

Life in a surveillance society—new challenges for DPAs and new challenges for business

Bridget Treacy, a partner in the Global Privacy Practice at Hunton & Williams, examines the new international accord on data protection enforcement

“Each time we give up a bit of information about ourselves to the Government, we give up some of our freedom.

For the more the Government or any institution knows about us, the more power it has over us. When the Government knows all of our secrets we stand naked before official power.” [Introductory remarks of Senator Sam Ervin on S3418, Legislative History of the Privacy Act of 1974.]

How often have we heard the challenge, from colleagues, management and friends, that data protection regulation is complex, theoretical, a barrier to business or, simply, irrelevant? Yet, as technology increasingly lies at the heart of how our society functions, more and more of our personal data are gathered and used, frequently without our permission and sometimes for purposes we could never have dreamed of. Unchecked, the power created by this accumulation of personal data can undermine the heart of our democratic and free society. Many Data Protection Authorities consider that we are now waking up to a surveillance society.

In this article, we examine what challenges the surveillance society poses for Data Protection Authorities and how these challenges will, in turn, affect the business world.

A wake up call

For some two years now Richard Thomas, the UK’s Information Commissioner, has warned us that we have been “*sleepwalking towards a surveillance society.*” He has painted for us a world in which our every move is recorded on CCTV or is capable of being tracked from electronic signals emitted from devices we carry; where everything we buy is recorded, profiled and stored on a computer in India; where those in official positions know who we are, whether our council tax is in arrears and what social services we consume. This is presented not as some dark, Orwellian warning, but as the reality of life in England in 2006.

At the 28th International Conference of Data Protection and Privacy Commissioners held in London in November 2006 (the “London Conference”), representatives of data protection and privacy authorities from across the globe went further: they warned that the so-called surveillance society is already with us and that we must now wake up to this new reality.

But what is the new reality? Is it just about surveillance? Although frequently arousing suspicion and creating mistrust, the ability to monitor individuals using surveillance tools is not entirely a negative activity. If undertaken proportionately, it can bring many benefits to society, not least the fairer distribution of resources and, in these times of increased fears of terrorism, enhanced security for our country.

Further, data protection regulation is not just about surveillance: it is about preserving for each of us the right to control what others know about us, our private lives and activities, our preferences, our beliefs and our past. It is as much about the right not to have our spending habits logged in the databases of shops, knowing when our bank or mobile phone operator sends our personal data abroad for processing, and the right not to receive unsolicited marketing material and telephone calls. Losing control over our personal information makes us vulnerable.

How is this right to control our personal data protected? At one level it is protected by law: in the UK by the much maligned Data Protection Act 1998 and, to a lesser extent; the Human Rights Act 1998. The reality, however, is that the protection comes not just from enforcement of this legislation but from the desire of all of us to conform with accepted norms of behaviour. Richard Thomas, the UK Information Commissioner, takes the view that “*Privacy and data protection are tested in two courts: the court of law and the court of public opinion. Ultimately, the court of public opinion is probably more important.*”

(Continued on page 4)

(Continued from page 3)

Response of Data Protection Authorities to challenges posed by the surveillance society

Some 58 data protection and privacy authorities participated in the London Conference. During their closed session, the Commissioners took as their theme the need to deal with the challenges posed by our surveillance society. As one aspect of this, the Commissioners discussed and reassessed their role as data protection regulators in securing and protecting data protection as a fundamental right.

There is perhaps a sense of déjà vu at the thought of further discussions by data protection regulators of co-operation and co-ordination of enforcement activity on an international basis. After all, similar sentiments were expressed at Montreux in 2005 and, prior to that, in 2004 the Article 29 Working Party issued a declaration on enforcement (12067/04/EN WP101). The latter identified reasons underlying the apparently low level of public awareness of data protection and focussed on the role of enforcement activity in increasing levels of public awareness. Ultimately very little of a concrete nature resulted from the paper although it did signal the possibility of pan European, cross sectoral enforcement activity, not dissimilar to the approach the competition authorities have taken. This has led directly to the current pan-European investigation into the processing of personal data by private healthcare providers, al-

though given the relatively small healthcare market in the UK, this is an initiative which has received limited publicity in the UK.

London initiative: “Communicating Data Protection and Making it More Effective”

—————
“Richard Thomas has signalled the arrival of a new mindset and a new breed of data protection regulator, keen to adapt their approach to make data protection more visible and to make better use of their opportunity, as regulators, to safeguard this fundamental right.”
 —————

The paper recognises the fundamental importance of data protection, identifies and analyses the key risks to this fundamental right, proposes co-ordinated activities for the supervisory authorities and proposes a new, common communication strategy.

The initiative was inspired by a recent survey undertaken in France which indicated that the majority of the French do not understand data protection. Similar survey results would no doubt be obtained in many other jurisdictions, including in the UK where data protection is

This time, there is a sense of greater resolve on the part of the Commissioners to look afresh at their role and to approach the discharge of their regulatory obligations on a more structured, comprehensive and collaborative basis. This is evidenced, in particular, by the joint initiative presented to the London Conference by the President of the French Data Protection Authority, Alex Turk, and supported by Richard Thomas and by the European Data Protection Supervisor, Peter Hustinx, entitled “Communicating Data Protection and Making it More Effective.”

frequently regarded as irrelevant or as overly theoretical. The danger, of course, with such a situation is that individuals give up their data protection rights too freely, without a proper understanding of the consequences for a democratic society. Indeed, in the Closing Communiqué of the London Conference, the Commissioners characterised privacy and data protection as being “*as precious as the air we breathe: both are invisible, but when they are no longer available, the effects may be equally disastrous.*” Once people give up their right to protect their personal information, the right cannot easily be reinstated.

In his paper, Alex Turk articulates three key areas of risk for data protection generally:

- the pace of technological change;
- concern with anti-terrorism; and
- reputational issues for data protection and for the regulators.

Pace of technological change

The pace of technological change is increasing at a rapid rate, making it difficult for regulation to keep up. In addition, technological change has resulted in other types of change, such as facilitating globalisation and the resultant international transfers of personal data. There are other, less positive consequences of the pace of technological change, such as ambivalence, ignorance or a lack of interest in the risks that the technology might bring. The proposed identity card database in the UK is an example, with many people unaware of what personal data the database will contain about them and who may have access to it..

Concern with anti-terrorism

The need to implement new measures to combat terrorism has led to many tensions. Whilst the Data Protection Authorities acknowledge the need for anti-terrorism policies and measures, the difficulty lies in finding the right balance and then

maintaining it, particularly in the face of subsequent attempts to use data for different purposes.

Reputational issues

The reputational issues concern both public perception of the laws themselves and of the Data Protection Authorities who enforce the laws. For many businesses and individuals, data protection laws are overly complex, difficult and abstract. The level of enforcement activity by local Data Protection Authorities is perceived as non-existent by many, largely due to the absence of high profile prosecutions.

Practical challenges raised by the London initiative

What practical steps will Data Protection Authorities take to address these issues? Two key strands of activity are proposed by Turk. The first is to co-ordinate strategies to enable Data Protection Authorities to act more effectively and more relevantly as a whole. As an integral part of this, there should be a greater emphasis on understanding, analysing and anticipating technological development. This could involve encouraging regulators to work alongside researchers within businesses and within the public sector with a view to raising awareness of data protection issues at an early stage of the development of new technologies. This mirrors the current approach of some businesses which regularly use impact assessments to analyse the implications for data protection within their organisations of new systems and technology.

Further, the London initiative urges Data Protection Authorities to assess their own effectiveness in regulating and enforcing data protection. Specifically, does each authority have an impact and make a real difference in practice? Turk anticipates that some authorities will claim that they lack sufficient powers and resources to be effective. This issue was raised by the Article 29 Working Party in their 2004 paper on enforcement (12067/04/EN WP101) following which the UK Information Commis-

sioner sought the power to issue “stop now” orders and also to be able to conduct audits without having to obtain prior consent of the target company.

In addition, authorities are encouraged to prioritise enforcement activity by reference to the seriousness of the behaviour and the likelihood of harm. There is also a warning here for Commissioners to refrain from being excessively rigid or purist on minor issues. Data protection regulation is often about how something is done, rather than whether or not it can be done. In other words, although often characterised as a barrier to doing business, compliance should really focus on how to act with least intrusion into the rights of individuals.

These thoughts reflect fairly closely the approach we have seen for a period from our UK Commissioner who seeks to prioritise his enforcement activity. His office emphasises education and is active in the provision of guidance. The Commissioner’s formal powers tend to be exercised only in the event of persistent or deliberate breaches of the Act (for example the Scottish National Party were found guilty of breaching the Act by using an automated system to cold call numbers listed with the Telephone Preference Service; recently a husband and wife were convicted on numerous counts of obtaining personal information unlawfully and selling it—see page 1). Further, within the UK we have seen a higher profile for data protection, not just because of the Commissioner’s enforcement activities, but because of a greater use of PR by his office to bring issues to the attention of a wider audience in the mainstream press.

The second key strand of activity outlined by Turk involves gaining further international recognition of the role of Data Protection Authorities and promoting the involvement of other stakeholders internationally.

Finally, and perhaps most significantly, Turk encourages the urgent development and implementation of a new communication strategy at both national and international levels.

How practical is the follow up and what can we expect? The paper lists a series of follow up activities including workshops on the following topics:

- strategic issues, including conditions for making Data Protection Authorities more effective;
- developing guiding principles for supervision;
- providing guidance on best practices for Data Protection Authorities and discussing the development of an international convention on data protection;
- communication, to explain the available tools and strategies and to coordinate campaigns across the regulators;
- enforcement, to cover monitoring and measuring compliance (including effective use of audit) and intervention;
- internal organisation of Data Protection Authorities with a focus on improving efficiency and effectiveness.

Significantly, a timetable has been set for these workshops and the issue is scheduled to be revisited at the Commissioners’ next workshop in 2007. Practical action on practical issues perhaps signals a change in attitude amongst the Commissioners to their role and a move to a more practical, less theoretical approach to enforcement.

What might the Data Protection Authorities’ new approach to enforcement mean for businesses?

Within the UK we have seen the Commissioner seek to promote good data protection practices and compliance with data protection regulation as a form of “enlightened self interest.” This has been evident from guidance which highlights for businesses the commercial advantages of maintaining up to date data (see, for example, the Information Commissioner’s guidance on buying and

(Continued on page 6)

(Continued from page 5)

selling customer databases—available by sending an email to docs@pdpjournal.com), Alex Turk's paper and subsequent discussion of this issue with Richard Thomas. In the Information Commissioner's Corporate Plan 2006-2009, one of three "top priorities" is to "strengthen public confidence in data protection by taking a practical, down-to-earth approach—simplifying and making it easier for the majority of organisations who seek to handle personal information well, and tougher for the minority who do not." The UK approach may well become a blue print for other Data Protection Authorities.

The approach itself recognises that there is a limit to what the law can achieve and encourages regulators to adopt a targeted approach to their enforcement activity. It is likely to result in a change in the current perception that some regulators have, to date, adopted an overly technical approach to compliance, punishing companies for technical breaches. The UK Commissioner takes the view that good data protection regulation is about addressing how activities are undertaken, and seeking to find a constructive solution to an issue, rather than having data protection characterised as a barrier to doing business.

The approach requires a greater level of awareness amongst the general public of data protection issues. Richard Thomas has indicated that the UK can expect to see his office continuing to issue specific, targeted guidance focusing on the "how" of good data protection. We can also expect to see a greater use of the media, including the mainstream press, to publicise and encourage wider public awareness and debate of data protection.

Such a strategy will raise the profile of data protection, not just in the minds of businesses, but in the minds of customers, who will be encouraged to think more carefully about who holds their personal data, what they do with it, and what rights they have in relation to those data.

Businesses can expect greater awareness of consumers of the extent to which their data are shared with

third parties or transferred abroad, perhaps in the context of an outsourcing arrangement. Businesses can also expect their employees to be more aware of the extent to which they are monitored in the workplace.

Currently, there are relatively few businesses for whom data protection lies at the heart of their business code of ethics. For the majority, their data protection strategy involves focusing on avoiding a breach of regulation, rather than proactively incorporating the key principles of good data protection into their corporate culture.

We may, perhaps, be witnessing the seeds of change on this issue as companies such as Hewlett Packard are taken to task, by the media as much as by regulators, for failing to take issues of data protection and privacy in the business world seriously. The fact that in Hewlett Packard's senior management were required to accept personal responsibility for intrusive surveillance techniques employed by the business, sends a powerful message. That message is all the more remarkable given that the issues arose in a jurisdiction (the United States) without the comprehensive data protection regime that we have in Europe.

For businesses which are frustrated by the lack of harmonisation in data protection laws between jurisdictions, including between the European jurisdictions, Richard Thomas is predicting a greater focus by regulators on harmonisation of key issues and on the practicalities of ensuring compliance across jurisdictions, rather than on seeking precise harmonisation across the European jurisdictions.

Finally, Richard Thomas has signalled the arrival of a new mindset and a new breed of data protection regulator, keen to adapt their approach to make data protection more visible and to make better use of their opportunity, as regulators, to safeguard this fundamental right.

The message for businesses is to take the issue seriously and to focus on the basic principles:

- why are you collecting the data?

- what are you going to use it for?
- is it accurate and up to date?
- for how long will you keep it?
- do individuals know this?
- are you planning to share it with third parties or send it abroad?
- are you satisfied that the data are adequately protected by appropriate security measures?

Those who fail to address these issues in a serious way may well find themselves at the heart of enforcement activity, where a targeted approach can mean that infringers are made more of an example, resulting in greater public criticism and reputational harm.

Bridget Treacy
Hunton & Williams
btreacy@hunton.com
