



DIALOGUE

Volume 2 • No. 7 | 2009 December

WORKSHOP REPORT

Restrictions on the Implementation of the EU Data Protection Directive for Public Interest, Security, and Defense

IN THIS ISSUE

- 1 *Workshop Report*
Restrictions on the Implementation of the EU Data Protection Directive for Public Interest, Security, and Defense
- 3 *Feature Article*
CCTV in 2009: Policy, Evidence, and Expansion
- 7 *News and Notes*

DIALOGUE is published quarterly by The Hastings Center, a HIDE Partner.

PRINCIPAL INVESTIGATOR
Thomas H. Murray, *President and CEO*

EDITOR & PROGRAM MANAGER
Karen J. Maschke, *Research Scholar*

ART DIRECTOR
Nora Porter

MANAGING EDITOR
Joyce A. Griffin

CONSULTING EDITOR
Gregory E. Kaebnick

This work was supported in part by the European Commission under contract FP7-217762 HIDE, Homeland Security, Biometric Identification & Personal Detection Ethics.

by **Simon Dobrišek, University of Ljubljana, Slovenia**

One of HIDE's objectives is to promote international dialogue on the ethical and political issues that tend to polarize the wide range of stakeholders involved in biometrics and personal detection technologies. In September 2009, the University of Ljubljana organized the second HIDE problem-solving workshop, "Restrictions on the Implementation of the EU Data Protection Directive for Public Interest, Security, and Defense." Its aim was to bring together individuals and representatives from governmental and nongovernmental organizations (with an emphasis on the new member and Balkan states) to identify and discuss ethical and other issues related to the restrictions on the scope of rights in the implementation of EU data protection principles.

The main theme of the workshop emphasized Article 13 of the EU Data Protection Directive, which states that EU member states may adopt legislative measures to restrict the scope of the rights provided for in the directive when such a restriction constitutes a necessary measure to safeguard national security, defense, pub-

lic security, and crime prevention. It is well known that existing practices

“We are on the boundary of two societies—one where privacy is the norm, and the other where most movements are monitored.”

and legislative measures regarding the Data Protection Directive are not harmonized across the EU member states. This is especially true for the new member and Balkan states. The world economic crisis, organized crime activities, and terrorist and health threats have forced member states to adopt new legislative measures and deploy biometric and personal detection technologies that are used for security, defense, and to safeguard the public interest. However, what each member state wants to do in order to determine its level of secu-



ity differs from state to state, and each state's appreciation of what may constitute "a necessary measure" and an "important public interest" is, by its very nature, a major source of discrepancy across the national laws. For this reason, reconciliation of the varying practices in this field remains an important issue.

With these objectives in mind, the workshop was organized around four main themes: 1) the circumstances that may lead to the restriction of EU data protection principles; 2) the impact of counter-terrorist border control legislative measures on privacy protection; 3) the application of the principle of proportionality to the restriction of data protection rights; and 4) the implementation of harmonizing practices in the new member and Balkan states.

“The workshop successfully demonstrated the importance of a dialogue among the different actors in a field that is ethically and politically sensitive.”

During the workshop, 16 invited speakers (nine of them from new member and Balkan states) addressed all the above themes. Together with the other workshop participants, the speakers identified several important issues and offered small-step suggestions for solutions.

I Have a Gun, So I Have the Right to Shoot!

In the opening lecture, Nataša Pirc Musar wondered whether we take advantage of all the possibilities modern technology offers us just because we can. Numerous sophisticated gadgets that make it possible to intrude on someone's privacy are available on the market, but does that mean we can use them with no limitations? She argued that fundamental principles of personal data protection—such as data minimization, proportionality, security, purpose specification, accuracy, and quality—are the

only stable principles that should be able to withstand the technological challenge. Musar said that, for this reason, it is very important to build upon the fundamental principles of data protection and to combine them with proactive privacy protection tools, such as privacy impact assessments and privacy by design. Following the main workshop theme, she gave several examples of establishing limitations for law enforcement authorities (especially on the secret services) with regard to the secret supervision of individuals who have computers.

Restrictions on Personal Data and Privacy Protection Rights

In the first session, participants focused on the circumstances that may lead to the restrictions of rights regarding their personal data and protection of privacy, and under what conditions such restrictions can be applied. Rudi Rizman, who chaired the session, pointed out that we are actually standing on the boundary of two societies—one where freedom and privacy are the norm, and the other where most movements, habits, and transactions are monitored as aberrant behaviors. He also reminded the participants of the famous statement by Warren and Brandeis that the right to privacy is "the right to be let alone."

Neil Robinson argued that much of the current privacy-versus-security debate occurs at an emotional level, with little evidence informing the argument. His presentation outlined the results of a study that sought to understand the real privacy/security tradeoffs of individuals so that policymakers can be better informed about their true preferences in this area and, thereby, better match policies to user preferences. Some participants responded to his presentation by expressing doubts about how one can set a price tag on civil liberties and

rights. Wayne Crews focused on the principles for preserving anonymity and privacy in the global "homeland security" and "surveillance state." Saša Jankovic contended that for ensuring adherence to the rule of law and respect for human rights, the application of restrictions must be freely and fully overseen by authorities that are independent of the security apparatus and the executive branch in general. He said that an ombudsman may be one of them, at least in countries in which this institution is mandated not only to monitor administration in delivering good governance, but also to ensure respect for human rights, as is the case in Serbia. Joseph A. Cannataci examined the extent to which the notions of "a necessary measure" and an "important public interest" are already addressed by statute and case law. He questioned whether a surveillance technology, once unleashed, can ever be reasonably constrained by legally enforceable rules.

The Impact of Border-Control Legislative Measures on Privacy Protection

Terrorist and other threats force EU member states to adopt new legislative measures and deploy biometric and personal detection technologies to ensure border security. These measures and technologies greatly interfere with data protection principles. The presentations and discussion in the second session addressed these issues. At the beginning of the session, Iztok Prezelj reminded the audience that historically borders were always present as demarcation lines between us and "the others," and as such, they greatly contribute to our identity. François Géré said that it is often argued that biometrics provide security against clandestine migration and potential terrorist activities. Then he considered the problem the other way round. Western societies have themselves become migrant. More and more citizens cross national borders both for business and leisure. Therefore, they

CONTINUES ON PAGE 4



FEATURE ARTICLE

CCTV in 2009: Policy, Evidence, and Expansion

By Polo Black Golde, The Hastings Center

In September of this year, CameraWatch—an organization in the United Kingdom that monitors the use of closed-circuit television (CCTV) and compliance with the government's data protection laws and policies—described a government plan to expand the use of CCTV into an existing family monitoring program that is designed to focus on the “small number of families that account for a disproportionate amount of anti-social behavior” in the United Kingdom.¹ According to the Home Office, “we now know that this small number of families need an intensive, persistent and, if necessary, coercive approach . . . this work is very much targeted at those whose anti-social behaviour is threatening their tenancies, is putting their children at risk or is likely to lead to them facing significant enforcement action.”² The family intervention program is a coordinated effort that includes among its resources social services, education departments, and criminal justice and police forces.³ CameraWatch reported that 20,000 “‘problem families’ who have run afoul of social service officials will be watched around the clock and subjected to surprise inspections by government agents.”⁴

This surveillance program raises some of the underlying and longstanding concerns about the government's use of CCTV to monitor behavior. Policy debates regarding civil liberties, data protection, and crime deterrence have quite under-

standably latched onto CCTV—which is used more extensively in the United Kingdom than anywhere else in the world—as the poster child of excessive surveillance technology. Many commentators have vigorously argued that there is little evidence to support the UK government's extensive use of CCTV as a crime deterrent. Yet even though government officials have begun to scrutinize the use of CCTV over the past 15 years, they continue to embrace the technology and to broaden its scope of use. This article will examine recent developments in the U.K.-centered debate regarding evidence-based policy-making for CCTV and highlight the surveillance creep that occurs with each expansion of the deployment of this form of surveillance technology.

A Brief Introduction to CCTV

In a closed-circuit television system, a camera transmits a signal only to a limited number of monitors for viewing and recording; it differs from broadcast television in that its signals are not publicly transmitted. A typical system comprises a camera, a viewing monitor, and a recording/storage system. The technology has evolved considerably since its first testing in the 1970s, with improvements in image resolution and color, the ability

for cameras to pan and zoom, and in some cases the introduction of speakers so that surveillance personnel can speak to the individuals being viewed.

There are two main methods that surveillance personnel use to imple-

“Philosophical, political, and legal debates have centered on a range of surveillance issues in which CCTV is implicated, many of which pertain to civil liberties and data protection.”

ment CCTV. The first is proactive: video feeds are actively monitored and immediate responses to events are possible. The second is called reactive or postevent: footage is not monitored, only stored, and can be called up after an event is reported. Optical recognition software like Automatic Number Plate Recognition can be used with either approach and works with preexisting CCTV infrastructure.

The Home Office's 2007 *National CCTV Strategy* describes the history of the implementation of CCTV in the United Kingdom. The report points out the important role CCTV has played since the 1990s in prosecuting terrorist and serious criminal cases, and notes that between 1999 and

CONTINUES ON PAGE 5

Workshop Speakers

- Strahinja Brajuškovic
The Anti-Trafficking Center
- Joseph A. Cannataci
University of Central Lancashire
- Wayne Crews
Competitive Enterprise Institute
- François Géré
Global Security Network
- Snjeana Grgic
Croatian Personal Data Protection Agency
- Alexander G. Ivanchenko
Russian Security Industry Association
- Saša Jankovic
Ombudsman of the Republic of Serbia
- Juliet Lodge
University of Leeds
- Marijana Marucic
Directorate for Personal Data Protection
- Vojislav Milošević
Center for Counter-Terrorism and World Peace
- Nataša P. Musar
Information Commissioner of the Republic of Slovenia
- Hana Pecháčková
European Commission
- Neil Robinson
RAND Corporation
- Mario Zadro
Migration, Asylum, Refugees Regional Initiative Project
- Judit Zeller
University of Pecs
- Vít Zvánovec
The Office for Personal Data Protection

want to travel quickly and securely. Not only are they ready to abandon parts of their freedom and privacy, but they are asking for more security, regardless of the potential dangers. He said that on the basis of a mutual contract between the state and its citizens, democratic governments must refrain from enacting measures that in the future could turn negative, and that they have a duty to protect the average traveller against the consequences of some of these excessive

demands. Alexander G. Ivanchenko argued that the introduction of biometric travel passports and new border-crossing regulations by many countries contributed to a heightened public interest in biometrics that is not necessarily altogether positive. The dispute over biometrics cannot be resolved by administrative measures alone and, taking a sociohumanitarian turn, should be treated accordingly. Strahinja Brajuškovic presented an approach to reform the security system in the Western Balkans, developed by the European Union with the North Atlantic Treaty Organization, the Organization for Security and Cooperation in Europe, and the Stability Pact for Southeastern Europe in the context of the stabilization and association processes.

Proportionality of the Restrictions on Personal Data and Privacy Protection Rights

All the restrictions on individual rights in the context of personal data and privacy protections must pass the proportionality test; however, the principle of proportionality has many different formulations, and even in the same court it can be articulated differently. Under the proportionality test, the burden of justification for government actions affecting privacy rights varies tremendously, depending on the public interest being pursued, on the one hand, and the right at stake, on the other. Hana Pecháčková contended that any necessary step the European Commission takes to enforce public security must always be accompanied by adequate safeguards to ensure scrutiny, accountability, and transparency. Judit Zeller explained that biometric identification is still a foreign body in the Hungarian legal system. In the light of the decisions of

the Constitutional Court of Hungary on data protection and self-determination in connection with personal information, the question arises of whether the use of biometric data complies with the postulates of necessity and proportionality. Juliet Lodge argued that by focusing on proportionality, we show our values but do not ask the right question.

Implementing Harmonizing Practices

Dialogue is a model for progress toward harmonization. The workshop concluded with several presentations of harmonizing practices in new member and Balkan states. Integrated border management is crucial for improving regional stability in the Western Balkans. Practical measures—including the exchange of experiences on border control, training, and joint operations—have a key role in further improvements in this field. Mario Zadro provided information about the experience of the Migration, Asylum, Refugees Regional Initiative in applying new technologies in migration management. At the end of the workshop, Antonio D’Amico and Stane Štefancic discussed the activities of the European Civil Registry Network.

The workshop successfully demonstrated the importance of a dialogue among the different actors in a field that is ethically and politically sensitive. The most important goal of such events—hopefully achieved here—is taking another small step toward establishing a standard system of values for all the key actors in the security-versus-privacy conflict.

The full workshop report, including the abstracts of the talks, the biographies of the speakers, the slides of the presentations, and other materials, is available at HIDE’s Web site, <http://www.hideproject.org>.

2003, the Home Office-funded Crime Reduction Programme was the “biggest ever single investment in CCTV.”⁵ After this period of dedicated funding, the Home Office continued to develop CCTV initiatives using various funding streams not specifically dedicated to CCTV, as well as through local public authorities’ partnerships with private businesses.⁶ CCTV has been incorporated as a major arm of national policy to deter and prevent crime and disorder.

Philosophical, political, and legal debates have centered on a range of surveillance issues in which CCTV is implicated, many of which pertain to civil liberties and data protection. CCTV policy is an ideal venue for such debates because video recording

that the government’s adoption since the late 1990s of the evidence-based policy approach conflicts with the actual evidence of the impact of CCTV in the United Kingdom. Based on recent research into the use of CCTV, Webster identifies five categories of concern.

First, many studies cast serious doubt on the success of CCTV at deterring crime. Some even go so far as to deny the existence of *any* rigorous evidence to substantiate such a claim. Second, the use of CCTV may not be as widespread as some estimates suggest. In particular, Webster doubts one current estimate of approximately five million cameras nationally, although the Home Office refers to a similar estimate.⁸ However,

one study revealed only 21,000 cameras in use; moreover, many existing cameras are deployed in private settings. These privately owned and operated cameras are not deployed in coordination with the gov-

ernment. They have limited use for the state because data storage procedures and image quality vary even more widely with private cameras, and anything they record is only available postevent. Third, unequivocal public support for CCTV as a crime-reduction strategy is problematic. Public support depends on an assumption of CCTV’s effectiveness in curbing crime. With this in question, Webster wonders whether public support would really be so high. This is tightly related to his fourth concern: that public understanding of the full technological capabilities of CCTV is limited. And finally, the stated primary justification for using CCTV as a crime deterrent is belied by the government’s increasing use of cameras to achieve multiple objectives, including monitoring suspicious individuals and providing evidence for criminal prosecutions.⁹ He claims that a discussion about reconsidering the use of CCTV is warranted given “the

aging nature of current CCTV stock—many systems are now over ten years old—and the costs associated with their maintenance, upgrading and/or replacement.”¹⁰

A month after the Webster article was published, the Constitutional Committee of the House of Lords released a report, *Surveillance, Citizens and the State*. The report features 44 recommendations for surveillance policy, two of which address CCTV in particular. It also includes a volume of written and oral evidence gathered over a 20-month period. The committee’s task was to examine “the impact that government surveillance and data collection have upon the privacy of citizens and their relationship with the state.”¹¹ The governmental undertaking was spurred in part by the 2007 document from the Royal Academy of Engineering, *Dilemmas of Privacy and Surveillance: Challenges of Technological Change*, and a 2008 work written for the Information Commissioner, *A Report on the Surveillance Society*.¹² The latter was explored at length in a previous issue of *Dialogue* by McCarthy and Jacobsen.¹³

“A focus on the evidence of actual use, efficacy, and oversight of CCTV would certainly serve the broader discourse on surveillance.”

is both a familiar paradigm and a straightforward example of public surveillance. But the ease with which CCTV discussions fall in stride with general surveillance debates may limit direct attention to the particularities of CCTV. For instance, Fernandez and Huey recently noted that “social discourse on surveillance is shallow and uncritical at best, merging important but different types of surveillance as if they formed a universal project.”⁷ Those critical of the evidence base for CCTV are pushing these conversations toward a focus on evidence of actual use, efficacy, and oversight, and such consideration would certainly serve the broader discourse on surveillance in the United Kingdom and elsewhere.

Evidence-Based Policy-Making

In an article published in January 2009, William Webster—a lecturer in the Department of Management at the University of Stirling—argued

Surveillance: Citizens, the State, and CCTV

Of the 44 recommendations the Lords Constitutional Committee made in its report, six are relevant to the use of CCTV:

- The Home Office should commission an independent appraisal of the evidence regarding the effectiveness of CCTV to prevent, detect, and investigate crime.
- The government should introduce a statutory regime for public and private CCTV use and oversight, including a system for complaints and remedies.
- The Regulation of Investigatory Powers Act of 2000 should be amended to include judicial oversight for surveillance carried out by public authorities.
- The Data Protection Act of 1998 should be amended so that any new data collection or processing scheme

includes an independent and publicly available Privacy Impact Assessment (PIA) before its inception.

- The Information Commissioner's role should be expanded to include inspections of both public and private surveillance. The Information Commissioner should also be included earlier in future policy-making and legislative processes.

- A Parliamentary Joint Committee should be convened to address surveillance and data collection powers.¹⁴

In its discussion of these issues, the committee made a concerted effort to be evenhanded. For instance, in its discussion of public opinion and CCTV, the committee noted that while there was evidence of public support for CCTV, there was also evidence of public concern about the government collecting and using personal information. The committee noted that despite national legislation supporting "informational self-determination," CCTV surveillance and Automatic Number Plate Recognition are nonconsensual in nature, and thus, the impact of such activities on informational self-determination requires more extensive examination.

Several of the committee's recommendations call for more efforts at public education and engagement.¹⁵ The report speaks directly to the general concerns Webster outlined in his review, and it adds support from some government officials to the request for a critical reappraisal of CCTV that various scholars and professional organizations have also made. Yet the report is not without its critics. As special advisers to the committee, Raab and Goold pointed out

the structural limitations of the committee's investigation—for instance, "that the Committee had to focus on the *constitutional* implications of surveillance and data processing," and that the nature of the parliamentary inquiry process itself limits the possible scope and strength of the report's recommendations. Many such reports, they note, are influential, albeit usually incrementally and indirectly.¹⁶

Looking Forward

The inclusion of CCTV in the Home Office's family intervention program despite the increasingly critical analyses of its use raises concerns about the continuation of camera-based surveillance creep. Exactly how CCTV will be used in this program's expansion is still only a matter of speculation. In principle, its use could mean that families involved in the program would not need as much face-to-face contact with the program's public service personnel. But its deployment in this kind of program is also a marked change in public officials' use of CCTV, moving from monitoring public spaces to surveillance of personal family settings. Additionally, though it may fit under the umbrella of crime reduction and prevention, this program seems not to target crime directly, but antisocial behaviors that may or may not lead to crime. To be clear, the family intervention program may be a meritorious strategy in and of itself—the only concern is with the involvement of CCTV surveillance. And while it may be that CCTV policy in the United Kingdom has always sought to discourage not only criminal behaviors

but also antisocial ones, this represents yet another new implementation strategy for CCTV in the face of growing calls for reexamination of its purpose, use, and impact. CCTV may be neither as ubiquitous nor as efficacious as many commentators assume, but this is all the more reason for paying close attention to how and for what purposes it is used.

1. Home Office. Respect Family Intervention Projects Guide. 21 January 2009. http://www.asb.homeoffice.gov.uk/uploadedFiles/Members_site/Documents_and_images/Supportive_interventions/FIP_Respect_Projects_0026.pdf.

2. Ibid.

3. Ibid.

4. <http://www.camerawatch.org.uk/news/september-2009/cctv-for-problem-families.aspx>.

5. Gerrard G, Parkins G, Cunningham I, et al. National CCTV Strategy. October 2007. <http://www.crimereduction.homeoffice.gov.uk/cctv/National%20CCTV%20Strategy%20Oct%202007.pdf>.

6. Ibid.

7. Fernandez L, Laura H. Is resistance futile? Some thoughts on resisting surveillance. *Surveillance & Society* 2009;6(3):198-202.

8. McCahill M, Norris C. Working Paper No. 6: CCTV in London. June 2002. http://www.urbaneye.net/results/ue_wp6.pdf.

9. Webster W. CCTV policy in the UK: Reconsidering the evidence base. *Surveillance & Society* 2009;6(1):10-22.

10. Ibid., p. 10-11.

11. House of Lords Select Committee on the Constitution. *Surveillance: Citizens and the State. Volume I*. 6 February 2009. <http://www.publications.parliament.uk/pa/ld200809/ldselect/ldconst/18/1802.htm>.

12. Ibid.

13. McCarthy P, Jacobsen K. Surveillance in the UK: A view from the House of Commons. *Dialogue* 2008;1(3):1-4.

14. House of Lords Select Committee on the Constitution. *Surveillance: Citizens and the State*.

15. Ibid., chapter 8.

16. Raab C, Goold B. Putting surveillance on the political agenda: A short defence of Surveillance, Citizens, and the State. *Surveillance & Society* 2009;6(4):408-413.

HIDE Upcoming Events

- **26 February 2010**
Focus Group Meeting on Embedded Technology, Maastricht, the Netherlands
- **14 May 2010**
Focus Group Meeting on Privacy Enhancing Technologies, Manchester, UK
- **21 June 2010**
Focus Group Meeting on System Interoperability, London, UK
- **14 September 2010**
Focus Group Meeting on Technology Convergence, Paris, France

Recent Publications

- Erkin EZ, Martin F, Jorje G, et al. Privacy-preserving face recognition. *Lecture Notes in Computer Science* 2009;5672:235-253.
- Introna LD, Nissenbaum HF. Facial recognition technology: A survey of policy and implementation issues. Center for Catastrophe Preparedness and Response, New York University, 22 July 2009.
<http://ssrn.com/abstract=1437730>
- Irish Council for Biometrics. Biometrics: Enhancing security or invading privacy? Opinion.
http://www.bioethics.ie/uploads/docs/Final_Biometrics_Doc_HighRes.pdf
- Neyland D. Who's who? The biometric future and the politics of identity. *European Journal of Criminology* 2009;6(2):135-155.
<http://euc.sagepub.com/cgi/reprint/6/2/135>
- Riley C, Buckner K, Johnson G, Benyon D. Culture and biometrics: Regional differences in the perception of biometric authentication technologies. *AI and Society* 2009;24:295-306.
- Ryan R. The importance of biometric standards. *Biometric Technology Today*, July/August 2009, 7-10.
- UK Home Office. Keeping the right people on the DNA Database. Science and public protection. Summary of responses. Public consultation. 7 May–7 August 2009.
<http://www.homeoffice.gov.uk/documents/cons-2009-dna-database/>
- UK Home Office. Written ministerial statement. Home Office. DNA and fingerprint retention. November 2009.
<http://www.homeoffice.gov.uk/documents/cons-2009-dna-database/>
- UK Information Commissioner's Office. CCTV in schools. 6 November 2009.
http://www.ico.gov.uk/upload/documents/pressreleases/2009/schools_salford_061109.pdf

Centre for Science, Society and Citizenship
Rome, Italy

Centre for the Economic and Social Aspects of Genomics
Lancaster and Cardiff, UK

Centre for Biomedical Ethics—Yong Loo Lin School of Medicine
Singapore

Eutelis Italia SRL
Rome, Italy

Fraunhofer Institute for Computer Graphics Research
Darmstadt, Germany

International Biometric Group
London, UK

Optel Ltd
Woclaw, Poland

Sagem Sécurité
Paris, France

The Hastings Center
Garrison, NY, USA

University of Ljubljana
Ljubljana, Slovenia

Zuyd University
Heerlen, the Netherlands