallimard, Paris, 1976; Foucault, M., *Sécurité, territoire, population. Cours au Collège de France. 1977-78*, Gallimard/Seuil, Paris, 1997.

we live in a “maximum security society” or in a *société de contrôle* which relies on a refined technological framework to influence, even “program” the daily lives of citizens[12]. The main point is the expansion of control outside the “panoptical buildings” in the open, in real time, automatically, on a larger scale, without the loss of the disciplinary institutions as a “core”. Alongside the “exclusionary mode of social control”, with its disciplinary incarcerations, isolation and stigmatization, Cohen also sees the development of an “inclusionary mode of social control”.[13] Gary Marx has pointed out that such evolution towards a maximum security society could only be realised through the capacities of information and communication technologies. Other scholars have also suggested that the introduction of new, smart technologies have allowed a shift from discipline to control through differentiation.[14] Thus, the conceptualisation of surveillance has expanded from systems of keeping watch over prisoners and other unfortunates to pervasive systems employing a wide range of technologies for manipulating social behaviour and, as a consequence, impacting social values, including especially privacy.

3 UBIQUITOUS SURVEILLANCE

Living in a surveillance society means more than just being under the watchful eyes of CCTV cameras: Today, every transaction and almost every move of the citizens is likely to create a digital record.[15] The so-called Internet of Things and ambient intelligence are already developing fast through the use of RFID tags. Digitalised characteristics of the human body (biometrics) are increasingly used. This leads to an increasingly connected world in which public security organisations may have access

[12] Marx, G.T., “La société de sécurité maximale”, *Déviance et société*, 1988, pp. 147-166. See also Deleuze G., “Contrôle et devenir” and “Post-scriptum sur les sociétés de contrôle” in *Pourparlers. 1972-1990*, Minuit, Paris, 1990, pp. 240-247. English translation available at: http://www.watsoninstitute.org/infopeace/vy2k/deleuze-societies.cfm

[13] Cohen, S., “The punitive city: notes on the dispersal of social control”, *Contemporary crises*, 1979, pp. 339-63; Cohen, S., *Visions of social control: Crime punishment and classification*, Polity Press, Cambridge, 1985.

[14] Lyon, D. (ed.), *Surveillance as Social Sorting: Privacy, risk and digital discrimination*, Routledge, London, 2003.

[15] Gutwirth, S., *Privacy and the information age*, Rowman & Littlefield, Lanham MD, 2002.

to vast amounts of potentially useful information, which can directly affect the life of the persons concerned.[16]

In their recent report on surveillance, the UK House of Lords said that surveillance continues to exert a powerful influence over the relationship between individuals and the state, and between individuals themselves.[17] While the population seems in general to be content with the massive colonisation of the streets by CCTV[18], mass surveillance has the potential to erode privacy. As privacy is an essential pre-requisite to the exercise of individual freedom, its erosion weakens the constitutional foundations on which democracy and good governance have traditionally been based.[19]

A strong indication of the concerns raised by surveillance came recently on the occasion of the 31st annual meeting of the International Conference of Privacy and Data Protection Commissioners held in Madrid in November 2009. More than 80 civil society organisations and about the same number of individual privacy experts joined together to issue a declaration on Global Privacy Standards for a Global World.[20] Their declaration noted “the dramatic expansion of secret and unaccountable surveillance, as well as the growing collaboration between governments and vendors of surveillance technology that establish new forms of social control” and warned “that privacy law and privacy institutions have failed to take full account of new surveillance practices, including behavioural targeting, databases of DNA and other

[16] European Data Protection Supervisor (EDPS), Opinion on the Communication from the Commission to the European Parliament and the Council on an Area of freedom, security and justice serving the citizen, Brussels, 10 July 2009.
http://www.edps.europa.eu/EDPSWEB/edps/Home/Consultation/OpinionsC/OC2009.

[17] House of Lords Select Committee on the Constitution, *Surveillance: Citizens and the State*, Vol. I: Report, The Stationery Office Limited, London, 6 Feb 2009, p. 5.
http://www.parliament.the-stationery-office.com/pa/ld200809/ldselect/ldconst/18/1802.htm.

[18] Lyon, D., *Surveillance Studies: An Overview*, Polity Press, Cambridge, 2007, p. 39.

[19] House of Lords, op. cit., p. 10. The close relationship between privacy and freedom has featured in many scholarly texts, but the classic is that of Westin. He defined privacy as “the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.” He goes on to say that “a balance that ensures strong citadels of individual and group privacy and limits both disclosure and surveillance is a prerequisite for liberal democratic societies”. Westin, Alan F., *Privacy and Freedom*, Atheneum, New York, 1967, p. 7, p. 24. Privacy, as manifested in the secret ballot, is at the heart of democracy, but as Westin and others have argued it is not an absolute right and must be balanced against other values.

[20] http://thepublicvoice.org/madrid-declaration. Among the civil society organisations were the Electronic Frontier Foundation, the Electronic Privacy Information Center and Privacy International. Among the experts were Colin Bennett, Roger Clarke, David Flaherty, Joel Reidenberg and Marc Rotenberg.

biometric identifiers, the fusion of data between the public and private sectors, and the particular risks to vulnerable groups, including children, migrants, and minorities". The declaration issued a "Call for a moratorium on the development or implementation of new systems of mass surveillance, including facial recognition, whole body imaging, biometric identifiers, and embedded RFID tags, subject to a full and transparent evaluation by independent authorities and democratic debate".

The routine surveillance of citizens that pervades society today has raised concerns of individuals, civil society organisations, the media and policy-makers.[21] Local authorities in the UK routinely use surveillance to spy on residents for all sorts of perceived offences, including littering, letting dogs foul the pavement and checking whether citizens live in school catchment areas.[22] This kind of surveillance is not only unnecessary because it does not reduce crime but also counterproductive because it limits freedom.[23] While some forms of surveillance do enjoy public support, others do not. A mechanism is needed to rein in surveillance to the critical parts – where it safeguards society and its values – and to ensure respect for privacy and protection of personal data.

4 SMART SURVEILLANCE TECHNOLOGIES

[21] Athow, D., "Tories Promise To Slash Surveillance State Programme", ITProPortal, 17 Sept 2009. http://www.itproportal.com/portal/news/article/2009/9/17/tories-promise-slash-surveillance-state-programme.

[22] A recent report of the Interception of Communications Commissioner, compiled by Sir Paul Kennedy, has stated that one in every 78 adults in UK is under surveillance and nearly 1,400 requests are made by government agencies every day to snoop on the public. Athow, D., "Personal Privacy Threatened By Snooping Councils", ItProPortal, 10 August, 2009. http://www.itproportal.com/portal/news/article/2009/8/10/personal-privacy-threatened-snooping-council.

[23] There has been a lot of debate about the effectiveness of CCTV. A UK Home Office study found that "the best current evidence suggests CCTV reduces crime to a small degree. CCTV is most effective in reducing vehicle crime in car parks, but it had little or no effect on crime in public transport and city centre settings". Welsh, Brandon C., and David P. Farrington, *Crime prevention effects of closed circuit television: a systematic review*, Home Office Research, Development and Statistics Directorate, August 2002. A second study for the Home Office three years later concluded that "Assessed on the evidence presented in this report, CCTV cannot be deemed a success. It has cost a lot of money and it has not produced the anticipated benefits." It did say, however, that CCTV "has potential, if properly managed… [but] ill-conceived solutions are unlikely to work no matter what the investment." Gill, Martin, and Angela Spriggs, *Assessing the impact of CCTV*, Home Office Reserch, Development and Statistics Directorate, Feb 2005, pp. 120-121. While CCTV may not reduce crime, it does have the merit of recording crime the images of which may be helpful in apprehending those who have committed them.

In this section, we take a closer look at emerging surveillance technologies that have the power to make significant impacts on social behaviour and on our privacy. We see three major technical trends that will significantly change the face of surveillance: the emergence of *new image analysis algorithms* in CCTV; the inclusion of *new sensor systems* that go beyond visual surveillance; and *new data integration capabilities* that combine traditional surveillance with advanced profiling and data mining techniques. At the same time, these technical trends fuel two novel *social* trends that significantly affect traditional surveillance practices: *self-surveillance*[24] and *self-exposure*, i.e., the act of monitoring and recording one's own actions in order to gain a better understanding about oneself, and the act of (digitally) sharing one's thoughts and actions with the public at large. We will briefly discuss each of those trends in turn.

Firstly, advances in imaging algorithms facilitate the *automated operation* of CCTV networks, freeing CCTV operators from having to manually monitor video footage and thus greatly expanding system coverage. Computerised systems for automated number plate recognition, face recognition, gait recognition and complex activity recognition can continuously scan hundreds of video streams and direct the attention of human operators only to critical events. Alternatively, detected non-critical events can also be logged into a database and later correlated with other digital information (cf. *data integration* below).

Secondly, the use of novel and improved sensors such as infrared and microwave sensing, infrastructure sensing (e.g., smart power meters), chemical sniffing, rapid DNA analysis and neuro-imaging (brain wave scanning) greatly expands the *type of data* that surveillance systems are capable of recording. Instantaneous genetic testing will greatly expand the reach of genetic databases, while chemical sniffing, infrared scanning and portable brain wave scanners can complement CCTV footage with additional information. Medical sensors installed at home (e.g., smart toilets), as well as fine-grained and real-time infrastructural sensing for utilities such as power, water and gas, will provide the basis for advanced data mining applications that can infer occupancy, movements and even individual activities inside buildings.

[24] The term self-surveillance is typically used in a slightly different context in the existing literature. See, e.g., Vaz, P., and F. Bruno, "Types of Self-Surveillance: from abnormality to individuals 'at risk'", *Surveillance and Society*, Vol.1, Issue 3, 2003, pp. 272-291.

Last but not least, the growing *digitalisation of everyday life* furthers the creation of comprehensive profiles across all aspects of one's daily routines.[25] Digital rights management systems are tracking personal media consumption (audio, video, TV, games), while RFID tags facilitate real-world activity tracking (e.g., through toll gates, public transport records, event attendance). Health records are being not only increasingly digitised, but also often outsourced to commercial third party providers (e.g., Google Health[26] or Microsoft's HealthVault[27]) and thus stored "in the cloud". And national and international travel is increasingly tracked in large national databases that combine multiple sources (payment, travel agencies, transportation companies, national registers).

The following tables identify some of the smart surveillance technologies that are likely to emerge over the next decade.

Table 1: New image analysis algorithms (smart CCTV)

ANPR – Automated Number Plate Recognition	The identification of number plates from CCTV footage has long since been perfected. Many systems are already in use, most notably on British motorways and for implementing the London congestion charge. Once this information is recorded with time and place, it can be correlated with other databases (see Table 3 below).
Activity recognition	IBM's S3-R1 system (Smart Surveillance System Release 1) can analyse the behaviour of people captured on video, in real time.[28] This allows for both alerts and for indexing of video footage. Video analysis moves through three stages: object detection, object tracking and object classification. Object classification will eventually allow not only a differentiation between humans and, say, cars, but also between different behavioural classes (e.g.,

[25] Hildebrandt, M., and S. Gutwirth (eds.), *Profiling the European citizen, Cross-disciplinary perspectives*, Springer, Dordrecht, 2008.
[26] See www.google.com/health/
[27] See www.healthvault.com
[28] Hampapur, A., L. Brown, J. Connell, A. Ekin, N. Haas, M. Lu, H. Merkl and S. Pankanti, "Smart Video Surveillance", *IEEE Signal Processing Magazine*, March 2005, pp. 38-51. http://ieeexplore.ieee.org/xpl/tocresult.jsp?isYear=2005&isnumber=30488&Submit32=View+Contents

	"drunken drivers", "suspicious humans"), thus implicitly performing *activity prediction*: members of the "drunken drivers" class are expected to cause an accident, while members of the "suspicious humans" class who are found in a parking lot might soon try to steal a car.
Facial recognition	Face recognition is still a hard problem and currently only works well in ideal conditions. However, when combined with additional sensors and information sources, more reliable identification may be possible. Famous early video-based face recognition deployments include the Super Bowl XXXV in 2001[29], as well as the BSI deployment in Mainz main station in 2007[30]. Such technologies are also being deployed at airports.[31]
Gait-based identification	Identifying individuals by gait has the advantage of working even with low-quality video footage. As part of the HumanID Gait Challenge Problem[32], the research community has been testing several algorithmic approaches since 2002, though no commercial systems exist yet.

Table 2: New sensors (beyond CCTV)

Brain wave scanning / neuro-imaging	With the recent advances in neuro-imagery and brain scanning, criminologists are already discussing "brain privacy" issues.[33] There is active work on making neuro-imaging equipment portable, e.g., by using lasers instead of the huge magnets typically needed to detect the magnetic signals inside the brain.[34] Another alternative, in particular for use in the criminal system, might be

[29] Rutherford, E., "Facial-recognition tech has people pegged", CNN.com, 17 July 2001. http://archives.cnn.com/2001/TECH/ptech/07/17/face.time.idg/.

[30] Weimer, U., "Augen des Gesetzes", *Die Zeit*, Issue 5, 25 Jan 2007. http://www.zeit.de/2007/05/T-Biometrie.

[31] Scott, J., "Heathrow rolling out facial recognition tech", ITPro, 30 Nov 2009. http://www.itpro.co.uk/618298/heathrow-rolling-out-facial-recognition-tech.

[32] Phillips, P.J., S. Sarkar, I. Robledo, P. Grother and K.W. Bowyer, "Baseline Algorithm and Performance for Gait Based Human ID Challenge Problem", Proceedings of the International Conference on Pattern Recognition, 2002, pp. I:385-8. http://marathon.csee.usf.edu/GaitBaseline.

[33] Kerr, I., M. Binnie and C. Aoki, "Tessling on My Brain: The Future of Lie Detection and Brain Privacy in the Criminal Justice System", *Canadian Journal of Criminology and Criminal Justice*, Vol. 50, No. 3, June 2008, pp. 367-87. http://iankerr.ca/images/stories/tessling_on_my_brain.pdf.

[34] See http://neurophilosophy.wordpress.com/2006/09/06/hi-res-cheap-portable-mri/

	the implantation of a communication chip to interface a remote reading device with individual sensors inside the body.[35]
Infrared non-contact temperature measurements	With recent concerns surrounding flu pandemics, remote infrared non-contact scanning has received increased attention for securing, e.g., airports. Companies such as Fluke, Raytek and IRCON offer a range of products for airports. Infrared imaging has a long tradition in privacy circles, in particular, for detecting heat sources in private homes (often indicating marijuana plantations).
Power meters and other infrastructure sensing	Research in improving energy awareness has seen large deployments of smart meters in private homes, which can accurately measure individual power use and send such data to a central server. Such data may equally reveal huge energy consumption such as infrared lamps used in growing marijuana plants.[36] Recent research indicates that a smart meter might also be able to identify individual devices and their on-off state.[37] Similarly, a single pressure meter installed in a house's water flow can be used to detect individual appliances and faucets being operated.[38]
Chemical sniffing	Similar to drug dogs, devices are being developed that measure the presence of certain chemicals in the air.
Portable microwave scanner	Microwave scanners allow the detection of concealed items, such as metal, plastic, ceramic, carbon fibre and even liquid explosives. Several airports have already installed full body scanners. These deployments have been met with strong criticism, as they

[35] Gasson, M., B. Hutt, I. Goodhew, P. Kyberd and K. Warwick, "Invasive neural prosthesis for neural signal detection and nerve stimulation", *International Journal of Adaptive Control and Signal Processing*, Vol. 19, Issue 5, Dec. 2004, pp. 365-75. http://www3.interscience.wiley.com/journal/109858489/abstract.

[36] Knivett, V., "Privacy issues stall smart metering", *Analog DesignLine Europe*, 25 Aug 2009. http://www.analog-europe.com/blogs/219401485.

[37] Patel, S.N., T. Robertson, J.A. Kientz, M.S. Reynolds and G.D. Abowd, "At the Flick of a Switch: Detecting and Classifying Unique Electrical Events on the Residential Power Line", *Proceedings of Ubicomp 2007*, pp. 271-288.

[38] Froehlich, J., E. Larson, T. Campbell, C. Haggerty, J. Fogarty and S.N. Patel, "HydroSense: Infrastructure-Mediated Single-Point Sensing of Whole-Home Water Activity", in *Proceedings of Ubicomp 200*9.

	practically show a naked view of a person.
Mobile phone sensors	With properly installed software, mobile phones can be remotely instructed to activate their microphones and thus act as a portable bug. This works even if the phone is turned off, as most models still operate in such a state, e.g., to trigger an alarm. This has been used, e.g., by the FBI to wiretap organised crime.[39] Services such as “CenceMe”[40] instrument a range of sensors on modern smart phones to provide others real-time updates of the phone owners’ activities (running in a park, in a meeting, etc.).
Home health infrastructure	Japan has already seen a number of health-related online products, in particular, the “smart toilet” which analyses the urine of the user and sends updates to a physician.[41]

Table 3: New data integration efforts (multimodal surveillance)

Online DRM	Media consumption (audio, video, games) increasingly involves online checks, thus offering content providers detailed information about indoor and mobile activities.
RFID tracking	While we are still several years away from a comprehensive retail roll-out, RFID chips are increasingly being used in transportation system, e.g., toll roads (EZ-Pass) or public transport (Suica, Oyster Card). In several instances, movement data from such systems has been used in legal proceedings.
Location data mining	Location-based services such as Mobile Google Maps, Whrrl or the Google Phone allow companies other than the mobile network operators to collect detailed movement data of large parts of the population. Services such as “CitySense” record and mine the

[39] McCullagh, D., and A. Broache, “FBI taps cell phone mic as eavesdropping tool”, CNet News, 1 Dec 2006. http://news.cnet.com/2100-1029-6140191.html.

[40] http://www.cenceme.org

[41] Saenz, A., “Smart Toilets: Doctors in Your Bathroom”, May 2009. http://singularityhub.com/2009/05/12/smart-toilets-doctors-in-your-bathroom.

	location trails of users in San Francisco, in order to detect hot spots of activity.[42]
Electronic health records	Electronic health records are increasingly being used to streamline health administration. Several companies already provide outsourcing of health records, e.g., GoogleHealth or Microsoft HealthVault.
Counterterrorism databases	The FBI National Security Branch Analysis Center holds over 1.5 billion records from public and private sources.[43] The Dept. of Homeland Security holds travel records (PNRs) of millions of travellers.

This digitalisation of our everyday lives is not always happening against our will. *Self-surveillance* systems such as Microsoft Research's SenseCam[44], the myZeo personal sleep coach, Philips' DirectLife or Nike's Nike+SportBand[45] allow one to digitally record various personal parameters (vision, sleep, vital statistics and workout) and often upload it to a commercial website for analysis. Google offers to save one's searches in order to remember what was previously searched (and found).

From self-surveillance, it is only a small step to *self-exposure*, where we freely share the digitally collected information about ourselves not only with our friends and family, but often with "friends" on the Internet or even the public at large. The Nike+SportBand allows one to "compete" with others over the Internet, while location-based services such as Foursquare or Gowalla[46] make it a game to "conquer" parts of your city by sharing the places you go most often and writing reviews on them, ultimately becoming the "mayor" of your local corner café.

[42] http://www.citysense.com

[43] *St. Petersburg Times*, "Americans' privacy put at risk again", editorial, 3 Oct 2009. http://www.tampabay.com/opinion/editorials/americans-privacy-put-at-risk-again/1041104.

[44] Hodges, S., L. Williams, E. Berry, S. Izadi, J. Srinivasan, A. Butler, G. Smyth, N. Kapur and K. Wood, "SenseCam: A retrospective memory aid", *Ubiquitous Computing, Proceedings of Ubicomp 2006*, Springer, pp. 177-193.

[45] See the websites www.myzeo.com, www.directlife.philips.com, and nikerunning.nike.com/nikeos/p/nikeplus/en_US/products/sportband respectively.

[46] See the websites www.foursquare.com and www.gowalla.com.

What, then, is “smart surveillance”? How is it defined, and what makes a particular surveillance practice “smart”? Or conversely: what would constitute “dumb” surveillance?

While there is no accepted definition of smart surveillance yet, we see a smart surveillance system as being capable of extracting application-specific information from captured information (be it digital images, call logs or electronic travel records) in order to generate high-level event descriptions that can ultimately be used to make automated or semi-automated decisions. Many modern information systems, e.g., consumer credit scoring, thus already fall within the scope of this system – it is the increasing inclusion of many hitherto analog sources (e.g., video images, movement tracks, brain waves) into this digital mix, the new technological trends described above, that will soon significantly expand the reach of such systems. Combined with increasing levels of self-surveillance and self-exposure, institutional surveillance could soon reach unprecedented levels of control over our lifes.

5 SOCIO-POLITICAL CONTEXT

The development and use of new surveillance technologies, systems and assemblages such as those listed in the tables above were given a strong impetus by the events of 9/11. The new threats resulting from the changed geostrategic situation and challenges such as international terrorism were recognised in December 2003 with the adoption of the EU Security Strategy “A secure Europe in a better world”[47] and the European Commission’s decision to establish an EU Security Research Programme (ESRP).

As a first step, the European Commission decided to form a “Group of Personalities” (GoP) with members from the Commission, research institutions and the European security and defence industry to oversee the development of the ESRP. In their report, presented in March 2004, the GoP stated that the EU needs to develop capabilities to protect the security of its citizens and that “Europe must take advantage of its

[47] Council of the European Union, “A secure Europe in a better world – The European Security Strategy”, Approved by the European Council held in Brussels on 12 December 2003 and drafted under the responsibilities of the EU High Representative Javier Solana, Brussels, 2003.
http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressdata/EN/reports/104630.pdf

technological strengths" to achieve these goals.[48] The Commission seized upon these suggestions in its Communication "Security Research: The Next Steps".[49] The 2006 European Security Research Agenda specifies that security research should be aimed at identifying and protecting against unlawful or intentional malicious acts harming European societies.[50]

The GoP report makes the point that "technology itself cannot guarantee security, but security without the support of technology is impossible." It provides public authorities with information about threats, which is needed to build effective protection against them. The European Security Research Advisory Board (ESRAB), which was established to provide advice to the European Commission and to oversee the ESRP, explained in 2006 that improved situation awareness and assessment requires "the capture, fusion, correlation and interpretation of disparate forms of real-time and historical data and their presentation in a clear manner, facilitating effective decision-making and performance in a complex environment. Interoperable databases will be essential to allow surveillance information to be cross-referenced against multiple heterogeneous sources".[51] This is a comprehensive description of "smart surveillance".

Many of the projects funded under the European Commission's Preparatory Action for Security Research (PASR) and in the first two calls on security research in the EC's Seventh Framework Programme concern smart surveillance of one kind or another. Smart surveillance is especially stressed for border security, protection against terrorism and organised crime, and critical infrastructure protection.[52]

[48] Group of Personalities in the field of Security Research, "Research for a Secure Europe", Office for Official Publications of the European Communities, Luxembourg, 2004. http://ec.europa.eu/enterprise/policies/security/files/doc/gop_en.pdf.
[49] European Commission, "Security Research: The Next Steps", COM(2004) 590 final, Brussels, 2004. http://cordis.europa.eu/documents/documentlibrary/69322111FR6.pdf.
[50] European Security Research Advisory Board (ESRAB), "Meeting the challenge: the European Security Research Agenda", A report from the European Security Research Advisory Board, Office for Official Publications of the European Communities, Luxembourg, 2006. http://ec.europa.eu/enterprise/policies/security/files/esrab_report_en.pdf.
[51] ESRAB, op. cit.
[52] ESRAB, op. cit. European Commission, "Towards a more secure society and increased industrial competitiveness: Security research projects under the 7th Framework Programme for Research", DG Enterprise and Industry, Brussels, 2009. ftp://ftp.cordis.europa.eu/pub/fp7/security/docs/towards-a-more-secure_en.pdf.

However, the GoP and the Commission acknowledge that the technologies in question are not limited to security purposes but can often be used for applications in another area. They especially point to the dual use of technologies with an increasing overlap of functions and capabilities required for military and non-military security purposes.[53]

Recognising this problematic potential of smart surveillance technologies, the Commission stated as early as 2004 in its Communication on "Security Research: The Next Steps" that in security research "individual rights, democratic values, ethics and liberties need to be respected. A balance must be struck between surveillance and control to minimise the potential impact of terrorist action, and respect for human rights, privacy, social and community cohesion and the successful integration of minority communities."[54]

In its recent Communication on freedom, security and justice, Commission reinforced this claim: "The area of freedom, security and justice must above all be a single area in which fundamental rights are protected, and in which respect for the human person and human dignity, and for the other rights enshrined in the Charter of Fundamental Rights, is a core value".[55] The same Communication goes on to state that the EU must be increasingly aware of privacy and data protection issues related to emerging technologies and act accordingly in order to fulfil the above claim.

Important actors have already expressed their concerns about the amount of collecting, storing and processing of data in security-related surveillance systems. Here are a few examples (among many others that could be cited):

[53] GoP, op. cit.

[54] EC, COM(2004) 590 final, op. cit.

[55] European Commission, "An area of freedom, security and justice serving the citizen", COM(2009) 262 final, Brussels, 2009. This Communication is the basis of the multi-annual programme in the area of freedom, security and justice, known as the Stockholm programme. See also: http://www.se2009.eu/en/the_presidency/work_programme/the_stockholm_programme. The Swedish Presidency [of the EU] says (at the last mentioned website) that "The vision for work with the Stockholm Programme is a more secure and open Europe where the rights of individuals are safeguarded."

- The European Data Protection Supervisor: “The policies in the Area of freedom, security and justice should not foster the gradual move towards a surveillance society.”[56]
- Statewatch: “If ‘collective security’ demands the surveillance of all movements and all telecommunications and the collection of all the fingerprints of everyone living in the EU there can be no individual freedom, except that sanctioned by the state.”[57]
- UK House of Lords: “The widespread use of surveillance technology poses a significant threat to personal privacy and individual freedom... As surveillance is potentially a threat to privacy, we recommend that before public or private sector organisations adopt any new surveillance or personal data processing system, they should first consider the likely effect on individual privacy.” The Lords also recommended that each new surveillance measure should pass a technology and privacy impact assessment process before being introduced.[58]

A particular concern is the tendency towards function creep – i.e., where data collected for one purpose is used for another. For instance, at the 2006 Law Enforcement Information Management Conference, the presenters of IBM’s “Smart Surveillance Solution” stated: “There is a lot of video captured and stored, and often the value of the video is unknown until well after the time of capture. Stored video is *potentially valuable later*” [Italics added].[59] This is just an indication of how little awareness exists among technologists and business people about considering the possible negative social effects. A second concern arises from the fact that the digitalisation of information makes it easier to create new databases and to mine data from different databases.

6 LEGAL ISSUES

[56] EDPS, op. cit., para 23.

[57] Bunyan, T., *The Shape of Things to Come*, version 1.3, Statewatch, London, 30 Sept 2008, p. 7.

[58] House of Lords 2009, op. cit., p. 26, p. 28.

[59] Cooke, R., and K. Scruggs, “Smart Surveillance - Effective Information for Public Safety”, Paper presented at: 30th Annual Law Enforcement Information Management Conference, Grapevine, TX, 5-9 June 2006. http://www.iacptechnology.org/LEIM/2006Presentations/Smart_Surveillance%20_Cooke_and_Scruggs.pdf

There are legal protections against function creep and some of the applications and practices facilitated by smart surveillance that do or might intrude upon our privacy, but some improvements to the legal framework are becoming increasingly apparent.

The protection of individual privacy at the EU level is mainly governed by Article 8 of the 1950 European Convention for the Protection of Human Rights and Fundamental Freedoms (Council of Europe 1950) and Article 7 of the 2000 Charter of Fundamental Rights of the European Union. In addition, data protection in the EU is governed by Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the Data Protection Directive), Directive 2002/58/EC on privacy and electronic communications (the e-Privacy Directive), the Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters (the so-called Data Protection Framework Decision)[60], Article 8 of the Charter of Fundamental Rights of the European Union, and the Council of Europe (1981) Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention No. 108).

Notwithstanding such abundance of privacy and data protection legislation, when it comes to security, surveillance and third pillar activities[61], the European legislation framework seems to become more complex and less coherent. In the context of a growing use of information technologies and a tendency towards mutual access to private and public databases, the EU pillar structure has been considered a major obstacle to the definition of a more effective framework. For instance, the main piece of EU legislation on data protection, the Data Protection Directive of 1995, does not apply to "processing operations concerning public security, defence, State security… and the activities of the State in areas of criminal law" (Directive 95/46/EC, Art. 3(2)). Furthermore, as underlined by the Court of Justice in its judgement on

[60] European Council, Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L 350, 30 Dec. 2008, pp. 60-71.

[61] The 1993 Treaty of Maastricht introduced the three pillar EU structure. The first pillar comprised European Community economic, social and environmental policies. The second pillar was that of the Common Foreign and Security Policy and the third pillar supported police and judicial co-operation. The Lisbon Treaty did away with the three pillar structure on 1 December 2009.

passenger name records (PNR), the Data Protection Directive does not apply to the processing of data firstly collected by private actors and later accessed for public security purposes.[62] This aspect is even more worrying, because it risks leaving the access of public authorities to commercial data in a sort of no man's land. Finally, the adoption of the Data Protection Framework Decision in December 2008, while achieving some first results in extending most of the data protection principles to the exchange and processing of data in the framework of police and judicial co-operation in criminal matters, will not address all the lacunae that have emerged in the field of security and surveillance.[63]

Thus, despite the fact that security-related processing within Europe lacks a common regulatory basis, specific sectors have gone ahead alone, as indicated in the Schengen Agreement,[64] the Europol[65] and Eurojust[66] Agreements, and the Prüm Council Decision.[67] All include detailed data protection rules and procedures in their respective texts (admittedly using as basic principles and procedures those introduced in the Data Protection Directive). Therefore, what is actually in place at present within the EU in relation to the processing of personal data for security and surveillance purposes is a series of sector-specific approaches that co-exist together with the 1981 Council of Europe Convention on data protection and the Data Protection Framework Decision.

[62] European Court of Justice, European Parliament v Council of the European Union (C-317/04) and Commission of the European Communities (C-318/04), Joined cases C-317/04 and C-318/04, European Court reports, 2006, p. I-04721.

[63] See Hijmans, H., and A. Scirocco, "Shortcomings in EU Data Protection in the Third and Second Pillars. Can the Lisbon Treaty be Expected to Help?", *Common Market Law Review*, Vol. 46, No. 5, 2009, pp. 1493-97; De Hert, P., and M.V. Papakonstantinou, "The data protection framework decision of 27 November 2008 regarding police and judicial cooperation in criminal matters. A modest achievement however not the improvement some have hoped for", *Computer Law and Security Review*, Vol. 25, No. 5, 2009, pp. 403-14.

[64] Actually referring to Schengen I (Agreement between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders, entered in 1985) and Schengen II or CIS (Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders, entered in 1990).

[65] European Council, Europol Convention, Brussels, 26 July 1995.
http://www.europol.europa.eu/index.asp?page=legal.

[66] European Council Decision of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime (2002/187/JHA), OJ L 63/l, 2002.

[67] European Council, Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ L 210, 6 Aug. 2008, pp. 1-11.

Case law offers some guidance in this area. Of particular relevance is case law of the European Court of Human Rights on Art. 8 ECHR, and especially its recent judgements on secret control and mining of telecommunications[68] and retention and processing of DNA and fingerprints[69]. This last case sets up important limits and should offer guidelines to the implementation of Member States' legislation on DNA and fingerprint databases.[70] "Should" is the operative word. Despite the Court's judgement, the UK seems reluctant to comply with the Court's decision.[71]

The entry into force of the Lisbon Treaty will, probably and partially, modify the landscape of privacy and data protection in the EU, also with respect to security and surveillance measures. Indeed, the Lisbon Treaty brings into force the EU Charter of Fundamental Rights and introduces a new provision on data protection (Art. 16 of the Treaty on the Functioning of the European Union). It also expands the decision-making powers of the European Parliament, both with regard to EU and international instruments at a time when several existing agreements based on the processing of personal data have been re-opened for discussion (such as the PNR and SWIFT agreements) and when negotiations of a binding transatlantic agreement on privacy, data protection and data sharing have been announced.[72]

[68] European Court of Human Rights, Case of Liberty and others versus United Kingdom, Application no. 58243/00, Strasbourg, 1 July 2008.

[69] European Court of Human Rights, Case of S. and Marper versus the United Kingdom, Application nos. 30562/04 and 30566/04, Strasbourg, 4 Dec 2008.

[70] De Beer, D., P. De Hert, G. Gonzalez Fuster and S. Gutwirth, "Nouveaux éclairages de la notion de la notion de 'donnée personnelle' et application audacieuse du critère de proportionnalité", Obs. Cour européenne des droits de l'homme Grande Chambre *S et Marper c. Royaume Uni*, 4 décembre 2008, *Revue Trimestrielle des Droits de l'Homme*, no. 81, January 2010, pp. 141-61. See also Gonzalez Fuster, G., "TJCE - Sentencia de 04.12.2008, *S. y Marper c. Reino Unido*", *Revista de Derecho Comunitario Europeo*, no. 33, May-Aug. 2009, pp. 619-33.

[71] Travis, A., "Police routinely arresting people to get DNA, inquiry claims", *The Guardian*, 24 Nov 2009. http://www.guardian.co.uk/politics/2009/nov/24/dna-database-inquiry. The way in which the UK government will implement the ECtHR decision is particularly relevant in a context characterised by the proliferation of international and European legal instruments aiming at establishing DNA analysis files in each EU Member State and fostering their exchange. See Bellanova, R., "Prüm: A Model "Prêt-à-Exporter"? The 2008 German–US Agreement on Data Exchange", CEPS Challenge Paper No. 13, 12 March 2009.

[72] EU-US Joint Statement on "Enhancing transatlantic cooperation in the area of Justice, Freedom and Security", 20 Oct 2009.
http://www.se2009.eu/polopoly_fs/1.21271!menu/standard/file/EU-US%20Joint%20Statement%2028%20October%202009.pdf. On the EU and US privacy and data protection frameworks covering security measures, see also Bellanova, R., and P. De Hert, "Protection des données personnelles et mesures de sécurité: vers une perspective transatlantique", *Cultures & Conflits*, Vol. 74, 2009, pp. 63-80.

Thus, an analysis of the legislation on data protection and privacy relating to security and surveillance practices brings four main sets of challenges.

- First, if security and surveillance frequently conflate, and international and internal securities are blurring into each other, how should privacy and data protection principles be applied to those practices?
- Second, what is the legal protection of data about non-identified persons, when those kinds of data are acquiring a growing relevance for a wide range of state activities and law enforcement?
- Third, what is the relevant framework of privacy and data protection when data of a commercial and non-commercial nature are increasingly processed for security and surveillance purposes? And how is that framework applied?
- Fourth, how should the use of powerful new technologies, such as data mining and profiling, that challenge the very principles of data protection, be regulated?

Policy-makers need to address these questions.

7 PRIVACY IMPACT ASSESSMENTS

Policy-makers should also engage other stakeholders[73] as they address such questions. One way to engage stakeholders is through the mechanism of privacy impact assessments (PIAs). PIAs are a useful complement to privacy safeguards such as privacy by design, privacy certification schemes (such as the EuroPrise label[74]), best available practice and privacy standards[75]. PIAs provide a way of instilling more trust and optimising the configuration, safety and security of policies, projects or services using personal data. PIAs can be regarded as a specialised tool of risk management. A PIA, tailored to smart surveillance, can also be seen as responding to the “need for reflection on the consequences for law enforcement authorities [among others] and for European citizens before new instruments are adopted. This reflection should duly take into account the costs for privacy and the effectiveness for law enforcement, in

[73] We define “stakeholder” to mean anyone interested in or affected by an action by a third party.

[74] www.european-privacy-seal.eu/

[75] The Resolution on a privacy standard governing international data transfers adopted at the 31st Annual Conference of Privacy and Data Protection Commissioners in Madrid in early November 2009 is a step in this direction.

the first place when new instruments are proposed and discussed, but also after those instruments are implemented, by means of periodic reviews".[76]

Privacy impact assessments have been defined in various ways, but essentially a PIA is "a systematic process for evaluating the potential effects on privacy of a project, initiative or proposed system or scheme" and finding ways to mitigate or avoid any adverse effects.[77] According to privacy expert Roger Clarke,

> The concept of a PIA emerged and matured during the period 1995-2005. The driving force underlying its emergence is capable of two alternative interpretations. Firstly, demand for PIAs can be seen as a belated public reaction against the increasingly privacy-invasive actions of governments and corporations during the second half of the twentieth century. Increasing numbers of people want to know about organisations' activities, and want to exercise control over their excesses… Alternatively, the adoption of PIAs can be seen as a natural development of rational management techniques… Significant numbers of governmental and corporate schemes have suffered low adoption and poor compliance, and been subjected to harmful attacks by the media. Organisations have accordingly come to appreciate that privacy is now a strategic variable. They have therefore factored it into their risk assessment and risk-management frameworks.[78]

A few countries have been using PIAs in recent years, notably Australia, Canada, Hong Kong, New Zealand, the UK and the US.[79] Other countries, such as Denmark and the Netherlands, have been considering the introduction of PIAs.

[76] EDPS, op. cit., p. 4.

[77] This definition combines two: one from the Treasury Board Secretariat of Canada, *Privacy Impact Assessment Guidelines: A framework to Manage Privacy Risks*, Ottawa, 31 August 2002. http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paipg-pefrld1-eng.asp. The other comes from Clarke, R., "Privacy impact assessment: Its origins and development", *Computer Law and Security Review*, Vol. 25, Issue 2, 2009, pp. 123-35. Clarke has also compiled a list of various definitions in Appendix 1 of his paper.

[78] Clarke, op. cit.

[79] Another important term to distinguish in this context is "prior checking", which appears in Article 20 of the European Data Protection Directive and which says in part that "Member States shall determine the processing operations likely to present specific risks to the rights and freedoms of data subjects and shall check that these processing operations are examined prior to the start thereof." The European Data Protection Supervisor (EDPS) has a similar power under a Regulation of the European Parliament and Council, which obliges European Community institutions and bodies to inform the EDPS when they draw up administrative measures relating to the processing of personal data. See Regulation (EC) No 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, 18 Dec 2000. http://www.europarl.europa.eu/tools/disclaimer/documents/l_00820010112en00010022.pdf

In its RFID Recommendation, the European Commission said that those organisations planning to introduce and use RFIDs should undertake a PIA and it called upon Member States to provide their inputs to the Article 29 Data Protection Working Party within a year of the release of the RFID Recommendation (i.e., by May 2010) and that the Article 29 Working Party should consider the development of a “privacy and data protection impact assessment”. Although this was mentioned only in the context of RFID, there seems no reason why such a privacy and data protection impact assessment could not be applied in instances involving other technologies, services or policies that impact our privacy and data protection.

In addition, the International Organization for Standardization (ISO) has produced a standard for PIAs in financial services, which describes the PIA activity in general, defines the “common and required components” of a PIA, and provides guidance.[80]

More recently, the 31st International Conference of Data Protection and Privacy Commissioners adopted a resolution on international standards of privacy which called upon States to implement “privacy impact assessments prior to implementing new information systems and/or technologies for the processing of personal data, as well as prior to carrying out any new method of processing personal data or substantial modifications in existing processing”.[81]

There are differences in approach between the existing PIA methodologies. That developed by the UK Information Commissioner’s Office (ICO), for example, places an emphasis on consultations with relevant stakeholders. In Canada, government departments and agencies are required to perform and include the results of a PIA in their funding submissions to the Treasury Board, which manages the government’s purse strings. As well, copies of the PIAs are to be forwarded to the Office of the Privacy Commissioner, who can and does audit the PIAs. In the US, PIAs are to be posted on the websites of the government departments that undertake them.

[80] International Organization for Standardization, ISO 22307:2008: Financial services -- Privacy impact assessment, Geneva, 16 Apr 2008. http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=40897.

[81] https://www.agpd.es/portalweb/canaldocumentacion/common/estandares_resolucion_madrid_en.pdf

A PIA methodology, like that promoted by ICO, offers a good mechanism to engage stakeholders in the consideration of the impacts and issues arising from the increasing deployment of smart surveillance, and in the consideration of alternatives or safeguards to mitigate the negative effects. With regard to smart CCTV, Introna and Wood comment that "seemingly mundane design decisions may have important political consequences that ought to be subject to scrutiny".[82] PIAs would provide that scrutiny. While the public has not objected strenuously to the proliferation of some forms of surveillance, e.g., video cameras on streets, in the Underground, around shops, etc., especially as they have been useful in apprehending evil-doers, the public has objected to other forms, such as personalised advertising. How the public will react to the emergence of new, smart surveillance technologies in particular contexts is not at all clear.

However, the risks are rather clearer. The advent of smart surveillance greatly facilitates social sorting, as David Lyon[83] and others have noted. Among the risks attending social sorting is that it turns nominal democracies into something repugnant politically and socially, where choices and opportunities are much greater for some people and decidedly fewer for others. Graham and Wood stress "the subtle and stealthy quality of the ongoing social prioritizations and judgements that digital surveillance systems make possible… These systems are being used to prioritize certain people's mobilities, service quality and life chances, while simultaneously reducing those of less favoured groups. Importantly, both beneficiaries and losers may, in practice, be utterly unaware that digital prioritization has actually occurred."[84]

A PIA, especially if it engages stakeholders, including the public, is potentially a powerful tool for risk management and transparency. If a policy-maker or developer

[82] Introna, Lucas D., and David Wood, "Picturing Algorithmic Surveillance: The Politics of Facial Recognition Systems", *Surveillance & Society*, Vol. 2, Issue 2/3, 2004, pp. 177-198 [p. 178]. http://www.surveillance-and-society.org/cctv.htm. The authors also make the useful observation that "If there is any 'law' in the history of technology it is that technologies are rarely used in ways that their inventors intended" – which is another reason why a PIA should be undertaken, i.e., so that stakeholders can give consideration to ways in which technologies might be used in addition to the way they are intended to be used.

[83] Lyon has written extensively on the subject. See Lyon, David (ed.), *Surveillance as Social Sorting: Privacy Risk and Digitial Discrimination*, Routledge, London, 2003. See also Lyon, David, *Surveillance Studies: An Overview*, Polity Press, Cambridge UK, 2007.

[84] Graham, Stephen, and David Wood, "Digitizing Surveillance: Categorization, Space, Inequality", *Critical Social Policy*, Vol. 23, No. 2, 2003, pp. 227-248 [p. 231].

or operator of surveillance technologies and systems initiates a PIA well before a policy or system is launched, he or she has an opportunity to minimise or eliminate the risks and liabilities that might flare up after launch. Engaging and consulting stakeholders early on will help ensure transparency and minimise undue criticism from stakeholders. Best of all, by consulting stakeholders, policy-makers or developers might profit from new ideas or alternatives suggested by stakeholders that they might not have considered otherwise.

While PIAs are a useful tool, existing PIAs focus almost entirely on data protection rather than privacy. Thus, a true PIA should cover the four aspects traditionally associated with privacy, i.e.,

- Privacy of personal information – which is concerned with protection of our personal data held by others
- Privacy of the person – which is concerned with potential intrusions such as body searches and biometrics
- Privacy of personal behaviour – which is concerned with potential intrusions such as video and audio surveillance and media intrusion
- Privacy of personal communications – which is concerned with potential intrusions arising from telephonic intercepts, monitoring e-mail, etc.

In addition, existing PIA methodologies are ill-equipped to deal with surveillance involving law enforcement activities, security or third pillar issues (those issues delineated in Art. 3(2) of the EU Data Protection Directive), especially those involving transborder flows of data. Assessments in these fields are carried out in a non-transparent way based on evidence that is often not accessible for the public. Furthermore, existing PIA methods deal with existing information technologies. A new PIA framework and policy seem necessary for dealing with third pillar surveillance and smart surveillance technologies expected to emerge over the next decade.

Thus, we see a need to extract the best elements of existing PIA methodologies and to build on those to construct a PIA methodology designed to address the particularities of surveillance projects, technologies, applications and policies while recognising security sensitivities. The PIA methodology should be fit to deal both with prohibitive and regulatory aspects of surveillance projects: when to enforce the opacity of the individual, when to impose accountability, control and transparency on the surveillants.[85] When privacy is at stake, the outcome of a PIA may result in a simple "no" to a proposed technology, policy or programme. The sheer fact of conducting an assessment does not mean the broader legitimacy question is answered.

So far, nothing like this exists at the European level. Accordingly, we believe it is important to design a PIA methodology suitable for sorting out smart surveillance projects (using the word "projects" in its widest sense), including those involving transborder flows of personal data.

8 CONCLUSION

The tension between technologies of surveillance, security goals and privacy, especially data protection, is not new, and has been thoroughly examined since the mid-1970s. But this literature is mainly rooted in an IT literature with a legalistic perspective, and concerns either national cases in Europe (e.g., UK, Sweden, Germany, France) or the US and Canada. Recently, we have seen a transformation with specific research in the EU and quite interesting comparisons emerging from joint research between Canada and Europe on the extensive reach of surveillance in relation to the societal and political contexts[86], as well as a better understanding of the competition between world companies for the demands of stakeholders (police, border guards, intelligence services or other private bodies) concerning interoperability, transnational exchanges of data and new technological means.[87] Nevertheless, this research often means an approach describing the rise of the surveillance society in general, without a thorough understanding of the transnational and international political contexts.

[85] De Hert, P., and S. Gutwirth, "Privacy, data protection and law enforcement. Opacity of the individual and transparency of power" in E. Claes, A. Duff & S. Gutwirth (eds.), *Privacy and the criminal law*, Intersentia, Antwerp, 2006.

[86] Bigo, D., E. Guittet and A. Scherrer (eds.) *Mobilités sous surveillance, comparaison Europe et Canada*, Athena, Montréal, October 2009.

[87] Page, L., "Interpol proposes world face-recognition database", *The Register*, 20 Oct 2008. http://www.theregister.co.uk/2008/10/20/interpol_face_scan_plan/.

To improve privacy and data protection under the new security and surveillance parameters implies a need to be aware of the international context, of the development of transnational networks of technology providers and of the international efforts in criminal justice and security. PIAs have so far only been used within countries. They have not been used to address security and surveillance issues at the international level.

The time seems ripe to do so. With the adoption of the Lisbon Treaty and especially Article 16, the three pillar structure has been swept away. Now the privacy and data protection rules can be the same for law enforcement and security as for other sectors to which the European Data Protection Directive applies. Also, the EC's Communication re the Stockholm Programme, as referenced above, signals again that the Commission (like the EDPS) believes the pendulum has swung too far toward security at the expense of privacy and other fundamental rights since 9/11. The European Parliament's rejection of a new agreement on the transfer of data about Europeans' financial transactions shows that the European Parliament, newly strengthened by the Lisbon Treaty, intends to flex its muscle on privacy.

If the European Commission's Directorate General for Justice proposes amendments or revisions to the Data Protection Directive, it would be a good opportunity to make provision for the conduct of PIAs, preferably mandatory PIAs[88], whenever any organisation undertakes a new initiative potentially impacting our privacy or involving the use of personal data, even if it is an initiative involving security or the transborder flow of data.

It would also be useful if the Article 29 Working Party were to consider development of a PIA framework applicable not only to RFID but other forms of smart surveillance. The Commission has recently funded a Living in Surveillance Societies COST[89] action which supports surveillance studies and which comprises more than 100 experts from 26 countries. This group could usefully conduct studies on how

[88] Wright, David, "Should privacy impact assessments be mandatory?", *Communications of the ACM* , 2011 (forthcoming).
[89] COST = Cooperation in Science and Technology. See http://www.liss-cost.eu/

PIAs could be tailored to address the prospective deployment of smart surveillance technologies, services and policies, including those at the international level. Although surveillance in its many forms continues to expand largely unchecked by inputs or considerations from stakeholders, including the public, it is time to give stakeholders a voice in the decision-making processes which affect the privacy and data protection of all of us.

David Wright (david.wright@trilateralresearch.com) Managing Partner, Trilateral Research & Consulting, London; **Michael Friedewald** (Michael.Friedewald@isi.fraunhofer.de) Senior Researcher, Fraunhofer Institute for Systems and Innovation Research, Karlsruhe; **Serge Gutwirth** (serge.gutwirth@vub.ac.be), Professor of Law, Centre for Law Science Technology & Society at the Vrije Universiteit Brussel, Brussels; **Marc Langheinrich** (marc.langheinrich@unisi.ch) Assistant Professor of Computer Science, Faculty of Informatics, University of Lugano; **Emilio Mordini** (emilio.mordini@cssc.eu), Director, Centre for Science, Society and Citizenship, Rome; **Rocco Bellanova** (rocco.bellanova@vub.ac.be) Researcher, LSTS Vrije Universiteit Brussel and Facultés universitaires Saint-Louis; **Paul De Hert** (paul.de.hert@vub.ac.be) Professor of International and European Criminal Law, Vrije Universiteit Brussel; **Kush Wadhwa** (kush.wadhwa@trilateralresearch.com) Partner, Trilateral Research & Consulting, London; **Didier Bigo** (didier.bigo.conflits@gmail.com), Professor, Department of War Studies, King's College London.