

Privacy laws 1987-2007 and beyond

James Michael and **Stewart Dresner** put some questions about data protection, past and future, to several of the international authorities on the subject who have been involved in it for at least 20 years, all of whom have spoken at PL&B conferences.

Here are the responses of Francis Aldhouse, former United Kingdom Deputy Information Commissioner and currently consultant solicitor at Bird & Bird; Peter Blume, Professor of Information Technology Law, University of Copenhagen; Dr David Flaherty, consultant and former Information and Privacy Commissioner, British Columbia, Canada; Masao Horibe, Professor of Law, Chuo Law School; and Peter Hustinx, European Data Protection Supervisor.

1. Twenty years ago, would you have predicted that data protection legislation has grown and spread as much as it has? Has the growth been more or less than you anticipated?

Peter Blume: First, my congratulations to Stewart and all the people who are or have been associated with PL&B during the first 20 years. Reading this newsletter is one of the best ways to keep up to date with the ever developing world of data protection.

The volume of data protection legislation is today much larger than I would have anticipated in 1987. At that time only few countries had comprehensive laws, and although a European Directive was contemplated it was not at all certain that it would become a reality. Outside Europe the situation was even more bleak, and the thought that countries such as Argentina, Australia and Canada would have federal laws was much more a hope than a probability. With respect to growth, these 20 years have been a success for data protection law.

David Flaherty: As a historian, I resist predicting the future, but I am astonished at what big business data protection has become, not only in a business sense, and necessarily so. With more than 40 countries in the data protection fold, it is becoming a global phenomenon, as it needs to be.

Advanced industrial countries without robust data protection laws and oversight agencies in place are now at risk of being branded as outlaws.

Masao Horibe: Please accept my sincere congratulations on 20 years of Privacy Laws & Business.

Twenty years ago, there were about 12 countries which enacted data protection acts. While I was writing a book entitled *Privacy in an Advanced Information Society*, which was published in 1988, I had a feeling that ideas of data protection would spread all over the world. The growth has been more than I anticipated because former socialist countries began to make laws in the 1990s and 2000s.

Peter Hustinx: Twenty years ago, the present number of national laws and initiatives around the globe was inconceivable. However, it fully confirms the continued relevance of data protection principles in a world increasingly dependent on widespread use of information and communications technology.

2. How has data protection changed from its international origin in the Council of Europe Convention?

Peter Blume: The centre of data protection has shifted from the Council of Europe to the European Union, but comparing the 1981 convention and the attached recommendations with the directives and connected EU law there are many similarities. Basically, the principles and the general structure of the regulation are the same but due to the legal setup of the EU, it has been possible to make the regulation more comprehensive and detailed. It is mainly in this way that the regulation of data protection has changed.

David Flaherty: I date the origins of fair information practice to the US and the UK in the early 1970s. I prefer to think of the phenomenon as a product of concern for the human rights and dignity of each individual, even though the push for legislation from country

specialists and privacy advocates has often masked the human rights concern beneath commercial imperatives for free trade that were more saleable. We will take our legislative victories anywhere that we can find them.

Masao Horibe: There have been some similarities and dissimilarities among data protection laws in the world. Those laws reflect the legal tradition and culture of each country. In some east Asian economies in particular, the system of data protection has changed from its international origin in the Council of Europe Convention.

Peter Hustinx: The origins in the Council of Europe Convention No. 108 and the OECD Guidelines are of similar importance internationally. The Convention has been specified in the EU Directive 95/46 [Recital 11] and the geographical scope of both has increased due to profound changes in the European landscape. The influence of the European model around the world has also been quite considerable. However, more important in my view is the growing emphasis on effective implementation, and inclusion of technological and self-regulatory approaches for better protection. This is necessary and inevitable to make sure that legal principles continue to be a practical reality in a changing world.

3. Are there any countries that you could identify as being particularly effective or ineffective at data protection in the content of the laws themselves, the interpretation of the laws or in law enforcement?

Peter Blume: The world is very differentiated with respect to data protection regulation and enforcement. Some countries, such as the EU Member States, have general and sectoral laws, some countries have only some sectoral laws and others do not have any laws. However, it is very difficult to compare, and it is well known that

there is no field of law with so many mistakes as comparative law. I will not pinpoint specific countries as better or worse than others. This is too risky. An example is that the level of sanctions is much higher in southern Europe than in Northern Europe, but this is not a sufficient indication of where data protection is performing best.

David Flaherty: Despite its plethora of specific legislation, the US and its states continue to do a very poor job at implementation because of the lack of institutionalised oversight agencies with an ongoing focus on the articulation of privacy interests at stake in any situation. I favour a generic oversight body rather than the sectoral approach in the US. While Canada is often held up as a model of effective implementation, I am only too aware of how much remains to be done to make privacy rights meaningful for the individual at the federal, provincial and territorial levels. If one looks around the world, the institutionalisation and implementation of privacy rights in most countries are quite weak or non-existent.

Masao Horibe: From the Japanese viewpoint, the data protection laws of many countries which implemented European Union Directive 95/46/EC are effective in terms of rules and law enforcement.

Peter Hustinx: It would not be appropriate or feasible for me to single out individual countries as particularly effective or ineffective. But from my previous reply, it follows that it would be those countries most – or least – successful in creating the crucial mix of elements that is required for making data protection a practical reality.

4. Some countries extend data protection legislation to legal persons as well as natural ones. Do you have a personal opinion about this question?

Peter Blume: Data protection concerns physical persons as they have integrity and a need of privacy. In my opinion, the extension of data protection rules to other entities such as legal persons blur the purpose of the regulation as the reasons for protection are very different. A physical person can feel shame and embarrassment; a legal person cannot. It may in some cases be practical that specific data protection

rules also cover legal persons, for example rules on credit reporting, but in general this should not be the case.

David Flaherty: Legal persons, as such, have no moral or ethical claims to privacy rights. Only the people who work there have such rights, and I regard the protection of employee privacy rights as another neglected area of data protection.

Masao Horibe: In the context of human rights, data protection legislation is closely related to the right of privacy and personal data of natural persons.

Peter Hustinx: There are legitimate reasons to include legal persons, but from a practical point of view, it is not a first priority. This is what most countries seem to have concluded. At this point, it is a typical non-issue.

5. What do you think are the most pressing issues in data protection today?

Peter Blume: Although it is tempting to mention international surveillance together with refined and complex new technologies, that is, pervasive computing, as the most pressing issues, I will prefer to focus on somewhat less spectacular issues. First, data sharing within the framework of e-government. Although we have stopped talking of Big Brother, he has not entirely disappeared, and it is a huge risk that e-government will create an environment where personal data are merged in one big database or network, providing the state full knowledge of its citizens, at the same time as processing is not at all transparent. Secondly, increasing the general public's knowledge of data protection. The survival of data protection in the long run depends on real support from citizens. This presupposes knowledge and much more effort should be put into explaining the reasons for and the rules of data protection.

David Flaherty: Getting privacy and data protection commissioners, and their staff, to do the jobs they were appointed to do in an expeditious, brave, and articulate way. In this regard, I have very high regard for the current work of the U.K. Information Commissioner and his office.

Masao Horibe: One of the most pressing issues in data protection is

how to develop international mechanisms of cross-border enforcement of privacy laws. The OECD Recommendation of the Council on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy will be adopted in spring, 2007.

Peter Hustinx: First of all, there is a continued great need to raise awareness and to ensure effective implementation of data protection principles. This is why the initiative adopted at the 28th International Conference in London in 2006 is entitled: "Communicating Data Protection and Making It More Effective". Secondly, the question how to deal with various new technologies, such as RFID and other building blocks of "intelligent environments". Thirdly, making sure that security concerns are not seen as necessarily overwhelming legitimate privacy interests. In my view, we need an integration of both in a sound world.

6. How, and when, do you think the issues of SWIFT and PNR between Europe and the US are likely to be resolved?

Peter Blume: I believe that these issues will be solved this year. Whether they will be solved in a satisfactory way is not at all certain. I will not guess what the solution will be. They will probably be different as it is my impression that citizens are more worried with respect to PNR than Swift. However in both cases the terror/crime argument that life is more important than private life will be persuasive. There will be restraints due to data protection but they will be modified.

Peter Hustinx: It will not be very easy in the short term, but there is a growing potential to think of these and other current issues in transatlantic relations, in a wider and more balanced perspective. The European Parliament is presently trying to set up a dialogue with the US Congress, which might be a good step. However, both issues are truly global and should be dealt with accordingly. Whatever happens in EU-US relations is therefore also an important benchmark for future arrangements.

7. What do you think data protection will be like twenty years in the future?

Continued on p.24

Continued from p.23

Peter Blume: In the next 20 years there will be many developments and they will be influenced by the fact that a greater proportion of the population only knows a digital world. It seems likely that the scope of data protection will have been limited so that it only will cover sensitive data. Article 6 [Principles relating to data quality] of Directive 95/46 will have been repealed. As there have been no major scandals, widespread surveillance is generally accepted. People think it provides safety. Privacy is not dead and in their own homes citizens want to be private. In public, data sharing is common and generally accepted.

David Flaherty: In 1987, I predicted that by the year 2002, data protectors were at risk of being individuals trying to hold back the flood of abuses with their finger in a dyke; I think the same risks will continue to exist into the foreseeable future because of the powerful forces of technological innovation, the inadequacy of resources to achieve robust data protection, the adoption of electronic health records (with the accompanying huge risks), and the ongoing digital revolution.

Masao Horibe: Developments in global communication networks will change the relationship of most economies in the world and most of them need data protection laws. At the same time, it will be necessary to harmonise them.

Peter Hustinx: Data protection will have been recognised as a core asset of democratic states based on the rule of law, and other states will follow similar principles to ensure and protect global information infrastructures, which have become essential in a highly integrated world environment. Multinational enterprises have a considerable leverage: “good client relations” and “seamless efficiency” could together make a good business case.

Francis Aldhouse: First, I congratulate Stewart Dresner and Privacy Laws & Business for twenty years of publishing its newsletters. The growth of the business over that period has been a mirror of the growth in public and organisational concern about privacy issues.

Look back to 1987 and remind ourselves of the concerns of Eric Howe, the first UK Data Protection Registrar. His Annual Report for that year, three years after the passing of the first UK Data Protection Act, told us not just of the mechanics of setting up a new office

and the registration system. More importantly it alerted us to the development of “massive collections of personal data” covering the bulk of the UK population. These databases were typically in the public sector, but the early enforcement action against the credit reference agencies demonstrated equal concern about the policies and practices of equally large private sector data processing schemes. At the same time, research showed that the general public attached great importance to the protection of individual privacy.

Twenty years on we seem to be faced with the same concerns: an identity card scheme, “spy-in-the-sky” vehicle tracking and other manifestations of the “surveillance society”. Citizens have, however, become sensitised to the issues and “identity theft” stories makes headlines in a way they did not twenty years ago. Should we look to the future with optimism or not? Every modernising initiative by government seems to propose another invasion of privacy – justified either by public security or efficiency of public administration. But the public and their representatives are fighting back and perhaps the wave of “breach notification” laws across the US is a sign that all is not lost.