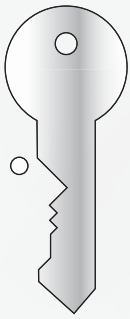
2011.hu

PL2011.eu



International
Data Protection
Conference

2011

TABLE OF CONTENTS

Foreword 4

Róbert Répássy: Welcome speech at the International Data Protection Conference in Budapest 6

Françoise Le Bail: Keynote speech: Reform of the data protection rules 10

Aurora Mejía: Keynote speech of the Budapest Conference 12

Peter Hustinx: Where we are now and where we are heading - current and future dilemma's of privacy protection 16

Janni Christoffersen: Cloud computing – a challenge to data protection? 20

Urszula Góral: Educational activity of the Polish Data Protection Authority 24

Professor Paul De Hert: From the Principle of Accountability to System Responsibility – Key Concepts in Data Protection Law and Human Rights Law discussions Summary 32

Endre Győző Szabó: New data protection principles in light of the debate on Council conclusions 35

Christopher Kuner: Global standards for data protection and privacy from the business point of view 38

Jörg Polakiewicz: Convention 108 – still going strong after 30 years? 42

Attila Péterfalvi: Closing speech of the budapest conference 47

Wojciech Rafał Wiewiórowski: Privacy and the Liability of Intermediary Service Provider in the Clouds. E-Governmental Aspects 49

Jörg Polakiewicz: Keynote speech of the Warsaw Conference 60

Jacob Kohnstamm: Effectiveness of personal data protection principles in the changing world 62

Eng. Wacław Iszkowski, Dr. T.S.: Illusion of Personal Data Protection? 64

David Wright: The state of the art in privacy impact assessment 69

Daniel Drewer: A tailor-made data protection framework for the European Police Office 77

Graham Greenleaf: The influence of European data privacy standards outside Europe: Implications for globalisation of Convention 108 Summary 79

Jean-Philippe Walter: The modernization of the Convention of the Council of Europe for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108): moving from a European standard towards a universal standard for data protection? 81

Annex 87

Professor Paul De Hert: From the Principle of Accountability to System Responsibility – Key Concepts in Data Protection Law and Human Rights Law discussions 88

Graham Greenleaf: The influence of European data privacy standards outside Europe: Implications for globalisation of Convention 108 121

Programmes of the data protection conferences 154

FOREWORD

Where are we now and where are we heading? – this question was asked by the topic-raising document prepared for one of the conferences of our data protection project, to be closed by this publication. With our partners, the Ministry of the Interior of Poland, the Polish Data Protection Authority (GIODO), the Ministry of Justice of Spain, the Council of Europe, the Academy of European Law and the Office of the Hungarian Data Protection Commissioner, we were seeking answers in three consecutive conferences to several issues that are related only to data protection in the narrow sense of the term, but in a broader context, they relate to several activities of economy and governance. During the term of the Hungarian Presidency we afforded special attention in the field of home affairs and justice to data protection and treated it as a priority in Council work. The project gave us an excellent opportunity to discuss the current issues with academic representatives, the experts of the subject.

The data protection framework of the European Union is going to be renewed comprehensively. The process of globalization, the emergence of new technologies, as well as the entry into force of the Treaty of Lisbon all require a review of the legal framework.

The Directive of the European Union on data protection serves the protection of the individual and the free flow of personal data in the entire territory of the Union. It is expected that these two fundamental objectives will remain the focus of the future regulation as well. The lectures of the conferences also underpinned the concept that a stronger legislative harmonization would serve both protection of the rights of the individual and the free flow of data better than the current fragmented regulation that varies significantly by country.

In the field of protecting the rights of the individual, the European Union should not set any other aim than to extend the data protection norms guaranteed within its own borders to data management regimes that affect third countries or to cases where data are forwarded to countries outside the Union. For that purpose, it has become urgent to explore the opportunity provided by the Convention of the Council of Europe, furthermore, ultimately the development of global benchmarks. This work is now in progress, and obviously, the European Union must take the initiative in this field.

The sociological effects of global information society and its impact on public life could affect the lives of current and future generations to an extent not yet known. As deep as these impacts may be, concerning the handling of personal data we must never lose sight of our original objective: the

protection of the individual and human dignity. The exercise of individual rights should be enabled in a global environment as well, for that purpose, while maintaining the current level of protection, legal regulation should be adapted to the new conditions to the necessary extent.

In addition to a global outlook, the European Union should develop a data protection regime that focuses on and serves its own objectives. Economic considerations call for a smoothly operating internal market without obstacles, within that data protection regulations ensuring the flow of data. The conferences have validated both the necessity and the feasibility of that.

Our publication presents the written transcripts of selected lectures from the conferences organized under the project. I trust that the readers of this volume will find useful and interesting ideas in the publication. I would like to thank everyone who helped us with the completion of the project for their support and efforts.

Tibor Navracsics
Deputy Prime Minister
Minister of Public Administration and Justice

WELCOME SPEECH AT THE INTERNATIONAL DATA PROTECTION CONFERENCE IN BUDAPEST

Róbert Répássy
Minister of State responsible for Justice

By the middle of the year the Hungarian Presidency hands over the presidential duties of the European Union to Poland, both symbolically and in reality. During these weeks it already seems timely that we should draw up some kind of balance based on the achievements of the recent period. Topics of our conference focus around the legal environment protecting the private sphere of the individual, more specifically the assessment of the implementation of the right to the protection of personal data. Nevertheless, please let me give you a brief summary of the efforts of the Hungarian Presidency in the field of justice.

In January the Hungarian Presidency took over the presidential duties from Belgium with the firm belief that if we managed to make the European Union stronger during our term, all the twenty-seven member states would benefit from it, including Hungary. We did not intend to enforce our interests from the position of the Presidency, on the contrary, we used our Presidency to promote common European interests. It is a great pleasure to see that this approach proved to be not only honest, but also effective in many areas.

If I had to give a list about the priorities of the Hungarian Presidency in the field of justice, I would mention the following and would be pleased to give an account of the progress made in the individual areas.

- In order to implement the fundamental rights more efficiently, we support the accession of the European Union to the European Human Rights Convention. The preparation phase consisted of three negotiation rounds, and during the term of the Hungarian Presidency we managed to conclude the expert level negotiations;

- Also arising from our commitment to fundamental rights, we afford special attention to the first annual report on the implementation of the Charter of Fundamental Rights. Concerning the more efficient implementation of the rights contained in the Charter, we adopted Council conclusions;

- In order to alleviate the administrative obstacles making the implementation of rights in everyday life more difficult, we put on the agenda the questions raised in the communication of the Commission on the implementation of EU citizenship rights;

- It goes without saying that the protection and assistance of citizens victimized by crime was one of our priorities. In the field of protection of victims, the Council approved by means of a resolution the Hungarian Presidency's roadmap which provides determining guidelines on the efforts of the Union in this field, in relation to the Commission's victim protection package;

- Also in the field of cooperation in criminal law, we managed to make progress concerning the directive on attacks against information systems; in the Council meeting held in the middle of June, the ministers approved a general approach;

- Regarding the draft directive on combating the sexual abuse, sexual exploitation of children and child pornography, the so-called trialogues with the European Parliament are in progress and the enactment of this piece of legislation is now within reach;

- Concerning the general part of the legislation aimed at creating the European Investigation Order, we have reached a general approach in the Council.

- As regards participation in criminal procedure, we intended to make progress in the field of relevant legislation uniformly applied in the Union, by accepting the draft on the right of the accused to information. Concerning this dossier, the trialogues conducted with the European Parliament are progressing well;

- The Hungarian Presidency's intention has been to promote the adoption of the succession law regulation, which will mean a new accomplishment in the Union level unification of rules of private law, creating the "free traffic" of resolutions adopted on matters of succession between member states. In their road to the accomplishment of the dossier on succession law, the last meeting of the Council brought a very spectacular result: a compromise was reached concerning the most important political issues;

- In order to ensure implementation of the provisions of the Charter of Fundamental Rights as much as possible in the everyday life of EU citizens, the Hungarian Presidency afforded due attention to personal data protection, as a fundamental right identified by the Charter. In response to the Commission's communication issued in the field of the protection of personal data in November 2010, we adopted Council conclusions in the February meeting of the Council.

In Hungary in the field of personal data protection we have traditions going back to times before the political changes. Our Civil Code has contained provisions on the protection of an individual's image since 1977. Our data protection law has a tradition of almost two decades and the institution of the Data Protection Commissioner goes back to one and a half decade. In the field of personal data protection Hungary quickly got involved in the various European processes. This is spectacularly demonstrated by the fact that in the year 2000 the Commission stated in a resolution that in the field of personal data protection Hungary is providing an adequate level of protection with regard to relevant EU standards. Thanks to that, four years prior to its accession to the Union, Hungary had been considered, in terms of data transfer, a state not treated as a third country. The attention of the Hungarian state has not been diverted from this field since the time of our EU accession, either. It was after such preliminaries that we adopted the protection of personal data as one of our priorities, and the idea of organizing a conference came up quite naturally.

Preparations for the future legislation replacing the current data protection directive are in progress, although no Commission proposal has been adopted yet during the Hungarian Presidency. In response to the Council's communication released last November, on the proposal of the Presidency, in February this year we summarized the positions taken by the member states concerning the issues raised by the Commission in Council conclusions. At the beginning of the Presidency we also looked forward to the negotiation then starting between the European Union and the United States of America, aimed at preparing a framework agreement on the protection of personal data, which would serve the implementation of every

data exchange agreement aimed at the prosecution of crime. The negotiations are in progress under the leadership of the Commission as the chief negotiator. In addition to these, we also monitored the process of the review of the data retention directive then kicking off, which raises complex legal and legal policy issues. The commitment of Hungary to issues on data protection will remain after the end of our Presidency, and we look forward to continued cooperation in this field.

The enhancement of fundamental rights and the efficiently operating judicial area are connected to the subjects of the conference in a unique manner. We all make an effort to operate our national justice administrations efficiently and also to ensure that the cooperation with our international partners in this field should be smooth. The European Union provides an excellent framework for that. Data exchange in the judicial area is based on trust, which stems from the fact that the other member state takes as much care to protect the privacy of individuals as the state providing the data. The data protection directive is based on this principle, and ultimately this is what enables the smooth handling of data exchange operations also serving the safety of citizens. Therefore a good data protection regulation should have beneficial effect on the safety of our citizens as well.

The Charter of Fundamental Rights contains the right to protection of personal data and provides remarkable institutional protection for it: every member state is required to establish its data protection authority in charge of controlling the implementation of this right. That way a unique and efficiently operating network of national institutions in charge of the protection of a fundamental right has been established in Europe.

I consider it important that all circumstances affecting the implementation of the right to personal data should be discussed. Globalization and the dissemination of new technologies have led to a change in our lifestyle. The communication network reaching every point of the world and the application of tools of information technology are leading, by necessity, to a kind of global uniformization. Hooking up to the network is sometimes only an attractive opportunity, at other times it is almost a must. The development of a global virtual social network seems unstoppable.

However, we may not necessarily welcome an inevitable process without criticism. The uniformization of behaviour patterns and communication habits raises the necessity of legal regulation applying to every point of the world, with a level of intensity unknown before.

However, the protection of the individual also requires national efforts which could promote guidance closest to the citizens in getting information and exercising rights.

In order to protect the individual, we support joint European action, as this is the only chance to ensure that the area based on the implementation of the law should not show a fragmented picture, rather, the appropriate level of protection should be coupled with legal certainty, concerning both the data subjects and the participants of the economy.

I am convinced that the attempt of developing global standards is a task in which Europe should be a leader. The opportunity of developing the data protection Convention of the Council of Europe into a global standard deserves special attention, just as the Spanish initiative hallmarked by the so-called Madrid Standards does.

The flow of personal data at European and global level is a natural consequence of globalization. Nevertheless, lowering the standards of personal data protection for this reason would not be acceptable in the development of our international relations. We cannot watch idly any process leading to the erosion of the protection of the individual. The traditionally well-developed European data protection regulation is a value to be preserved.

KEYNOTE SPEECH: REFORM OF THE DATA PROTECTION RULES

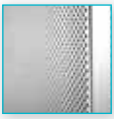
Françoise Le Bail
Director General of the European Commission, DG Justice

Following the Commission's communication in November 2010, which outlined our thinking on the envisaged data protection reform, the Council conclusions adopted under Hungarian Presidency in February have given focus to the EU-internal discussion on this subject.

As stated in the preambles to those Council conclusions, "the time-honoured data protection principles laid down in [existing] EU legislation are still valid and must be respected in all future legislative acts but […] emerging business and technological developments in the last fifteen years require [their] thorough evaluation […]".

The Conference marks perhaps one of the last stages of this evaluation and analysis, which will usefully feed the preparation by the Commission of legislative proposals beginning of 2012.

The subjects of the working sessions to be held also closely mirror key priorities of the reform that were identified in the Commission's communication and built upon by the Council conclusions, namely: further advancing the internal market dimension of data protection, strengthening individuals' rights in the face of technological change; better enforcement of data protection rules; and strengthening the global dimension of data protection.



Let me give a broad outline of the Commission's goals:

- We want to achieve a higher level of protection for individuals and greater harmonisation in the EU as well as legal certainty, which will be a benefit for individuals, public authorities and economic operators.

- At the same time, a revised data protection regime should keep bureaucratic and financial burdens to a minimum. We want to cut red tape and eliminate those administrative obligations that are unnecessary and ineffective.

- Individuals' rights should not remain abstract; they must be strengthened in practice, especially when faced with the challenges of an Internet economy and rapid technological innovation. For instance, where individuals have to give consent for data processing, this should always be meaningful.

- Regarding governance and oversight, the powers of national data protection authorities should be strengthened and harmonised in order to ensure effective enforcement of data protection rules. Given the increasingly global nature of data protection issues, we need greater coordination between data protection authorities at European level.

- Better enforcement of data subject rights is a key aspect of our reform. Beyond the importance of reinforcing data protection authorities and better harmonising their powers, I take

advantage of the presence of the Ministry of Justice to also underline the importance of rapid access to judicial redress and effective sanctions for any infringement of the data protection rules.

- Last but not least, looking again at the global dimension, we need to streamline and strengthen current procedures for international data transfers. Let me give you one concrete example.

- We want to encourage global approach for companies to ensure the protection of personal data. "Binding corporate rules" have proved to be a useful model for international transfers and we want to build upon this model. Cloud computing becomes a reality and we need adapted solutions to address it.

Clearly our detailed proposals on all these issues have yet to be finalised and agreed. I just wanted to give you a foretaste of the direction we are working in within the Commission. The Commission is looking forward to being able to table a legislative proposal beginning of 2012.

KEYNOTE SPEECH OF THE BUDAPEST CONFERENCE

Aurora Mejía
Director General for International Legal Cooperation and Religious Affairs, Ministry of Justice, Spain

Spain has been working closely together with Belgium and Hungary as partners within the framework of the *Trio of Presidencies*. Our Justice and Home Affairs Trio Presidency programme (January 2010 - June 2011) already addressed data protection. The programme states the following:

- "*The Lisbon treaty provides for a horizontal legal basis regarding the protection of personal data. Depending on a possible legislative proposal to be proposed by the Commission, the objective of the three Presidencies will be to further develop a consistent legal framework applicable in all EU fields to the processing of personal data both in the Member States and by EU institutions. Within this legal framework, specific rules will be needed regarding judicial cooperation in criminal matters and police cooperation…*"

- "*…The EU should develop a proactive and consistent approach of data protection in the relations with third States. In this regard, on the basis of the proposition of the Commission, the three Presidencies will negotiate a data protection and data sharing agreement with the United States of America, achieving the work carried out by the EU-US high level data protection group, in particular concerning the right of judicial redress for European citizen in the United States.*"

Prior to that, the *Stockholm programme* had already acknowledged the need to protect citizen's rights in the information society "*When it comes to assessing the individual's privacy in the area of freedom, security and justice, the right to freedom is overarching. The right to privacy and the right to the protection of personal data are set out in the Charter of Fundamental Rights. The Union must therefore respond to the challenge posed by the increasing exchange of personal data and the need to ensure the protection of privacy. The Union must secure a comprehensive strategy to protect data within the Union and in its relations with other countries…*"

Our societies are moving forward faster every day and therefore challenges regarding data protection evolve and change continuously.

Nowadays, for example, the growing use of the *Internet* by the European citizens is an area in which threats to privacy rights may very easily arise. Internet provides an opportunity for the development of services widely used by millions of citizens, but these citizens must have their rights and guarantees protected.

Another field in which the protection of personal data is crucial is that of *medical records*. In our legal systems heath-related data are among those specifically taken into account to which a strengthened protection regime is applied.

Finally, I would like to refer to the *international transfer of data* which is growing due to the globalisation of the economy; and this transfer is not only growing but it is also becoming more diversified, due to the fast development of emerging economies. In our case the main geographi-

cal areas to which data are transferred to from Spain are Latin-America, followed by the United States and Asia.

Where can the *answers* to these threats lie? *Legislation and harmonization* seem to be the best solution.

DATA PROTECTION IS HIGHLY DEVELOPED IN EUROPE.

The harmonization of our legal framework seems inevitable. This harmonization takes place at different levels. I would therefore refer in brief to the work done at the EU, to the work by the Council of Europe and finally, to the so called Madrid Standards.

Focusing on *EU level*, the Lisbon treaty provides a new legal basis for data protection. In particular, Article 16 of the Treaty on the Functioning of the European Union expressly recognises the right to the protection of personal data and provides for the adoption of new legislative provisions in three areas:

- the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies,
- the protection of individuals with regard to the processing of personal data by Member States when carrying out activities which fall within the scope of Union law,
- the free movement of such data.

"Article 16 TFUE (ex Article 286 TEC)

1. Everyone has the right to the protection of personal data concerning them.

2. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.

The rules adopted on the basis of this Article shall be without prejudice to the specific rules laid down in Article 39 of the Treaty on European Union."

Further to that, the European Union is based on the respect for fundamental rights and article 8 of the Charter of Fundamental Rights of the European Union expressly recognises the fundamental right to the protection of personal data.

On the other hand, Article 39 of the Treaty on the Functioning of the European Union, under the chapter on "Specific provisions on the common foreign and security policy", also foresees the adoption of a new legal framework.

The central piece of legislation is the '95 Directive.

In the area of police and judicial cooperation in criminal matters, the capital EU instrument is Framework Decision 2008/977/JHA. It can also be mentioned that in July 2011, the main conclusions of the Commission recently adopted evaluation if the Data Retention Directive[1] were also disclosed and that options for the future in this are being explored.

Likewise, instruments in the framework of police cooperation have an impact on the data protection system. On the one hand, at international level, it can be recalled that EU bilateral agreements with the USA, Canada and Australia on the transfer of PNR (Passenger Name Records) are being negotiated, the implementation of the Agreement between the EU and the USA on the processing and transfer of Financial Messaging data for the purposes of the Terrorist Finance Tracking Program (the famous TFTP) as well as the negotiations for an agreement between the EU and the USA on protection of personal data when transferred and processed for the purpose of preventing, investigating, detecting or prosecuting criminal offences, including terrorism, in the framework of police cooperation and judicial cooperation in criminal matters. On the other hand, at EU level, a proposal for a Directive on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime is currently being discussed.

The Commission is in the process of reviewing the general EU legal framework on the protection of personal data, with a view to:

- modernising the legal system, in particular, to meet the challenges resulting from globalisation and the use of Information and Communication Technologies,
- strengthening individuals' rights, and
- improving the clarity and coherence of the EU rules.

We are awaiting, therefore, with great interest the new proposal by the Commission on this area which will build upon their November 2010 Communication on "A comprehensive approach on personal data protection in the European Union" as well as upon the Conclusions adopted by the Council in February 2011, already under the Hungarian presidency, mentioned by the State Secretary, which confirmed that *"…Within the scope of European Union law, a new legal framework based on the comprehensive approach should guarantee that appropriate data protection standards are complied with in all areas where personal data are processed…"* while *"…Shares the view expressed in the Commission communication that the notion of a comprehensive approach to data protection does not necessarily exclude specific rules for data protection for police and judicial cooperation in criminal matters within this comprehensive protection scheme and encourages the Commission to propose a new legal framework taking due account of the specificities of this area…"*

Secondly, the 1981 *Council of Europe* Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data - in force since 1985 and supplemented by an additional protocol, which entered into force in 2004 - is a landmark. Its 30th anniversary, celebrated on 28 January 2011, confirmed it as a cornerstone of privacy and personal data protection in Europe. The challenges in Information and Communication Technologies together with changes in the nature and volume of personal data flows made necessary to establish a legal framework which brought together trans-border data flows with fundamental rights.

And last but not least, the *Madrid standards* adopted in November 2009 try to overcome problems caused by the existence of different data protection regimes around the world. They aim at promoting data protection and privacy at international level by establishing principles and rights that constitute the minimum standards to be respected by all countries, while facilitating a satisfactory exchange of personal data, which is an essential tool in order to guarantee security of our citizens and to remove undue obstacles for entities and competence. The standards try to establish a universal model of what should be understood to be an appropriate level of data protection, thus enabling transfers with fewer formalities among the countries that hold this model.

To conclude, I would like to highlight once more the relevance of data protection issues in a globalised world and the pivotal role they play for the development of an area of freedom, security and justice in Europe. We have to address this call for striking the right balance between the necessity for increased exchange of personal data whilst ensuring the utmost respect for the protection of privacy.

ENDNOTES

1 Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC

WHERE WE ARE NOW AND WHERE WE ARE HEADING - CURRENT AND FUTURE DILEMMA'S OF PRIVACY PROTECTION

Peter Hustinx
European Data Protection Supervisor

The European Commission had originally planned to submit its proposals for a comprehensive review of the EU legal framework for data protection before this conference. In that case, the conference would have provided a first occasion to jointly reflect on these proposals. However, the Commission has slightly rescheduled its work and its proposals are now expected around the end of 2011.

This delay also gives more space for reflection on the general context of the current review and on the two most strategic questions in this context: 1) why are we having this review of the EU legal framework for data protection, and 2) what are our expectations as to its results?

FIRST: WHY THIS REVIEW?

To answer the first question, we need to consider the state of the current EU legal framework for data protection, as well as the developments that took place since its adoption.

The key instrument of the current EU legal framework - the general Data Protection Directive 95/46/EC - was no doubt a great achievement. It has an impressive history building on human rights' protection in the Council of Europe and different member states. In that context, let me also mention the pioneering role of Hungary in Central and Eastern Europe in the late 1980's and early 1990's.

The initial results of the Directive were also impressive, both in bringing greater consistency in the national laws of the EU member states and in spreading the practice of data protection in a much greater part of Europe. Among the achievements of the Directive, we should also mention its impact on many third countries and the global discussion as a whole.

However, the truth is that the Directive is now also approaching its "final consumption date". It is starting to show its age and it is clearly not sustainable for a longer period. When the Directive was adopted in 1995, the Internet was still hardly visible and in any case far from its present highly dynamic reality. We now live in a world that is increasingly global, internet driven and dependent on the wide spread use of ICT in all areas of life, including the most private and intimate ones.

That means that there is not only a need for modernisation, but also an urgent need to ensure that the principles of data protection continue to be fully effective in a changing world. Let me emphasize that "effectiveness" is not only required in a legal sense, but also and most of all, in practical sense: legal safeguards are only effective if they are applied in practice, and provide the required protection where it is really needed.

As an additional problem, we now also see an increasing diversity of national and European measures, both within and outside the scope of the Directive. This diversity is increasingly unhelpful and calls for more harmonisation and more comprehensiveness, and more generally for an urgent streamlining of unnecessary complexity in the current data protection landscape.

Another important factor can be referred to as the "impact" of the Lisbon Treaty. The Treaty has provided a strong legal basis for comprehensive data protection, covering all areas of EU policy, including those outside the former First Pillar. The Treaty has also redistributed the roles of the Commission, the Council, the Parliament and the Court of Justice, particularly in the former Third Pillar. Both have led to dynamic effects in the context of the review and explain that Data Protection is now at the heart of the EU policy agenda.

A third element is that data protection has now become such a relevant factor for other important policy fields that it can somehow be described as a critical success factor for those other policies. Data protection plays a key role in the Stockholm Programme as a vital source of legitimacy, trust and confidence, and therefore also effectiveness, in the cooperation of the EU member states in the Area of Freedom, Security and Justice.

Data protection also plays a crucial role in the Digital Agenda. This is one of the "flagship initiatives" of the Europe 2020 agenda for "smart, sustainable and inclusive growth". Of course, that vision also needs a smart, sustainable and effective new legal framework for data protection in the future Information Society of 2015, 2020 and beyond.

Finally, there is an increasing global attention for more effective data protection. Let me just refer to the activities of the OECD, the recent initiatives in the US and the final declaration of the G-8 meeting in May, where *"effective protection of personal data and individual privacy on the Internet"* were explicitly mentioned as *"essential to earn users' trust"*.

All this adds up to a major window for more effective data protection, provided we use these different opportunities well.

So, taking stock of where we are now, it is fair to say that the Commission's Communication of November 2010 was generally well received. The Council has expressed overall support under Hungarian Presidency, and the Parliament gives strong support in the Voss Report that was widely endorsed in the LIBE Committee.

It is now more essential than ever that the Commission comes up with ambitious proposals that will meet the high expectations created by Vice-President Reding and provide a sound basis for more effective protection in the years to come. So let me now turn to our expectations as to what this could entail.

SECOND: WHERE ARE WE HEADING?

First of all, the strong emphasis on a "comprehensive approach" means that all fields of EU policy will be covered, including those of the former Third Pillar, i.e. notably police and justice. This is very welcome for different reasons: it will lead to a more horizontal approach without distinctions between different policy fields that not fully correspond with reality.

This approach is in line with the Lisbon Treaty that clearly mandates a horizontal and comprehensive approach. The present rules for police and justice are a patchwork of specific rules and a general framework of limited scope as it *only* applies to data flows *between* member states. A more comprehensive approach is therefore likely to lead to better rules overall.

Secondly, it should be clear that this is not the time to reinvent data protection. It has been invented and now recognised as fundamental right in the Lisbon Treaty. Instead, much attention should be given to making data protection more effective in practice.

This means a greater focus on implementation and enforcement of data protection principles and on the delivery of data subject's rights. A related concern is that some existing formal requirements could be simplified or abandoned, if they are no longer needed for effective data protection. The notification of data processing to supervisory authorities is a clear example of such a requirement.

Another point in this context is the need for greater harmonisation of rules across the EU. The present diversity of national rules - even within the scope of the Directive - is not helpful for effective data protection, and quite frankly counterproductive.

Let me emphasize at this point that a strong emphasis on the "internal market" perspective is not only good for international business and cooperating governments, but also for data subjects that increasingly move around the EU, and for the effectiveness of data protection in general. In spite of all good intentions, the present fragmentation of rules is likely to result in the opposite.

Thirdly, more effective data protection also requires a strengthening of the three main roles in data protection: those of the data subject, the controller and the supervisory authority. Data subjects should be enabled to exercise their present rights more easily and should be given a few additional rights to protect their interests where needed.

An interesting example is the right to require that personal data are deleted or transferred to another provider – the "right to be forgotten" or the "right to data portability" – which might be particularly useful in the context of social networks or other online services.

Strengthening the rights of data subjects would also require a clarification of the situations where consent is required and the conditions that have to be met for valid consent. A lack of clarity about this often leads to a weaker position of data subjects, particularly in the online environment.

Data controllers are now responsible for compliance with data protection rules, but in practice this often only leads to formal arrangements and responsibility "at the end" if something goes wrong. Instead, they should be mandated to be more active and to take all those measures which are necessary to ensure that data protection rules are complied with. This is referred to as the "principle of accountability" that would require data controllers to be able to demonstrate that they have taken all appropriate measures to ensure compliance.

This requirement should of course be related to the context and "scalable" to avoid undue burdens for small and medium enterprise. The principle of "privacy by design" would fit in the same approach: controllers should be able to demonstrate that appropriate measures have been taken to ensure that privacy requirements have been met in the design of their systems.

Supervisory authorities should be given adequate resources and stronger powers of enforcement that are equivalent in all member states. Supervisory authorities should also be allowed to use these powers more strategically, including the possibility to be more selective (e.g. in the case of substantial risks or systematic wrongdoing).

At the same time, the conditions for "complete independence" should be equivalent in all member states. This means that the judgment of the European Court of Justice of 9 March 2010 in case C-518/07 (*Commission v Germany*) is taken as a benchmark: data protection authorities "*should be free from any - direct or indirect - influence in the exercise of their duties*". These conditions are also essential for effective cooperation in cross-border situations.

Let me also highlight here that the Court in *Commission v Germany* has clearly stated that "complete independence" is not inconsistent with the principles of democracy and legality. It specifically mentioned that parliaments can provide for adequate legal frameworks, including transparent procedures for appointment and annual reporting on activities, so as to ensure a structured dialogue between independent authorities and governments or parliaments.

However, in case of legislative change, this may require special rules for transition, so as to avoid that a change of existing conditions may amount to - or be perceived as - an interference in ongoing procedures.

A legal framework that would provide all of the above elements would be much better in the position to deal with the challenges of technological change and globalisation.

The growing international dimension would ideally require a global consensus on data protection principles and standards. Although this global consensus is developing in practice, it is still far from perfect.

It is therefore also important to clearly define the external scope of EU data protection law. The concept that EU law should also apply where EU consumers are "targeted" - or more in general where services are provided to EU consumers - seems to attract more and more support.

It would also be important to simplify the present requirements for data transfers to third countries. The process for the approval of binding corporate rules (BCR) could be mentioned as an example.

All this may well happen by 2014, i.e. towards the end of the current mandates for the Commission and the European Parliament.

In the meantime, we should apply the existing rules more effectively. We should continue the current growing focus on compliance and enforcement, both at national and EU level. In the latter case, this might mean that more member states will be involved in infringement cases before the Court of Justice. We should also continue to ensure that privacy is "built in" in new legislation, new policies and new technology as far as possible.

Finally, we should continue to develop a close international cooperation, both inside Europe and beyond, as this will be required in a globalising world where effective data protection will continue to play a key role in ensuring the well being of our citizens.

CLOUD COMPUTING – A CHALLENGE TO DATA PROTECTION?

Janni Christoffersen
Director, Danish Data Protection Agency

Companies and private entities of varying size as well as the public sector are very interested in getting to know more about cloud computing and how to use it to cut their costs on computing resources. As a consequence, Danish politicians and the Danish media are taking quite an interest in this topic - so cloud computing is very much on the IT-agenda in Denmark right now. And with this short presentation I would like to share with you some experiences and challenges of cloud computing seen from our perspective – in the Danish DPA – up until now.

First, I would like to talk a little about the specific questions that we have identified and focused on in handling the cloud computing cases – and one could ask this key question: is cloud computing a new challenge to data protection at all? Or is it just business as usual?

Secondly, I would like to illustrate the issues raised by telling a little about two cases that are on the agenda in the Danish Data Protection Agency's work; the first case is about a Danish municipality's wish to use a cloud solution, the second case is about a security breach in connection with use of a cloud solution.

Finally, I will try to summarize and share a few thoughts concerning data protection in relation to cloud computing.

Cloud computing is a new way of delivering computing resources. Since cloud computing involves sharing of computing resources, transfer of data over the Internet and use of a data processor in a different way than we have been used to, we have focused on the following two areas: questions related to the security of the data processing and to the transfer of data to third countries.

In the Danish DPA we have not looked into the issue about the rights of the data subjects. So I cannot say that the use of cloud computing will not cause any problems for the data controller granting the data subjects their rights in accordance with the Directive 95/46. On the other hand, I am not in a position to conclude that there are no problems. Perhaps this is an area that needs further examination.

I will try to elaborate on the issue of security and the issue of transfer of data in the following.

Cloud computing involves the use of a data processor as defined in the Directive 95/46 article 2 – the provider of the cloud solution. And according to Article 17 of the Directive and the Danish Data Protection Act, the data controller has an obligation to ensure that the data processor provides sufficient technical and organizational security measures to protect the personal data against (accidental or unlawful) destruction or accidental loss, alteration, unauthorized disclosure or access. As we see it, one of the main problems – or perhaps the main

problem – of data protection in connection with cloud computing is that it is difficult for the controller to fulfil his obligation to ensure compliance and to supervise if the processor implements the appropriate security measures. This is due to a number of different circumstances: if the cloud provider (the processor) is a big international company, it can be difficult for the controller to establish a dialogue about the service and the conditions needed in the specific situation. Such international providers use standard contracts – "one size fits all" you could say. This means that the cloud user (the controller) has very little or no influence on the terms and conditions of the use of the cloud solution. Another aspect is that it is often uncertain where the data are located. As I see it, this is a key element in the cloud service – that it is flexible also from the provider's point of view. The providers of cloud solutions have data centres in several different countries to make it good business. A third element that I want to highlight here: is it possible for the controller to ensure that data are being deleted efficiently from the processor's servers? Until now it would be my assumption that the user of the cloud service in the end would need to have access to the cloud provider's data centres if he was to ensure that data have been efficiently deleted – and to ensure compliance as a whole. This leads me to the following question: is it at all possible for the controller to get access to the relevant data centre?

As you might recall the transmission of data over a network is highlighted in Article 17 of Directive 95/46, so it is relevant to give some attention to the transmission of the data taken place in cloud computing. Of course this is not a problem linked to the cloud solution in particular – so I just want to mention it here. And it is the same with the question about how to access data – the login-procedure.

The next issue I would like to mention is the transfer of data to third countries. Once identified, this is of course not an unsolvable problem. But it is our experience that in fact it is not easy for the controller – and for the DPA – to find out if data are transferred to third countries and if so, to which countries. Once this is defined – and if the countries in question are not safe third countries – the controller must use either the standard contractual clauses or establish that the provider subscribes to the Safe Harbour programme.

The initial case that we have worked quite hard with in the Danish DPA is one of the bigger Danish municipalities called Odense that wants to use a cloud solution (Google Apps) to file and store information about pupil's education, educational development, etc. According to the municipality, this involves data concerning health, serious social problems, and other, purely private matters.

This case was presented to us because of the Danish notification obligations. We had a dialogue with the municipality about the cloud solution where the agency asked quite a lot of questions about, for example, the security of data processing, transfer of data to third countries, and rights of the data subjects. We didn't have any contact with the provider of the solution – Google – in this process. In accordance with the Directive and the Danish Data Protection Act, we directed all our questions to the controller.

And finally, we gave an opinion to the Municipality as the controller. The opinion was issued after the case had been presented to and discussed in the Danish Data Protection Council which has 7 members in all and a Supreme Court Judge as Chairman.

The opinion is available in English on our website. So here I just want to highlight some of the main points.

The identified problems primarily concerned the following – and as you can see there is a direct reference to the issues I have already mentioned:

1) Transfer of data to third countries: Odense Municipality had not entered into an agreement based on the EU Commission's standard contractual clauses with Google.

2) Security on processing in general: in the opinion of the Danish DPA, Odense Municipality had not conducted an adequate risk assessment and thus had not implemented appropriate security measures to protect data against unauthorized disclosure. We recommended the Municipality the use of ENISA's checklist.

3) Requirements for use of a data processor: since Odense Municipality did not know where data were physically located, the DPA questioned whether the municipality could meet the requirements for a controller to ensure that the security measures are implemented and upheld by the processor.

4) Deletion of personal data: the Danish DPA found it to be unclear whether the data are deleted in such a way that they cannot possibly be recreated from Google's servers.

5) A number of other more specific security issues, for example, transmission and login were also pinpointed.

On this basis, the Danish DPA stated that the agency did not agree with the assessment made by Odense Municipality that confidential and sensitive data about pupils and parents can be processed in Google Apps. Status is that the DPA is willing to reconsider the case if the Municipality seeks solutions – and I think they try to do so in cooperation with Google.

The second case – I will make this very brief as this is an ongoing investigation and we still haven't got the full picture. But something went wrong concerning the authorizations of the users when the system for booking driving tests was transferred to a cloud solution. But as I understand from the explanation from the responsible organisation they don't consider this incident linked to the fact that is was a cloud solution – it could have happened in a traditional solution, as well. We will have to look into the case closer. But one of the things we understand by now is that the responsible organisation did not have any contract with the provider of the cloud solution securing that the obligations in the Danish Data Protection Act were fulfilled.

From my perspective as a lawyer – not as a technician – cloud computing is a challenge to data protection. I'm certain that cloud computing challenges the existing legal framework on data protection and I think that cloud computing is a challenge to data protection as such. The questions about security and transfer of data to third countries are the key ones. In Denmark the Minister of Science has announced that she wants to remove the barriers to using cloud computing. So recently she has decided to set up an expert group to examine the legal framework and to suggest adjustments in the Danish Data Protection Act to make it easier to use cloud computing.

In my opinion, it is not the right way forward. So what do we, as DPAs do about this challenge? I think that we need to have a dialogue not only with the controllers but – perhaps more importantly – with the processors (the providers of cloud computing) directly. So we can try to reach common ground on how to process data in the clouds while ensuring a high level of data protection.

EDUCATIONAL ACTIVITY OF THE POLISH DATA PROTECTION AUTHORITY

Urszula Góral
Bureau of the Inspector General for Personal Data Protection

This paper refers to educational activity of data protection authorities and focuses in particular on the Polish DPAs experience and solutions to be undertaken in order to improve its effectiveness.

LEGAL CONTEXT

At first, the legal context of the educational initiative of the Inspector General for Personal Data Protection (GIODO) should be discussed. It needs to be indicated that the Polish Constitution[1] (Art. 47) guarantees the right to legal protection of privacy and personal data.

Art. 47:

Everyone shall have the right to legal protection of his private life and family life, of his honour and good reputation and to make decisions about his personal life.

Moreover, Article 51 of the Constitution provides for the following:

Art. 51:

1. *No one may be obliged, except on the basis of statute, to disclose information concerning his person.*
2. *Public authorities shall not acquire, collect or make accessible information on citizens other than that which is necessary in a democratic state ruled by law.*
3. *Everyone shall have a right of access to official documents and data collections concerning him. Limitations upon such rights may be established by statute.*
4. *Everyone shall have the right to demand the correction or deletion of untrue or incomplete information, or information acquired by means contrary to statute.*
5. *Principles and procedures for collection of and access to information shall be specified by statute.*

The above mentioned principles are reflected in the Polish legal system in the form of the Act of August 29, 1997 on the Protection of Personal Data (unified text – Journal of Laws of 2002, No. 101, item 926) which sets out the rules of protecting personal data at the national level.

Article 12 of the Act on Personal Data Protection sets out duties entrusted to the Inspector General for Personal Data Protection, particularly in terms of initiating and undertaking activities to improve the protection of personal data. Article 12 enables the Polish DPA to develop a wide range of educational undertakings such as: training courses, workshops, conferences and academic seminars, publishing guidelines and handbooks. The Inspector General for Personal Data Protec-

tion is also empowered to initiate public discussions and consultations and cooperate with different sectors.

At this point, one should mention the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions "A comprehensive approach on personal data protection in the European Union", issued by the European Commission on November 4, 2010. The Communication comprises new solutions which will enable data protection institutions to thrive in the future.

One of the crucial issues raised there is the necessity of developing educational activities. In this key document we can read:

"there is also a need to make the general public, and particularly young people, more aware of the risks related to the processing of personal data and of their rights. A Eurobarometer survey in 2008 showed that a large majority of people in EU Member States consider that awareness of personal data protection in their own country is low. Awareness raising activities should thus be encouraged and promoted by a broad range of actors, i.e. Member State authorities, particularly Data Protection Authorities and educational bodies, as well as data controllers and civil society associations. They should include non-legislative measures such as awareness campaigns in the print and electronic media, and the provision of clear information on web-sites, clearly spelling out data subjects'rights and data controllers' responsibilities."

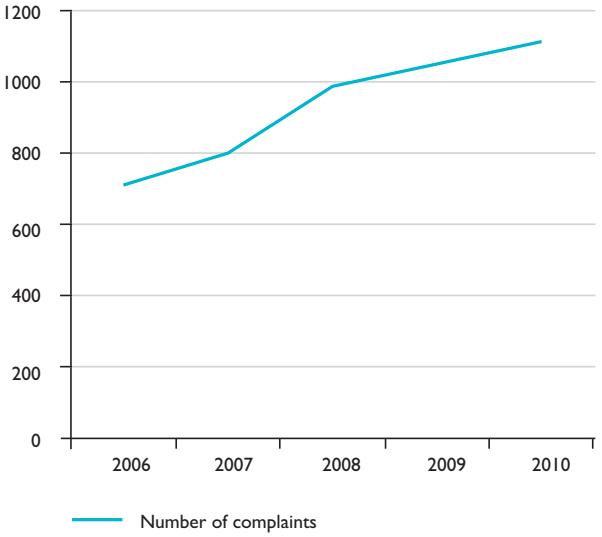
The Communication clearly states that *"the Commission will explore*:

- *the possibility for co-financing awareness-raising activities on data protection via the Union budget;*
- *the need for and the opportunity of including in the legal framework an obligation to carry out awareness-raising activities in this area."*[2]

We can recognise such approach as a green light for conducting and developing settled direction. Data Protection Authorities welcome this approach and look forward to new legal provisions and solutions.

Before describing the scope of activities of the Inspector General for Personal Data Protection, attention shall be drawn to the way of measuring efficiency of the Polish DPA, because after a few years of conducting the educational actions one has to know how effective it is.

In the period from 2006 to 2010 the number of complaints submitted to the Polish DPA has vastly increased (graph no. 1).



Graph no. 1

Using the number of complaints as an indicator, it can be said that after 4 years of conducting educational activities, the level of the awareness of data protection rights has grown, and had big influence on the number of complaints. Their number has been consistently increasing in recent years: from 712 complaints in 2006, 796 complaints in 2007, 986 in 2008, 1049 complaints in 2009 and until 1114 in 2010.

The reason for this situation is to be found in the increasing awareness of citizens on the issue of the protection of privacy and personal data and their greater involvement and activity in the enforcement of their rights.

After discussing the legal context of GIODO's initiative in the field concerned, the main educational activities of the Polish DPA shall be briefly presented.

EDUCATIONAL ACTIVITIES

The Bureau of the Inspector General for Personal Data Protection (GIODO Bureau) conducts within its competencies extensive information and educational activities.

The most important ones include:

- publications and educational programmes,
- training courses and workshops, also in the form of e-learning courses, addressed mainly to the representatives of government and self-government administration, as well as representatives of public institutions.

Furthermore, the Bureau of the Inspector General is an organiser and participant of a variety of conferences. While performing educational tasks, we cooperate with various partners, both at international (Council of Europe, European Commission, data protection authorities from other countries, including in particular the Central and Eastern European states) and national level (public administration authorities, non-governmental organisations and higher schools).

As far as publications are concerned, the Polish DPA developed a series of brochures called ABC of personal data protection. These handbooks provide explanation and guidelines how to comply with the data protection law and address crucial questions in the field of data protection. The "ABC of personal data protection" series currently comprises 9 pieces, and

the next one is being prepared – it will be "ABC of data protection in parliamentary elections".

The Bureau of the Inspector General also publishes leaflets on special occasions, for instance on the occasion of entering the Schengen Area.

Another publication is Annual Report, which is also accessible on our website, and which has become a very useful and certain source of information.

Attention should be also drawn to the publication called "Guide for Entrepreneurs". It is GIODO's latest initiative conducted together with partners from the Czech and Hungarian DPAs. This guide has been developed in order to provide comprehensive and clear to understand source of basic information for people who are just about to set up their own business. This guide will be published in four language versions – Polish, Czech, Hungarian, and English, and hopefully it will be a helpful tool for entrepreneurs.

The next area of the Inspector General for Personal Data Protection activity is educational programmes. Three of them shall be briefly described. The first programme was initiated by the Inspector General in 2009. The pilot programme "Your data – your concern. Effective protection of personal data. Educational activity addressed to students and teachers" aimed at developing effective methods of educating children and youth on personal data protection and the right to privacy. The pilot programme was realised by education centres in several cities in Poland and covered many schools in these cities.

The pilot lasted one year and included:

- training courses (conducted by experts from GIODO Bureau) for leaders who were later on training teachers in schools,

- developing scenarios of lessons for middle schools students.

After one year, the pilot programme became a Poland-wide education programme under the patronage of the Ministry of National Education. Now, the Polish DPA is still developing this programme by involving more and more education centres and schools, and it has met with vast interest in this programme, which could have been seen last week, when GIODO's conference for teachers was attended by almost 200 participants.

Last year, the GIODO Bureau was selected to organise a study visit financed from the European Union funds within the framework of the Study Visits Programme, the part of the Lifelong Learning Programme.

The objective of the visit was to exchange information and experience related to the ways and methods of providing knowledge on personal data protection addressed to children and youth.

The visit was attended by representatives of European data protection authorities and education institutions, and finished with a very interesting report, which acknowledged the importance of such meetings. Therefore, the Polish DPA is planning to continue these meetings.

Furthermore, it is worth noting that the GIODO Bureau created eduGIODO educational and informational platform - GIODO's educational website - which allows individuals to gain information on personal data protection. It was launched in October 2008 as part of a Community project co-financed by the Transition Facility Programme 2005/017-488.01.08 "Elastic reserve" - "Personal data protection - my rights, my responsibilities", and is available in Polish at http://edugiodo.giodo.gov.pl/. *The platform is directed to:* personal data controllers, personal data processors, and data subjects, i.e. each individual. It *contains two kinds of materials*: informational and training. *The informational module* contains, among others, the basic definitions concerning data protection, a list of rights which data subjects enjoy and the principles of data protection and legitimate data processing in selected sectors such as: telecommunications, information society, public healthcare, human resources management and consumer rights protection. *The training module* comprises three specialised electronic courses including multimedia and progress tests.

The GIODO's e-learning platform took part in the contest for the best practices concerning the protection of personal data in public administration organised by the Madrid Data Protection Agency 3 years ago.

Another important part of the Polish DPAs' activities are training courses conducted by its employees.

Entities from various sectors of economic and public life as well as natural persons show an apparent lack of systematised knowledge in this area. The demand for training courses is growing and the Polish DPA is doing its best to meet that demand. The GIODO Bureau organises approximately 60 courses per year. As regards statistics, the number of training courses for public administration and institutions in particular years was as follows:

- 2007 - 60 courses
- 2008 - 62 courses
- 2009 - 56 courses
- 2010 - 55 courses
- until May 2011 - 19 courses

However, this year the Polish DPA decided to change its approach in order to be more effective, and now focuses on teaching groups of trainers, who represent a number of public and private sectors. That way, hopefully much larger audiences will be reached and the impact will be wider.

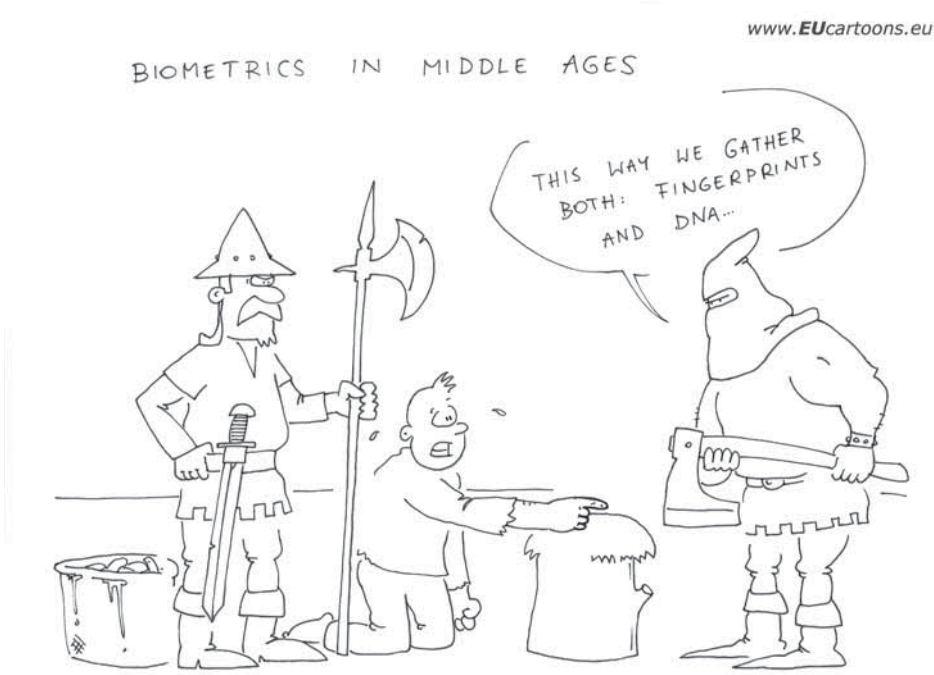
Last year, the Inspector General for Personal Data Protection launched public consultations on the amendments of the Data Protection Act. In recent months, a couple of seminars and conferences took place in order to discus necessary amendments in this regard.

The GIODO Bureau is also involved in organisation of workshops, the latest example of which is the tutorial on Binding Corporate Rules, which was held in Warsaw on 14 June 2011, and was attended by many representatives from other DPAs.

The Polish DPA is involved in celebrating Data Protection Day, as well. GIODO uses the occasion of Data Protection Day to organise so called Open Door Day, during which free legal advice is offered to all visitors.

The Data Protection Day has always served as an occasion to sign agreements on good practices on data protection with different entities, such as the Polish Bank Association or Direct Marketing Association, and promote the rules of data protection among them.

The Inspector General for Personal Data Protection has also initiated a good tradition whereby data protection experts meet every year on that day in the Permanent Representation of the Republic of Poland to the EU. Since the Polish DPA hopes that this tradition will last in the future, it tries to support it with new interesting ideas. Apart from raising serious matters, it tries to approach the current issues in a more light-hearted way. For example, cartoons were created exclusively for the celebration of Data Protection Day in the Polish Permanent Representation by Polish cartoonist Michał Narojek. Below you may see one of the cartoons.



Next area of GIODO's activity is cooperation with representatives of public and economic sectors.

In order to promote the rules of data protection GIODO started to collaborate with different sectors. The range of entities with which it cooperates is quite diverse, from the Direct Marketing Association, through the Polish Bank Association, Polish Real Estate Federation, Polish Bishops' Conference, Roman Catholic Church, Interactive Advertising Bureau Poland, Polish Automobile Manufacturers Association up to the Orthodox Church.

It has taken a lot of effort to reach agreements with these institutions, but it has been worth every bit of trouble, especially when it can be observed how greatly practices in these sectors have improved since introduction of Codes of Conduct. Problems and violations in the past were replaced by internal data protection standards.

What is also vital to the Polish DPA is working with NGOs - which are very active in Poland, as well as with universities and high schools.

GIODO has been deeply engaged in supporting these organisations and its work in this area seems to have been particularly fruitful.

A few words shall be said about one of these organisations – Nobody's Children Foundation. NCF is the non-governmental non-profit organization working toward the goals of protecting children from abuse and providing help for abused children and their families. The facilities run by the Foundation offer psychological, medical, and legal help to victims of abuse.

The Polish DPA has found that it has mutual goals with the NCF and supports the foundation in their preventive actions aimed at reducing threats to children on the Internet.

One of the awareness campaigns run by the Foundation was the „Child in Net" campaign aimed to raise awareness among both children and adults and serve as a warning to offenders who think they are anonymous and safe when using the Internet. The Polish DPA welcomes such valuable initiatives and is eager to support them.

As far as universities and high schools are concerned, GIODO cooperates among others with Koźmiński University in Warsaw, College of Finance and Business Administration in Gdańsk, National-Louis University in Nowy Sącz, Cardinal Stefan Wyszyński University in Warsaw, or University of Silesia in Katowice.

What are the Polish DPAs' goals for the future?

At this point, reference shall be made to the Study Visit mentioned before. It was a particularly important event, as its outcome largely determined GIODO's future strategy. The Inspector General for Personal Data Protection will now focus on the following issues: initiatives aimed at raising awareness, cooperation between different educational institutions, self-regulations, legislative measures, and introducing privacy and data protection topics to school curricula.

To sum up, it needs to be indicated that raising data protection awareness becomes of crucial importance.

Finally, it shall be emphasized that the Polish DPAs' educational activities have been possible thanks to support from its partners, who are encouraged to further cooperation.

ENDNOTES

1 Constitution of the Republic of Poland of 2 April 1997 (Journal of Laws of 16 July 1997).

2 Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions "A comprehensive approach on personal data protection in the European Union" of 4 November 2010, point 2.1.4.

FROM THE PRINCIPLE OF ACCOUNTABILITY TO SYSTEM RESPONSIBILITY – KEY CONCEPTS IN DATA PROTECTION LAW AND HUMAN RIGHTS LAW DISCUSSIONS

Professor Paul De Hert
Vrije Universiteit Brussel (LSTS) & University of Tilburg (TILT)

SUMMARY[1]

The principle of accountability is one of the features of current reform proposals of the EU Data Protection Regime. In this contribution I will first look at a possible definition of the principle, then turn to its application in the area of data protection law, and finally turn to European human rights law.

The paper wants to broaden the discussion about the reform of the Data Protection Directive by turning to human rights law and borrowing insights from a 2008 United Nations Report *Protect, Respect, Remedy* proposed by John Ruggie, Special Representative to the Secretary-General on Business and Human Rights. The report identifies three building blocks to respond to governance gaps in human rights protection caused by international corporations in weaker developing states. Although the report does not advocate accountability or enhanced responsibility for these global corporations, it contains a broader sketch of areas of legal attention to avoid governance gaps: the area of ex ante law making and ex ante and ex post enforcement (protection), the area of corporate responsibility (respect) and the area of access to remedies when violations have occurred (remedy (ex post)).

From a European human rights perspective, governments have to show that they are active in all three areas. The doctrine of positive human rights duties developed by the European Court of Human Rights is fundamental in this. This doctrine, as it is used by the Court, forces member states to take up their duties with regard to the Internet and other modern media.[2] It is not only about non-interference, but about the full package: to protect, create respect and to remedy. More specifically, governments must protect their citizens against human rights abuses by companies and against abuses by other users on the Internet (first building block); ensure that companies respect their human rights obligations (second building block); and provide easily accessible remedies or remedial action (third building block).

Hence my thesis that not only corporations or data controllers have to give account. On a broader level, governments have to give 'accounts' with regard to the three building-blocks. The idea of system responsibility nicely catches this broader responsibility.

My aim is double. I want to reflect about the principle of accountability as a starting point for legal reform. Secondly, I want to draw a parallel between the discussion about data protection law reform and the discussion within the United Nations about how to end human rights violations by transnational corporations in weaker states. In both discussions there are power asymmetries between strong, untouchable international corporations and weaker individuals that lack resources and knowledge to come up for their rights. Ruggie's approach refrains from an accountability ap-

proach towards firms, but it does contain a useful message concerning positive duties for states to regulate and enforce and to organise an accessible legal system that is made to be used by citizens whose rights are violated by corporations. The discussion in Part III of judgements like *I v. Finland* (2008) and *Armonas v. Lithuania* (2008) rendered by the European Court convinces me that the current European data protection review does not 'give account' of an awareness that next to enhancing responsibilities of data controllers, it also needs to enhance its system of protection and remedies.

Ruggie's *Protect, Respect, Remedy* scheme indicates well the indispensable basic building blocks for a complete scheme of protection of human rights in our information society. Whenever the theme of responsibility is addressed, all three blocks have to be considered for the sake of an integrative approach. The author of this contribution has not been able to temper his fascination for the third building block, the classical legal idea of remedy. However classical it may be, its relevance remains high. Too many public and private initiatives are launched and regulated from only one perspective, the perspective of the organism that takes the initiative. Seldom are initiatives looked at from 'the back end', from the perspective of the citizen that needs to be informed about his rights and from the perspective of the supervisory authority (judge or administrative authority) that needs to safeguard the fundamental right to an effective remedy. With Ruggie's threefold scheme and his insistence on 'real' access to justice and real transparency the above trap is avoided and the old legal lady of 'remedy' receives a second life. In a way this is very respectful to the qualitative dimension of the principle of accountability.

Public authority has an important role to play in every integrative approach to responsibility. It is up to governments to develop an efficient remedy system. Post-legislative scrutiny of key legal instruments adopted in the past should become the norm. A 2009 House of Lords' report with regard to surveillance contains several recommendations for specific actions by governments that can be repeated here by way of illustration.[3] Some of the questions that need to be put addressed are the following: Do these instruments contain clear guidance on necessity and proportionality? Is priority given to citizen-oriented considerations? Can the safeguards and restrictions placed on surveillance and data handling be improved? Are design solutions incorporated? Can the introduction of a system of judicial oversight for surveillance carried out by public authorities be foreseen? Are individuals who have been made the subject of surveillance to be informed of that surveillance, when completed, where no investigation might be prejudiced as a result? Is compensation available to those subject to unlawful surveillance by the police, intelligence services, or other public bodies acting under the powers?

Partly, these recommendations can be grouped together with state obligations to *protect* through effective regulations and effective enforcement (building block). Again a task for public authorities. In the 'Evidence' gathered by the House of Lords for its report on surveillance, that massive violations of security and privacy were not followed by appropriate sanctions was deplored: "When banks dump personal data in outdoor rubbish bins, in direct contravention of the Act, their punishment is to sign a form saying they won't do it again. When the identities of staff at Network Rail and the Department of Work and Pensions are stolen from a compromised HMRC portal to defraud the tax credit scheme, HMRC escapes unpunished".[4] Improving the legal framework with regard to cyber crime, review of the data protection directive and more effective enforcement of privacy rules are rightly on the EU agenda.

With regard to the second building block ('respect'), some favour a more stringent approach turning a duty to comply into a more active duty to prove that one is concerned and contributes to the protection of certain rights. The development should be applauded from a human rights perspective. Those who have power have to be held accountable. An information society that works, allowing providers, who do not see problems in unsafe and unregulated information services, is becoming less defensible. Citizens cannot be held responsible for a system where the government is not playing its role and forgets or refuses to hold relevant actors accountable. That is not how system responsibility works. The author of this contribution is aware of attempts to 'sell' more accountability in exchange of fewer formalities and less stringent data protection requirements on other fronts. From such a perspective, 'more accountability' seems to be instrumental for a kind of politics of good intentions ('something went wrong but I am not responsible since I actively embraced data protection'). We recall that our legal system seldom considers good intentions and motifs, but does look at behaviour and consequences. Ethically it is important to embrace the active incorporation of human rights values, but legally there would be a flaw in system responsibility if no governmental reaction followed from damage caused.

ENDNOTES

1 You can find the whole essay in the Annex

2 The excuse that technology is evolving rapidly and coming not from Eindhoven, but from Silicon Valley, is unconvincing.

3 House of Lords, Selected Committee on the Constitution, Surveillance: Citizens and the State, HL Paper 18-I, 2nd Report of Session 2008-2009, Volume I: Report, pp. 107-108

4 "Memorandum by the Open Rights Group" in HOUSE OF LORDS, Selected Committee on the Constitution, Surveillance: Citizens and the State, HL Paper 18-II, 2nd Report of Session 2008-2009, Volume II: Evidence, pp. 433-435, p. 433

NEW DATA PROTECTION PRINCIPLES IN LIGHT OF THE DEBATE ON COUNCIL CONCLUSIONS

Endre Győző Szabó
Deputy Head of Department, Ministry of Public Administration and Justice

In my study, instead of a detailed assessment of the basic principles, I would rather like to share my experiences about the chances I see for the new fundamental principles to become part of the new regulations.

My paper aims to report on how the Council conclusions adopted by the Council of the European Union in February 2011 reflect the new fundamental principles of data protection, and in the preparation of the document; and based on the positions explained by government experts of member states, what is Europe's public perception in general about the new fundamental principles.

In order to be able to assess the contents of the conclusions of the Council, we must highlight a few characteristic features. First of all, the Council conclusions were created on the proposal of the Presidency; nevertheless, we prepared this document in response to something. It was back on 4 November 2010 that the European Commission released its communication on the comprehensive approach to data protection in the European Union. The Communication gave an account of the approximate progress made by the Commission in the process of preparing the new legislation on data protection, the issues receiving special consideration and the related possible directions. Therefore the Council conclusions provide an answer to the communication of the Commission.

It is another important characteristic of the conclusions that unanimity is required for their acceptance. Although the Treaty of Lisbon introduced the qualified majority procedure as a main rule in the field of justice as well, this kind of document continues to be created by consensus. We will adopt the legislation replacing the current data protection directive with qualified majority, but it is not enough for the adoption of the Council conclusions preparing it. In practice, this meant in the wording of the document that if one single member state objected to a section or a sentence, we had to come up with a proposed wording that was acceptable for the objecting member state as well.

However, the document was created by unanimous approval, therefore we can assume that the provisions contained in it will provide important guidance for decision-making in the future.

The European Commission is a permanent participant of Council formations; it negotiates together with member states. I believe that in the working group on data protection, where we prepared the conclusions, both member states and the Commission benefited from monitoring and participating in the debate.

Based on the above points, it is perhaps not surprising to say that in this early phase the representatives of administrations of member states made special efforts to have us commenting the raised issues carefully, and as much as possible, leave the largest latitude for member states in the future. This is clear in decision-making: we should tie our own hands to the least possible extent concerning decisions to be made in the future. This careful approach could be seen concerning

the new fundamental principles as well, still, the finally approved wording enables us to draw some useful conclusions.

There are internationally elaborated fundamental principles in the centre of data protection regulations. The fundamental principles are in the focus of international documents as well as national legislation. The conclusions of the Council on the fundamental principles stipulate that they have stood the test of time. This conveys a clear message: member states would like the so-called old fundamental principles to continue being parts of the regulation in the future.

However, member states suggest that they should be carefully reconsidered, reviewing their applicability. In my understanding it is not a sign that any member state would like to remove, for example, the principle of purpose limitation from the set of fundamental principles, rather, it means that reconsidering the entire regulation could enable the adoption of new principles.

There are two principles expressly manifest in the conclusions: the principle of accountability and the principle of privacy by design.

Concerning the principle of accountability, the communication of the Commission was restricted to assessing the incorporation of this new principle into the new legislation. According to the communication of the Commission, the principle is designed to ensure more efficient compliance with the rules of data protection, at the same time, it is also meant to alleviate administrative burdens.

Assessing the reaction of the Council in that regard, I believe it should be appreciated in itself that member states unanimously welcome the emergence of this principle. In addition, they encourage the Commission to assess how this principle could be incorporated into the aquis. Otherwise, in the debate it was articulated that there is no full consent about whether the principle of accountability is ripe for codification or not. If I discern the majority opinion properly, it would be too early to incorporate the new principle into the set of the existing ones, at the same time, in the conclusions those elements were formulated that member states would like to see it adopted in the proposal of the Commission when presenting the case: these would be, liability assigned based on clear-cut rules, the minutely elaborated consequences of legal offences, and ultimately, the protection of the individual at a higher level. At this point the Council went beyond merely reacting, and formulated its expectations from the application of the principle of accountability.

That item of the conclusions is remarkable which provides that the principle of accountability should contribute, in addition to the tools of self-regulation, to the smooth operation of the single market and to improved compliance with the rules of law.

I do not believe that member states expressly expect codification of the principle of accountability, only that if such codification could serve to improve the quality of the wording of the norm, then we should utilize this principle, too, in codification.

According to the conclusions, a case in point for the implementation of the principle of accountability in practice could be extension of the duty to report data security incidents to new areas. At present such an obligation only applies in the field of telecommunications, even though the idea of extension is raised over and over again. The document proposes that reporting obligation should be imposed in cases required by the protection of the interests of the individual and his or her pri-

vate sphere. On the other hand, the obligation of reporting and notification should not cover every negligible irregularity, only those cases when there is a danger of real infringement of interests, and the only recourse to higher level protection of interests and rights is through the involvement of the authority or the affected person.

Concerning the principle of privacy by design, the communication of the Commission contains a reference to the privacy-friendly technologies and that this principle could also contribute to implementation of the requirement of data security. According to the communication, the Commission undertook to assess the specific applicability of the principal of privacy by design.

Member states reacted to this undertaking of the Commission supportively, and concurred that the principal of privacy by design should be incorporated in the new legal framework, if such incorporation is possible. Concerning this, the Council highlights that in the development of the new regulation the impact of new technologies on the private sphere should be taken into account. Starting from the need to protect the individual, it formulates the requirement that the relevant persons should receive clear information about the effects of the applied technology and those methods of utilization should be set as default (privacy by default) that respect the private sphere. Therefore, what member states highlight by this is that in the application of the technology the possible risks should be given advance consideration. We should not wait until interests have been violated, rather, we need to define the process and make the settings right from the start in such a manner that the affected persons should meet a privacy-friendly environment without any actions on their side. It is obvious that if the applied technology or the service utilized by the user takes into account the need of his or her protection, this will contribute to the enhancement of trust. Unfortunately, in practice we see it many times that this trust is still difficult to obtain.

As I see it, the two fundamental principles under consideration, i.e. the principle of accountability and privacy by design are connected at this point, the requirement of openness and transparency is endorsed by both. Both of these principles expect developers of technology and providers of services to behave in a manner compliant with the fair business model. That way, this is the concept implied by the conclusions of the Council.

Obviously, in this stage of decision-making the Council could not provide much more precise guidance than that concerning the wording of the legislation to be developed, nevertheless, hopefully it will constitute a sufficient basis for the Commission to come up with a wording that will be welcomed by member states as well. If the proposal of the Commission complies with the presented guidance of the Council, then the two principles mentioned above will be substantially incorporated into the new legislation.

GLOBAL STANDARDS FOR DATA PROTECTION AND PRIVACY FROM THE BUSINESS POINT OF VIEW[1]

Christopher Kuner
Chair, Task Force on Privacy and the Protection of Personal Data
International Chamber of Commerce (ICC), Paris

I. INTRODUCTION

The issue of whether a global framework for data protection is desirable, and if so what form it should take, is becoming more acute owing to the growing importance of data processing in the global economy. The processing of personal data has become a key activity of both private sector entities and governments, and the development of the Internet has made it possible for companies, governments, and individuals to transfer huge amount of data around the globe at the click of a mouse. Moreover, innovations such as "cloud computing" allow vast amounts of personal data to be processed across national borders on a routine basis, thus severing the gap between data processing and territoriality, and increasing the need for a global regulatory framework. These developments make it important to ensure both that the processing of personal data receives effective protection regardless of where it is carried out, and that data can flow freely between jurisdictions with as few impediments as possible. It is thus not surprising that many businesses have complained about differences between national data protection and privacy laws, and have called upon governments to adopt a more global approach to the topic.

All parties (including not only business, but also governments, data protection regulators, and individuals) seem to believe that a more global approach to data protection would be desirable. However, it is important to consider what this goal would mean in practice, and how it can most feasibly be implemented.

II. CONSIDERATIONS FOR AN INTERNATIONAL INSTRUMENT

Global standards for data protection and privacy are often discussed in terms of a binding global instrument (such as a treaty or convention) that States would adhere to. At a minimum, the following questions would have to be addressed in order to enact a legally-binding global legal framework for data protection:

Overcoming political hurdles and achieving true harmonisation: A binding legal framework would address the lack of data protection standards in many States, and the difficulties that data controllers face in applying differing legal standards to the same data processing. At the same time, it could take a long time to draft and approve, and would also be subject to political hurdles. Moreover, experience in the unification of private law has shown that States tend to give a low priority to the implementation of such conventions, so that it is questionable whether enactment of a convention would lead to true harmonisation.

Whether an existing instrument should be used, or a new one should be drafted: A number of international instruments already exist that could serve, at least in theory, as the basis for an international

legal framework for data protection, most prominently Council of Europe Convention 108. However, it is unlikely that a majority of countries outside of Europe would be willing to sign up to a Convention that is based on European data protection standards. Moreover, even Convention 108 is a high-level instrument that would not likely produce detailed harmonisation. The alternative would be to produce a new instrument, such as a convention drafted by the International Law Commission of the United Nations, but this could take decades.

The institution that would coordinate the work: An international institution would have to coordinate the work on a global instrument for data protection. Data protection law is a mixture of various legal areas, such as human rights law, public law, private law, and others, and not all these different areas have traditionally been covered in the work of the international institutions dealing with the harmonisation of law such as UNCITRAL and UNIDROIT. While the International Law Commission has produced instruments in many areas of public international law, it does not seem well-suited to dealing with a fast-moving and politically-charged area like data protection. Institutions such as the Council of Europe may be too closely tied to one region to produce an instrument of truly global application. Thus, either a new group would have to be created, or the mandate of an existing international organisation would have to be expanded.

The scope of the instrument: Difficult decisions would also have to be made regarding the scope of the instrument, such as whether it would cover only data protection or also privacy, and whether it should contain exceptions, such as for data processing by law enforcement. In particular, the growing appetite of government and law enforcement authorities for data held by the private sector will make it increasingly difficult to agree on and apply harmonised data protection standards throughout the world; an example is provided by the recent efforts by the government of India to establish a "National Intelligence Grid" that will result in unrestricted access by Indian law enforcement to private sector databases.[2]

III. OTHER OPTIONS

There are vehicles other than an international convention by which global standards could be promulgated, such as the following:

Model law. A model law on data protection could be drafted which States could enact into their own national legal structures. The International Law Commission has considered elaborating "general principles that are attendant in the protection of personal data", and has stated that it "would assist governments in the preparation of national legislation",[3] which approach seems similar to the preparation of a model law. The model law approach has been used successfully in a number of areas by UNCITRAL. On the other hand, it is not clear whether the adoption of a model law by States would truly lead to harmonisation of data protection law, though it would have the advantage of being more acceptable to States that might be uncomfortable with a binding convention.

Interfaces between regional data protection standards. Mechanisms could be developed to provide an easier interface between existing data protection standards developed in different regions. For example, similar instruments such as binding corporate rules (BCRs) in the EU and cross-border privacy rules (CBPRs) in the APEC region could receive mutual recognition between the two regions, perhaps through the use of common trustmarks, auditing standards, and other mechanisms.

This could gradually lead to a rising standard of data protection, as well as greater harmonisation of standards, as instruments become recognised across different regions.

Non-binding technical standards. Professor Lawrence Lessig famously proclaimed that "code is law", i.e., that "the software and hardware that make cyberspace what it is *regulate* cyberspace as it is",[4] and it could be argued that technical standards for data processing could lead to globally-harmonised data protection practices more swiftly and effectively than an international convention could. Bodies such as the International Telecommunications Union (ITU) and the World Wide Web Consortium (W3C) have promulgated technical standards that have proven highly influential for the processing of personal data, and several organisations are also working on data protection standards. For example, the International Organisation for Standardisation (ISO) has been working on voluntary standards for privacy protection, and regional bodies have also issued such standards.

IV. CONCLUSIONS

While there is broad international agreement on the principles of data protection law at the highest level, once one begins going into more detail, the differences between the different regional and national approaches become pronounced. It is precisely in areas where national law and policy differ that efforts to harmonise the law are most difficult, and the details of data protection law differ substantially between different regions and legal systems.

While a number of data protection principles are widely accepted, the different cultural and legal conceptions of data protection around the world, together with the lack of data protection law in most States, will make it difficult to reach broad international agreement on a defined set of standards. The level of strictness of such standards could pose a dilemma: if global standards were set too high, then it is likely that many States would be reluctant to enact them, while if they were set too low, then States and entities with a long tradition of data protection law might oppose them. A related question is whether any global standards should override local law: while many States would likely accept global standards only if they applied without prejudice to national requirements, allowing local law to apply on top of any global standards could defeat the goal of providing a reasonable degree of international harmonisation. To provide real added value, global data protection standards should thus harmonise the law as much as possible, and not just act as an extra layer of regulation on top of existing law.

The difficulty of selecting the standards that would serve as the basis for a binding legal instrument, of agreeing on its scope, and of selecting an appropriate international organisation to coordinate the work, indicates that the drafting of such an instrument is unlikely to be possible within a reasonable time period, and to a useful degree of specificity.

While an international convention on data protection may be premature, other actions could lead to a gradual harmonisation of the law. For example, an international body could draft a model data protection law, which could then be the basis for more States to enact data protection legislation, thus leading to greater international consensus on the substance of data protection standards. Widespread adoption of technical standards for data protection could also gradually lead to increased legal convergence, as could greater mutual recognition of regional data protection standards.

None of these steps would rule out discussions on a global legal instrument for data protection. Such discussions have come to fruition in the "Madrid Resolution", which was approved in 2009 by a group of data protection authorities, academics, business representatives, and non-governmental organisations under the chairmanship of the Spanish Data Protection Authority.[5] Such an effort is a useful way to explore the commonalities and differences between the various approaches to data protection, and can make a positive contribution to the eventual development of global standards. However, at this stage the primary value of such efforts is to facilitate discussion between representatives of the various approaches to data protection, without expecting that an international convention could be adopted any time soon.

This multi-faceted approach is in keeping with modern thinking regarding the harmonisation of laws, which stresses the need to consider other, more flexible approaches besides the drafting of international conventions. Data protection is deserving of further legal protection on a global scale, the need for which will continue to increase as both governments and private sector entities seek to process an increasing amount of personal data. The time for a global approach to data protection has definitely come, but efforts at global legal harmonisation must be flexible enough to encompass approaches beyond traditional instruments like international conventions. In the interregnum between a purely national or regional view of data protection and a legally binding international data protection framework, it will be necessary to make use of other mechanisms to achieve greater international harmonisation of data protection law.

ENDNOTES

1 The ideas in this paper are developed more fully in Christopher Kuner, "An International Legal Framework for Data Protection: Issues and Prospects", (2009) 25 Computer Law and Security Review, p. 307.

2 See http://news.rediff.com/report/2010/feb/06/natgrid-will-track-all-your-spending.htm.

3 ILC, "Report on the Work of its Fifty-Eighth Session" (1 May to 9 June to 11 August 2006) UN Doc A/61/10 para 257, Annex D, para 12.

4 Lawrence Lessig, Code and other laws of cyberspace (Basic Books 1999), p. 6.

5 "International Standards on the Protection of Personal Data and Privacy" (2009).

CONVENTION 108 – STILL GOING STRONG AFTER 30 YEARS?

Jörg Polakiewicz
Head of Human Rights Development Department,
Directorate General of Human Rights and Legal Affairs, Council of Europe

This year marks the 30th anniversary of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Convention 108"). The Convention's declared purpose, as laid down in an article[1], remains as valid today as it was 30 years ago: "to secure […] for every individual ... his right to privacy."

Convention 108 was opened for signature in Strasbourg on 28 January 1981. Together with its 2001 protocol, it has become a benchmark for more than 40 countries in Europe and has influenced legislation far beyond. I would like to use the SWOT analysis to examine the Strengths, Weaknesses, Opportunities and Threats for convention 108 as a global standard.

STRENGTHS

The Convention formulates a number of core principles, drafted in a simple and technologically-neutral way. The Convention's fundamental standards have stood the test of time. You find them reflected in the "international standards" adopted by the International Conference of Data Protection and Privacy Commissioners in Madrid (2009)[2] or in agreements that the European Union is currently concluding with Australia or the USA on the exchange of data for law enforcement purposes. They include purpose specification or limitation, data quality and security, individual access and rectification, independent oversight, transparency and redress.

The Convention is a legally binding international treaty, providing legal certainty and predictability. It has a cross-cutting scope of application. Convention 108 protects against privacy intrusions by public and private authorities, both in the off-line and on-line worlds. There are no loopholes regarding defence, national security or law enforcement.

Convention 108 provides a unique framework for multilateral co-operation through a conventional committee, where all states parties are working together on an equal footing. It is composed of representatives of governments and data protection authorities alike. It also allows for the participation of states that are not parties to the Convention (currently Australia and the USA) as well as non-state actors, such as the International Chamber of Commerce, the International Conference of Data Protection and Privacy Commissioners or the Francophone Association of Data Protection Authorities.

The T-PD (Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data) is much more than a forum for exchange of information and good practices. It has important standard-setting functions. Most recently, it has prepared a recommendation on profiling, which was adopted by the Committee of Ministers of the Council of Europe. Indeed, the complexity of issues concerning the effective protection of

personal data, caused in particular by the constant emergence of new technologies and practices, calls for innovative solutions and analysis. In such circumstances, soft law instruments, which allow for the further development of the Convention's core standards and lead to a certain degree of harmonisation of national practices, are preferable to treaty law, which is subject to cumbersome negotiation and ratification procedures.

Finally, Convention 108 is not a purely "European" instrument. It is worth recalling the Convention's point of departure, namely that, "certain rights of the individual may have to be protected vis-à-vis the free flow of information regardless of frontiers, the latter principle being enshrined in international and European instruments on human rights […]. It does not seem advisable; however, to rely solely on the European Human Rights Convention for data protection, *inter alia* because it is a 'closed' instrument, which does not permit the participation of non-European and non-member States."[3] Indeed, representatives from Australia, Canada, Japan and the United States of America took part in the drafting work which was carried out in close collaboration with the OECD.

WEAKNESSES - TOO EUROPEAN AND WITHOUT TEETH?

I remember vividly a panel discussion at the 2008 International Conference of Data Protection and Privacy Commissioners in Strasbourg, with the following intervention: the Convention's principles may be sound, but who is checking that states parties live up to their commitments? It was argued that the Convention lacks a strong follow-up mechanism. T-PD is a "consultative committee", with limited resources and without real enforcement powers. Moreover, is Convention 108 not too European to serve as a global standard? None of the non-European states that participated in its drafting have actually signed up it.

Both criticisms raise serious points that we must address in order to be credible when promoting Convention 108 worldwide. To start with the first point – absence of signatories outside Europe – the situation may change very soon. Uruguay has requested accession and may become a party later this year. We are confident that it will only be the first country in a long list.

But, more importantly, is it really surprising that so far no non-European countries, in particular those having participated in its elaboration, have signed up? The Council of Europe never really promoted the Convention outside Europe. It was only in December 2009 that the EU's Stockholm Programme explicitly called for the promotion of Convention 108 worldwide.[4]

30 years ago we lived in a different world, much less globalised and interconnected. 30 years ago, an American president would not have said: "This world – cyberspace – is a world that we depend on every single day… [it] has made us more interconnected than at any time in human history."[5] Today, over 2 billion people[6] worldwide regularly use the Internet. People go online to obtain information, communicate with each other and express themselves, to do business and to participate in social and political life.

Citizens have legitimate expectations that their personal data is not abused and governments have a responsibility to protect their citizens' privacy in an increasingly borderless world. That is why Ministers of Justice from 47 Council of Europe Member States at their conference in Istanbul in November 2010 called for the modernisation of Convention 108. They encouraged states from all over the world, NGOs, and the private sector to actively participate in this process.

The modernisation pursues two main objectives: (i) to deal with challenges for privacy resulting from the use of new ICTs. In their Istanbul resolution, Ministers of Justice echoed concerns voiced by civil society and highest jurisdictions in a number of member states when they noted, "that modern information and communication technologies enable observation, storage and analysis of most day-to-day human activities, more easily, rapidly and invisibly than ever before, thereby potentially creating a feeling of being permanently watched, which may impair the free exercise of human rights and fundamental freedoms." (ii) To strengthen the Convention's follow-up mechanism. The effective enforcement of data protection standards is crucial for their credibility. The Committee's functions in this regard could be strengthened, building on the experience and working in association with already existing initiatives such as the "global privacy enforcement network".

If we succeed in modernising and strengthening Convention 108 with the active participation of countries and organisations all over the world, the Convention will eventually fulfil the vision of its drafters, and become a truly international standard for data protection.

OPPORTUNITIES: THE MODERNISATION PROCESS – WHERE DO WE STAND, WHERE ARE WE GOING?

The revision process is in full swing. In March 2011, the Council of Europe's Committee of Ministers fully endorsed the conclusions adopted by the Ministers of Justice. This will be a priority for the Organisation during the next biennium 2012-2013. The Parliamentary Assembly will adopt a report on "Protection of privacy and personal data on the Internet and online media" at its October plenary session, in which parliamentary delegations from OECD member countries will also participate.

On Data Protection Day (28 January 2011), the Secretary General launched a public consultation aimed at hearing concerns of governments, civil society and the private sector. Some 50 replies from all sectors concerned: governments, data protection authorities, NGOs, private sector, professional associations, including many non-European contributors, mainly from the Americas and Africa.

The T-PD will have a first discussion of the results, with a view to defining options for the revision of Convention 108. Participation of Mexico and the US is already confirmed. Consultations on the future of Convention 108 will not only take place in Europe, but also in other regions of the world; in September at the Internet Governance Forum in Nairobi; at the 33rd International Conference of Data Protection and Privacy Commissioners in Mexico (31 October- 4 November); at the margins of the conference, on 31 October, a consultation of Latin American countries will be organised through the Iberoamerican Network on Data Protection.

From 29 November to 2 December 2011, the T-PD plenary meeting is expected to adopt a report on the modernisation already containing as far as possible draft provisions to be included in a revised Convention 108. The report will be used for multi-stakeholder consultations with private sector and civil society, notably in the context of the 2012 Data Protection Day, with a central event in Brussels that we would like to organise together with the European Commission.

The drafting of the legal instruments required for the modernisation will take place in 2012, with the participation not only of the 47 Council of Europe member states and the EU, but also as many other interested countries and organisations as possible.

Finally, I should mention the last element of the SWOT analysis.

THREATS

We are fully aware that setting global standards will not be an easy task. Privacy in the sense of the right to be left alone may not be understood in the same way by individuals living in places as diverse as Dakar, Mexico, Oslo, Washington or Tokyo.

However, our efforts will concentrate on a more limited and yet essential dimension of privacy, the right to the protection of personal data. Everybody, regardless of nationality or residence, has a right to decide how their personal information is collected, used and distributed. This right is the foundation of other freedoms and liberties that define our open societies, in particular freedom of expression.

Another challenge is the sheer speed of technological development which may make our efforts look like the famous race between a turtle and a rabbit, with the regulators always lagging behind. But do we have a choice? Addressing data protection issues with a view to ensuring a trusted Internet-based environment is both a social and an economic imperative. Global online transactions currently total an estimated $10 trillion annually. It will not pass to the predicted $24 trillion by 2020 unless there is confidence not only in security but also privacy.

Instead of the current patchwork of fragmented and unpredictable rules, which are sometimes enforced unilaterally and sometimes simply ignored, we need agreement on some basic norms facilitating the free flow of information and data across borders, while effectively protecting human rights. Transborder data flows will certainly be an issue that we shall have to re-examine in the context of the revision process. At our June meeting, we shall hear the views of a leading expert, the former UK Commissioner, Richard Thomas on this subject.

Only adherence to internationally agreed norms brings legal certainty and predictability to state conduct. Self-regulation and awareness-raising are important, but simply not enough. As the European Court of Human Rights emphasised in many of its judgments, where fundamental values and essential aspects of private life are at stake, state authorities have a duty to establish an efficient regulatory and enforcement framework of protection.

CONCLUSIONS

Convention 108's assets are its legally binding force and its technologically neutral, human rights and principle-based approach. After 30 years, time has come to revisit the Convention's principles, to test their relevance against the new realities of the on-line world and, where necessary, to complement or even amend them.

Without wanting to anticipate the conclusions of our experts and expressing a purely personal view, I would not expect radical changes. The results of the consultation process clearly indicate,

with governments, data protection authorities, private sector, professional associations and civil society all concurring, that the essential features of Convention 108 should be retained. As a Haitian proverb says, a new broom sweeps clean, but the old brush knows all the corners.

The Convention's modernisation process corresponds to the conclusions of the recent G8 summit in Deauville, which encouraged the development of common approaches regarding privacy.

We are well aware that we are not alone in pursuing this exercise. We can count on close collaboration with our partners, in particular in the European Union and OECD. The European Union will soon propose new legislation for its 27 member states. We expect them to be a driving force in negotiations leading to the revision of Convention 108. Consistency with EU law is another message that clearly emerges from the consultations.

But Europe alone is obviously too small to address data protection on a global scale. A thorough and balanced instrument can only emerge if we succeed in bringing closer together the various normative frameworks that have developed in different regions of the world, being prepared to learn from each others' experiences.

At the Council of Europe, we are convinced that a regulatory framework for privacy can only be effective if it is human rights based, facilitates transparency, promotes co-operation and strengthens multi-stakeholder governance.

Let me conclude by calling on all interested parties to actively participate in the modernisation process of Convention 108, which we want to be as international and inclusive as possible.

ENDNOTES

1 This article was written in a strictly personal capacity and does not necessarily reflect the official position of the Council of Europe.

2 Joint Proposal for a Draft of International Standards on the Protection of Privacy with regard to the processing of Personal Data (5 November 2009).

3 Paragraph 19 of Convention 108's explanatory report.

4 "... [I]t should promote the application of the principles set out in relevant EU instruments on data protection and the 1981 Council of Europe Convention on data protection as well as promoting accession to that convention", Extract from item 2.5 of the Stockholm Programme.

5 President Barack Obama, 29 May 2009.

6 www.internetworldstats.com

CLOSING SPEECH OF THE BUDAPEST CONFERENCE

Attila Péterfalvi
former Data Protection Commissioner, Member of the Board of the European Union Agency for Fundamental Rights

The basic subject of the conference was the summary and consideration of present and future data protection challenges. One of the most current issues is to what extent regulations within the Union should be concerted, and what concessions should be made to various national peculiarities? Every panel dealt with this topic directly or indirectly.

Looking back to the last one and a half decade of the data protection directive adopted in 1995, both positive and negative opinions may be voiced. It is a success that the directive was developed; it is a great accomplishment that the committee of data protection authorities, the so-called no. 29 Working Group contributed several positions to help the parties affected by the application of data protection law. However, we still cannot consider the directive as a norm that creates predictable conditions for every affected party. Why not? Two objectives are contained in the title of the directive:

- protection of individuals when handling their personal data, and
- free flow of personal data in the single market.

We could talk about the overwhelming success of the directive if these two objectives had been implemented.

In line with the intention of the organizers of the conference, the panel on the internal market dimension was not meant to sweep under the carpet the difficulties stemming from the lack of harmonization. I believe that the lectures clearly presented the deficiencies that the new legal act should remedy.

The second panel raised extremely interesting questions about the protection of the individual in the so-called cloud computing environment. Losing control over the data comes with a price, the careful consideration of risks and benefits imposes a serious responsibility on users of the service. It was a remarkable point that the providers of cloud computing have never been prepared for a situation where state agencies use their services. Obviously, this issue will receive increasing focus in the future. If it will lead to an improvement of service parameters, then it could initiate a useful process of thinking.

The panel on the education of citizens and promotion of rights approached the issues raised in the program from multiple aspects. The conclusion sounds somewhat alarming: an overly conscious exercise of rights may lead to an overload on data protection authorities, and ultimately to a more difficult exercise of rights. However, we should not accept it in general, the presented efforts need to be supported, and we wish much success to every player with their efforts made in this field.

The panel on the new fundamental principles raised topics that attract mass interest. Especially now, waiting for the proposal on the new data protection regulation, we do a lot of guessing on whether the time is ripe for a European level codification of the new principles. It could contribute to the enhancement of the quality of legislation both at European and national level if the legislator considers the voiced ideas.

Finally, we looked forward to the lectures on global standards with great expectations. Thinking about these is indirectly thinking about the preservation of our joint accomplishments, and ultimately about every citizen of the world. Thinking in this scale is not an exaggeration; what is more, I should encourage all of us to keep seeking common solutions to our common problems, sparing no effort.

PRIVACY AND THE LIABILITY OF INTERMEDIARY SERVICE PROVIDER IN THE CLOUDS. E-GOVERNMENTAL ASPECTS

Wojciech Rafał Wiewiórowski
Inspector General for the Protection of Personal Data, Poland
Faculty of Law and Administration, University of Gdańsk

1. Cloud computing as the business model became last years the leading paradigm in the development of the services offered by business in global network. The model seems to be more and more important in strategies of future development of electronic government systems all over the world. There are, however, important legal questions which still wait to be solved by individual cloud users, business and government entities who want to use clouds for their purposes, as well as by the cloud providers.

The article focuses on privacy and data protection questions which, however, cannot be discussed not mentioning the unsolved problem of the role of the cloud provider as the intermediary service provider (ISP) under European e-commerce law. The scope of this paper does not allow to discuss all these problems comprehensively, and thus the paper should be seen as the invitation – especially directed to those involved in personal data protection issues – to try to develop a European and global discussion on the privacy aspect of the cloud services with the special focus put on the e-government use of the cloud.

2. To start this discussion we have to reaffirm that the cloud computing is not a completely new phenomenon. Moreover, from technological point of view it does not invent the new will. The vast majority of ICT techniques used by cloud providers have been in use before either in telecom sector to enable fast transmission of data between remote sources and destinations or in ICT systems in order to allow numerous virtualization services. For this reasons we can say cloud computing is just a business model which uses and develops the telecom and virtualization technologies in order to give the synergy effect to the number of services already offered as so called intermediary ICT services.

Using the National Institute of Standards and Technology (NIST) definition of cloud computing we can describe it as an ICT sourcing and delivery model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. NIST itself stresses that cloud computing is NOT a new technology[1].

FIVE MAIN FEATURES OF THE CLOUD COMPUTING AS A MODEL INCLUDE:

a) On demand self service where a consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

b) Broad network access capabilities which are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g. mobile phones, laptops, and PDAs).

c) Resource pooling allowing the provider to pool his computing resources in order to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.

d) Rapid elasticity – capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.

e) Measured Service – cloud systems automatically control and optimise resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (for example, storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled and reported providing transparency for both the provider and consumer of the utilised service.

It is important for this discussion that the resource pooling includes a sense of location independence. But such "independence" means that the customer generally has no control or knowledge over the exact location of the provided resources, but may be able – under some circumstances to be discussed – to specify location at a higher level of abstraction (e.g. country, state, or data centre).

CLOUD COMPUTING IS BASED ON THE SERIES OF ICT SOLUTIONS SUCH US:

a) extremely fast and trusted network solutions,

b) large, global infrastructural solutions provided by external partner such as Google or Amazon,

c) virtualisation capabilities,

d) huge data centres,

e) mainly open source software (e.g. Linux, Apache or Hadoop) vastly minimising the costs of data processing in data centres,

f) acceptance of open Web 2.0 standards which make computing for clouds easier and faster.

3. While discussed legal problems apply to all three usually defined submodels –Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a service (SaaS) – all the following suggestions are addressed mostly to IaaS and SaaS, as the Platform as a Service submodel is used for the software development purposes which – in larger scope – include discussion on intellectual property questions which we do not explore here. The only important statement to be made on PaaS at this moment is that many lawyers like the word "platform" in this notion, and (wrongly)

think the use of a platform metaphor makes them easier to transfer the solutions they already use for Web 2.0 services and ISP liability. Such presumption is, however, absolutely wrong as the PaaS cloud computing submodel gives the platform to develop the software and not the "platform" to put the services or content on as it is in classic Web 2.0.

4. Both IaaS and SaaS begin to be more and more important for public authorities both for internal needs of agencies, A2A services and for e-governmental services directed to business and individuals. Two years ago D. C. Wyld has tried to predict the development of governmental cloud services in United States. Taking into consideration the development observed last two years and trying to pass some of these ideas in European ground, we can predict following developments[2].

a) Cloud computing will take off at the European, state and local levels through mostly rogue, "under the radar" initiatives over the next few years.

b) At the European and state levels, there will be a coordinated move to cloud computing, but with inevitable tension between agencies.

c) There will be two to three incidents a year worldwide with potentially massive security breaches, involving much media attention and attendant calls for greater regulation and oversight of cloud providers.

d) There will be much cooperation between private sector firms (seeking to be cloud service providers) and government agencies, with far more data and applications than expected today, transitioning to the cloud over the next decade.

e) Budget pressures will continue to drive more and more government IT to hybrid and even public clouds, as more and more former internal IT functions—and assets (hardware, software, data, and support personnel)—are outsourced with billions in procurement dollars shifting to the cloud.

f) There will be greater use of cloud computing in everything from health care and education to the military and national security.

g) Free cloud offerings - even beyond the e-mail, storage, and application functions found today - will be a significant part of IT portfolios in most governmental agencies.

h) The spillover effect of government use of cloud computing will include faster agreements among major cloud providers on standards and cloud interoperability protocols.

i) There will be significant legal action arising out of governmental uses of cloud computing, and legislation addressing both IT and business needs and consumer fears and protections will be a major focus over the next decade.

j) The "democratization of technology" brought about by cloud computing will impact the quality of our individual online lives, the growth of businesses, and the pace of innovation, benefiting us all[3].

5. There is no doubt that the most of existing legal problems with processing of governmental data in the clouds can be solved according to existing law and almost all arising questions – also those connected with protection of personal data – can be answered in well prepared and right negotiated contractual negotiations. Of course, the cloud provider is usually in much better situation in such negotiations as his business activities, as well as his ICT and practical knowledge on cloud computing is usually much higher than those of his counterpart, but this problem exists in many fields and is a matter of discussion on governmental management and the outsourcing of legal and technical skills. Nevertheless, the potential client of the clouds – no matter if it is individual, business entity or governmental agency – has to be aware of the fact that "common" legal knowledge and even "common" IT law knowledge of the manager and lawyer is most probably not enough to negotiate and close the contract on cloud computing services which would meet all requirements of the privacy protection in the clouds[4].

6. Definitely, there is no single contract standard under existing law which will cover all aspects of cloud computing. It is anyway true that each of the cloud computing contracts has to include both the data protection aspects usually solved in the contact for personal data processing between the data controller and data processor. It shall be remembered both by the cloud provider and the cloud user that, while that is not certain if the e-commerce exclusions for ISP liability (Articles 12-15 of E-Commerce Directive) apply to cloud provider, the problem of civil liability and penal responsibility for data processing in the clouds shall be regulated by the contract in question. At the same time, the standard contractual clauses (e.g. as far as hosting is concerned) have to be used carefully. Most probably they need to be rewritten in the world of cloud computing. The good practices in this field are still welcome.

7. One of the most important parts of contractual clauses – not to be forgotten by the user – should apply to security incidents and data breach notification obligations of the cloud provider and his subcontractors. No general solution exists under contemporary law and the contract is ultimately the only source of such obligations and the only source of rights to assess what security and data protection standard is actually applied by the cloud provider and his subcontractors.

8. Finally, the transparency on providers' private and public obligations is a crucial point. Such transparency is especially important as far as the obligations to cooperate with state security authorities are concerned. In theory we may assume we know, what the obligations of the ISP are as far as cooperation with security agencies is concerned. There is, however, a need to explore the problem at each stage of risk assessment[5]. Let us just use one of often neglected examples of such obligations. Amendments to the Foreign Intelligence Surveillance Act of 1978 made by the US Congress on July 10th, 2008 (H.R. 6304) were focused on increasing privacy of the American citizen in ICT systems. While the Patriot Act can be used to access data held in European countries and further afield, and already Microsoft admitted that it would hand over data, Caspar Bowden points out that "the Patriot Act has become a distraction" against the "real threat to European data". Bowden went on to describe a clause of the Foreign Intelligence Surveillance Act (2008 Amendment), pointing to 1881(a): "Procedures for targeting certain persons outside the United States…"[6].

FISAAA 2008 S.1881 authorizes political surveillance of non-US persons outside the US, and expressly includes Cloud Computing ("remote computing services"). It also prohibits the individual states from investigating, sanctioning of, or requiring disclosure by complicit telecoms or other persons and protects telecommunications companies from lawsuits for "'past or future cooperation' with federal law enforcement authorities and will assist the intelligence community in determining the plans of terrorists."

Immunity is given by a certification process. The certification can be overturned by a court on specific grounds. While it requires FISA court permission to target wiretaps at Americans who are overseas and to cease warranted surveillance of a targeted American who is abroad if said person enters the United States, it *a contrario* allows authorities to make surveillance actions if they are targeted to "remote computing services" and data stored out of the USA and not assigned to an American citizen.

Even taking into consideration the necessities advocated by American legislators, and even not protesting against all FISAAA 2008, the European state agency has to be aware that placing data (including public registers) in the cloud provided by an American company may appear only if the data is fully open – which should mean there is no confidentiality or privacy restriction connected with the data.

Surprisingly enough, it may allow us to come back to some requirements which have been set by American self-regulatory documents. On September 20, 2010, the ABA Commission on Ethics 20/20 Working Group on the Implications of New Technologies issued for comment its "Issues Paper Concerning Client Confidentiality and Lawyers' Use of Technology"[7]. As the American Bar Association makes clear, cloud computing raises "specific issues and possible concerns relating to the potential theft, loss, or disclosure of confidential information." ABA raises especially the issues of:

a) unauthorized access to confidential client information by a vendor's employees (or subcontractors) or by outside parties (e.g. hackers) via the Internet, see id.;

b) the storage of information on servers in countries with fewer legal protections for electronically stored information which can be especially problematic in regulated industries that have highly defined requirements with respect to the handling of such information throughout its life cycle;

c) a vendor's failure to back up data adequately.;

d) the ability to access corporate data using easily accessible software in the event that the corporation terminates its relationship with the cloud computing provider or the provider goes out of business;

e) the provider's procedures for responding to (or when appropriate, resisting) government requests for access to information.;

f) policies for notifying the corporation of security breaches;

g) insufficient data encryption;

h) unclear policies regarding the corporation's ability to "control" its own data;

i) policies for data destruction when the corporation no longer wants the relevant data available or transfers it to a different host;

j) the potential warrantless seizure of corporate electronic mail under the anachronistic Electronic Communications Privacy Act of 1986 ("ECPA"), 18 U.S.C. Section 2510, which includes the Stored Communications Act, 18 U.S.C. Sections 2701-12.

9. The use of classic legal terms in the cloud world may create substantive problems. It applies even to such basic terms as "controller" and "processor" according to the European Data Protection Directive. This issue was addressed by the Article 29 Working Party[8] in the example 8 of its Opinion 8/2010 (WP 179) on applicable law. European data protection commissioners gathered in this body stated: "Cloud computing, where personal data are processed and stored on servers in several places around the world, is a complex example of the application of the provisions of the Directive. The exact place where data are located is not always known and it can change in time, but this is not decisive to identify the law applicable. It is sufficient that the controller carries out processing in the context of an establishment within the EU, or that relevant means is located on EU territory to trigger the application of EU law, as provided in Article 4(1)c of the Directive.

The first decisive step will be to identify who the controller is, and which activities take place at which level. Two perspectives can be identified:

The user of the cloud service is a data controller: for instance, a company uses an agenda service on-line to organise meetings with clients. If the company uses the service in the context of the activities of its establishment in the EU, EU law will be applicable to this processing of data via the agenda on-line on the basis of Article 4(1)a. The company should make sure that the service provides for adequate data protection safeguards, notably with regard to the security of personal data stored on the cloud. It will also have to inform its clients of the purpose and conditions of use of their data.

The cloud service provider can also, in some circumstances, be a data controller: this would be the case when it provides for an agenda on-line where private parties can upload all their personal appointments and it offers added value services such as synchronisation of appointments and contacts. If the cloud service provider uses means in the EU, it will be subject to EU data protection law on the basis of Article 4(1)c. As demonstrated below, the application of the Directive would not be triggered by means used for transit purposes only, but it would be triggered by more specific equipment, e.g. if the service uses calculating facilities, runs Java scripts or installs cookies with the purpose of storing and retrieving personal data of users. The cloud service provider will then have to provide users with information on the way data are being processed, stored, possibly accessed by third parties, and to guarantee appropriate security measures to protect the information".

10. Describing roles and describing the allocation of resources used by the cloud provider for each of users is also essential to the provider. The users do not want to be locked into proprietary platforms."[9] The good example of threats caused by being locked-in the data centre where resources are not properly allocated comes from the USA again. FBI agents had raided a cloud centre to track down illegal activity. The Bureau shut down entire centre to search for evidence of a crime since FBI did not know where the specific data was located. This is the perfect example of searching for a needle in the haystack. Providers should map virtual machines and data to customers. Some hardware and software providers claim they can supply advanced platform metrics and capabilities that allow providers to gauge, track and understand what is happening on both a hardware and management level.

11. In my opinion, the only legal problem which cannot be solved with legal tools which are accessible today is the requirement of control on the side of controller. Passing its data to the processor,

the controller should stay in the position of the controlling party. That should require – among others – the possibility to inspect the way the processor stores and processes the data in question. One can argue that even in "non-cloud" world such requirement is a utopia as many of the controllers lack skills and resources to perform such control. In today's world, however, the controller takes the responsibility for the lack of control, and no matter what are his resources or skills he should be in the position to perform the inspection when it is necessary using e.g. outsourced resources or powers.

In the clouds this requirement is definitely a utopia. There is no technical possibility to perform such control when we operate in public clouds. It may be possible in private clouds, but even there it is quite hard to make it the real control. In public and hybrid clouds any contractual obligation connected with this requirement cannot become reality. Two extreme ways to solve this problem are: a) "forget" about this requirement and skip it at least as far as cloud computing is concerned or b) forbid to use the public cloud when the personal data is processed. Despite the fact that I cannot propose any ultimate solution, I would not advice to follow any of the above mentioned extremes.

Possible solution may arise in the legal acts which will deal with so called Binding Corporate Rules (BCR). If the cloud provider uses BCR which is approved by data protection authorities (DPA) we may pass some inspection powers to the lead BCR DPA. The lead DPA will not be able to perform all duties of the controller, but it can at least inspect the cloud provider as far as the security and the re-use of data are concerned. Such solution may be developed in future data protection frameworks and it can be relatively easily used towards European cloud providers. It is, however, problematic if this is a solution for non-European ones.

11. Summarizing this part of the discussion we may say that main problems constituting legal uncertainty around cloud computing are:

- uncertainty on the place the data is processed while the data protection law is "territorial" and forces the controller to specify such place(s);
- necessity to comply with international data transfer requirements if at least one of the places where the data is processed is located in the "third country";
- accountability of the controller and processor;
- changing roles of basic actors being controller and processor under different circumstances;
- problem of subprocessing;
- position of the parties in negotiating contractual clauses;
- resource allocation on the side of the cloud provider;
- possibility of re-use of the data by the cloud provider;
- transparency of data to public authorities.

12. The issue of changes in the practice of privacy protection with relation to popularisation of cloud computing services was raised by Neelie Kroes, Vice-President of the European Commission and Commissioner for Digital Agenda, during the conference « Les Assises du Numérique » held at the University of Paris-Dauphine on 25th November 2010. She reiterated the standpoint of the European Union that data processing in the cloud is more than technological challenge. Pointing at the danger of losing control over data processing in the cloud, she stated that only further studies on "privacy-by-design" and "privacy-enhancing technologies" combined with recognition of differences as regards implementation of the European rules of personal data protection in particular Member States can bring us closer to solving legal and organisational problems that cloud computing encounters in Europe. [10]

A very important announcement of the Commission, resulting from the aforementioned paper, is the statement that in the light of the European Commission's expectation that Europe will become a free market enabling unconstrained and simultaneously secure personal data exchange the standpoint of the Commission on this model will be "cloud friendly". Such support, however, will be provided only for those clouds which will support protection of personal data in a clear and strong manner. At the same time, attention is drawn to the role of self-regulation as regards data processing in the cloud. There are two ways to build an efficient and trusted market of data processing in the cloud. These are: self-regulation actions taken by the groups of entrepreneurs as well as binding corporate rules[11] set out by cloud providers.

On this occasion, the Commission disputes most frequent accusations directed to the European institutions in the field of privacy protection in data processing. The Commission agrees neither with accusations of protectionism and supporting of European operators, nor with accusations of hampering the modern business model in Europe. In order to fight against the first accusation, the Commission quotes exactly contradicting claims submitted by European operators, which say that the Commission clips their wings. The Commission itself is of the opinion that it plays the same role that has previously been played by European institutions, e.g. on the automotive market where security rules (seatbelts, airbags) have been imposed, which has been recognised at the beginning as an obstacle for competition, and now is seen as a justly enforced step in the right direction that has ultimately led to a situation where safety of the driver as well as marks of the crash tests have become an important part of the competitiveness among producers, improving on this occasion passengers and drivers' safety. Just like physical safety of the passengers and drivers has been "to be or not to be" for the automotive market, privacy protection should be one of the main objectives in creation of cloud services and, perhaps above all, in designing and building of the infrastructure of the cloud itself.

Continuing this metaphor, one shall go beyond the view presented in the paper of Commissioner Kroes, and state that first solutions concerning the safety of drivers and passengers were added to the existing vehicle design (e.g. seatbelts) rather than in-built at the beginning. Then safety was taken into account at the stage of designing a vehicle and at every further stage of its construction. Giving a finished vehicle to safety specialists and asking them for adding a safety function was not enough for the expressions such as "crumple zone" to be used in description of vehicle safety systems. A vehicle had to be designed from the very beginning in terms of its safety, technology and organisation of production as well as materials had to be changed. Such a solution entailed extra costs. Nevertheless, in fact only those who made the rules of driver's and passengers' physical safety to be their vehicle production philosophy eventually stayed at the market.

Equally, in case of ICT systems the idea of "privacy by design" aims at integrating privacy protection into the entire construction of the system. From the stage of its planning and modelling, through all the stages of creation, implementation and maintenance, the privacy protection principles shall be one of the main reference points to be followed by systems' authors. Certainly, such method of design, implementation and maintenance should be used not only for ICT systems, but should also apply to all information processing related projects.

13. At the same time, the Commission draws attention to the fact that the tasks related to personal data protection shall continuously comprise:

a) How do we ensure transparency in the processing of personal data? People should be aware of what they are signing up to. They should have the possibility to review their choice in a user-friendly manner at any time.

b) Data minimisation: what can be done to ensure that just the right amount of personal data is collected, and nothing more?

c) The „right to be forgotten" – how can that work in practice? … Let me be clear: in my view, the issue is not merely about deleting all data. Just like in real life, when you present yourself on the Net, you cannot assume no records exist of your past actions. What matters is that in those cases any data records are made irreversibly anonymous before further use is made of them.

d) Data portability. This is all about freedom of choice: the right for you to change your mind and preference about the services you need. Freedom of choice is only possible when a user can easily and freely transfer his or her data to him or herself and then possibly to another service provider.

e) Efficient use of the resources invested in data protection is important – both for the supervisory authorities and for the industry complying with it. Unnecessary administrative burdens should be removed where possible.

14. It has been previously mentioned that privacy protection and data security may become in the future an important argument in competition among various cloud providers or cloud services providers. Hopefully, it shall come true some day. Nevertheless, it is worth remembering that such situation may also be a kind of threat for the entities dealing with institutional protection of privacy, both at the level of the European Union, and at the level of particular Member States (DPA[12]). It may turn out that particular cloud or cloud services providers will be willing to instrumentally use the requirements of the European law and will convince us that because they built their services based on recommendations of DPAs they have a natural advantage over other cloud or cloud services providers. The very process will not be a threat. However, it will be worse if Data Protection Authorities will let themselves involved in the idea of clouds homologation. I don't think that any of the authorities will be able to issue a quality certificate to a cloud provider for what the latter has done till the time of its issuance or for the activities to be undertaken by him in the coming months or years.

15. The agenda of Commission activities includes:

- 20 November 2009: European Network and Information Security Agency (ENISA) issues report on security risks and benefits of cloud computing.

- 26 January 2010: European Commission outlines future directions for cloud computing research in Europe.
- 19 May 2010: Commission's 'Digital Agenda for Europe' suggests developing EU-wide strategy on cloud computing, notably for government and science.
- December 2010: Commission 'Study on security and privacy regulatory challenges in the Cloud'.
- December 2010: Commission review of economic impact of cloud computing.
- Summer 2011: Commission to consult stakeholders on regulation for cloud computing.
- 2012: Commission expected to propose EU strategy for cloud computing.

ENDNOTES

1 On "cloud" definitions of NIST look: P. Mell, T. Grance: The NIST Definition of Cloud Computing (Draft) Recommendations of the National Institute of Standards and Technology, Computer Security Division Information Technology Laboratory National Institute of Standards and Technology, January 2011 and W. Jansen, T. Grance: Guidelines on Security and Privacy in Public Cloud Computing. Draft NIST Special Publication, Computer Security Division Information Technology Laboratory National Institute of Standards and Technology, January 2011

2 Based on: D. C. Wyld: Moving to the Cloud: An Introduction the the Cloud Computing in the Govenment, IBM Center for The Business of Government 2009, p. 7.

3 More advices directed to the public authorities: Department of Finance and Deregulation: Cloud Computing Strategic Direction Paper. Opportunities and applicability for use by the Australian Government, Australian Government, April 2011; Council CIO, Proposed Security Assessment & Authorization for U.S. Government Cloud Computing. Draft version 0.96, US CIO, November 2010; D. Catteddu, G. Hogben, Cloud Computing. Benefits, risks and recommendations for information security, European Network and Information Security Agency (ENISA), November 2009; D. Catteddu: Security & Resilience in Governmental Clouds. Making an informed decision, European Network and Information Security Agency (ENISA), January 2011; J.Budszus, H.-W.Heibey, R. Hillenbrand-Beck, S.Polenz, M.Seifert, M.Thiermann: Orientierungshilfe – Cloud Computing. Version 1.0, Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, September 2011.

4 D. Catteddu, G. Hogben, Cloud Computing. Benefits, risks and recommendations for information security, European Network and Information Security Agency (ENISA), November 2009

5 The scope of this paper does not allow even to touch the problem of confidential information and state secrets processed in the clouds. This problem requires additional studies targeted to each institution and to each type of confidential or secret information.

6 Z. Whittaker: Facebook rebuked by EU privacy platform; Patriot Act a 'distraction'? ZDNet September

7th, 2011, http://www.zdnet.com/blog/btl/facebook-rebuked-by-eu-privacy-platform-patriot-act-a-distraction/57482 and C. Bowden: Privacy and surveillance on the Internet What happened, and what to expect next…, Panoptykon – Internet at the Crossroads. Warsaw September 20th, 2011, presentation online: http://wolnyinternet.panoptykon.org/sites/default/files/internet_surveillance_caspar_bowden.pdf

7 ABA Commission on Ethics 20/20 Working Group on the Implications of New Technologies: Issues Paper Concerning Client Confidentiality and Lawyers' Use of Technology, ABA September 2010, http://www.infolawgroup.com/uploads/file/letterhead-client-confidentiality-issues-paper-final-9_20_10-1(1).pdf, some comments on the document in T. L. Forsheit: Cloud Computing and Legal Ethics – Recent Perspective from the American Bar Association, the New York State Bar Association, and the State Bar of California, AIPLA Mid-Winter Institute Home 2011.

8 The Working Party on the Protection of Individuals with regard to the processing of personal data established by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 (OJ L 281, 23.11.1995, p. 31).

9 A. Etengoff: Intel says 2015 will be the Cloud computing tipping point , TG Daily March 7th, 2011 http://www.tgdaily.com/hardware-features/54501-intel-says-2015-will-be-the-cloud-computing-tipping-point.

10 N. Kroes: Cloud computing and data protection. Speech at the Les Assises du Numérique conference, Université Paris-Dauphine, 25 November 2010, RAPID Press releases, Speech 10/686, website: http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/10/686&format=HTML&aged=0&language=EN&guiLanguage=en

11 See documents of the Art. 29 Working Party: Working Document on Frequently Asked Questions (FAQs) related to Binding Corporate Rules, WP 155 rev.04, Working Document Setting up a framework for the structure of Binding Corporate Rules, WP 154 and Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, WP 153; all of 24 June 2008.

12 Abbreviation for the English term "Data Protection Authority".

KEYNOTE SPEECH OF THE WARSAW CONFERENCE

Jörg Polakiewicz
Head of Human Rights Development Department, Directorate General of Human Rights and Legal Affairs, Council of Europe

This is the 30th anniversary of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (*Convention 108* for the Protection of Individuals with regard to Automatic Processing of Personal Data).

It is not 30, but more than 60 years that the Council of Europe has been a forum of choice for pioneering work on data protection and privacy. The 1950 *European Convention on Human Rights* guarantees an enforceable right to privacy to every person in Europe, citizens and non-citizens alike.

Numerous legal standards beyond Convention 108 have been developed. As examples, I would like to mention the Committee of Ministers and privacy. The 1950 *profiling*, adopted only last year, and the one on the use of data by the *police*. This latter recommendation R(87) 15, took into account the particular requirements of effective crime fighting. It became even legally binding for EU member states under the Schengen Agreements.

We are currently at a *defining moment for data protection worldwide*. We face an unprecedented challenge to our privacy, but also exceptional efforts by regulators.

The *revision of normative frameworks* is underway in the Council of Europe, the EU and the OECD. New data protection laws have recently been adopted in many countries such as Costa Rica, India, Hungary and Russia. Bills are being debated in various African countries, Brazil, Singapore or the USA.

I am convinced that despite conceptual differences, the frameworks for regulating privacy are on the path to convergence. All these developments highlight two things:

Firstly, where human rights and essential aspects of private life are at stake, *self-regulation is not enough*. Take the example of the USA, where the Children's Online Privacy Protection Act ('Coppa') drawn up over a decade ago is currently being revised by the Federal Trade Commission due to, "an explosion in children's use of mobile devices, the proliferation of online social networking and interactive gaming." Many of the proposals made by the FTC echo concerns expressed in Europe as well, such as updating the definition of "personal information" to include geolocation information or introducing more reliable methods to obtain parental consent.

Secondly, *ensuring data protection in the age of the Internet requires international responses*. When calling for the modernisation of Convention 108 at their conference in Istanbul in November 2010, European Ministers of Justice therefore encouraged states from all over the world, NGOs, and the private sector to actively participate in this process.

The forthcoming *International Conference of Data Protection and Privacy Commissioners* in Mexico City will be a further opportunity for consultations and discussions that we are preparing with the

active support of the Federal Institute for Access to Information and Data Protection (IFAI). In this context, I am delighted to mention that in July *Uruguay* has become the first non-European country invited to accede to Convention 108.

The Council of Europe is not only making sure that its standards are in line with the new technological environment and habits of modern life. It also helps to ensure that those *standards are effectively implemented* and that national authorities have the capacity to do so.

We are currently supporting the Ukrainian authorities with a 12-month project co-financed by the European Commission aiming at ensuring that the Ukrainian data protection system complies with the principles set forth by Convention 108.

Another project has been prepared in cooperation with ECOWAS, the Economic Community of West African States. Its aim is to implement the regional legal framework in compliance with internationally recognised standards. We hope to rapidly ensure funding for this important project which translates so well the borderless nature of data flows and the need for international cooperation.

Finally, let me underline the importance of *close cooperation with the European Union*. Data protection is a good example of the complementarity between the activities of both institutions. On the basis of shared values and human rights standards, the EU adopts comprehensive legislation for its member states, while the Council of Europe sets international standards and provides a dynamic framework for cooperation including like-minded countries well beyond Europe.

I am convinced that we shall work even closer in the future to ensure that our normative frameworks complement and reinforce each other. We owe it to the citizens of Europe for whom the protection of personal data is a basic value. However, attempting to enforce European standards worldwide would be a wrong approach. Instead there is an imperative need to have a set of common minimum standards and collaborate in their effective implementation.

A set of core data protection principles, drafted in a simple and technologically-neutral way - what could be a more fitting description of Convention 108? When modernising it, we shall proceed carefully, maintaining its essential features, complementing and updating them only where necessary. In order to have internationally agreeable standards, it will be essential to build on the experiences gained not only in Europe, but also in other regions of the world.

Our aim is a truly international regulatory framework for privacy that is *human rights based,* facilitates *transparency*, promotes international *cooperation* and strengthens *multi-stakeholder governance*.

EFFECTIVENESS OF PERSONAL DATA PROTECTION PRINCIPLES IN THE CHANGING WORLD

Jacob Kohnstamm
Chairman of the Article 29 Working Party

Even though the groundwork of data protection in the EU will not be fundamentally changed, the revised legal framework for data protection in the EU will most certainly introduce a few new concepts.

This working session is meant to discuss how some of those concepts (notably: privacy by design, privacy impact assessments, and accountability) will need to be implemented in order to ensure *real* data protection. I try to point out my views, as regulator and enforcement authority.

By emphasising the word *real* I hope to have underlined the fact that these concepts are supposed to actually enhance the level of protection.

They should not become just another box ticking exercise which leads to the (false) impression that data are adequately being protected.

WHY IS THE CURRENT DIRECTIVE BEING REVISED?

The review is taking place to ensure data protection in today's globalised world. To enhance the protection of data subjects, for whom it has nowadays become practically impossible to understand what use is made of their data and what potential dangers exist.

Technology is great, we all profit from new technologies every day. But the use of data through new technologies is so widespread and has become so obscure, that the onus now is on data controllers. Data controllers should not only provide us (data subjects) with clear information about processing operations (why, where, how, etc). They should first and foremost take real responsibility for data processing and demonstrate that they have done their data protection homework.

This is what the concepts of privacy by design, privacy impact assessments and accountability are all about: demonstrating that data protection, from the very beginning and at all levels – be it management or workfloor - has been taken seriously, whether it concerns a product or a service.

Privacy should be one of the important first steps when designing, developing and launching new services, not the last. It is important that the best and brightest, when designing and developing new products and services, build in privacy safeguards in order to limit the chance of privacy intrusions or data breaches.

And why is this necessary? Because it forms the essence of trust. People need to trust the services they use and the products they purchase. If they don't trust, they will not buy or buy elsewhere. It is therefore also in the interest of data controllers to get it right at the start; not only for their business' reputation but also because getting it right at the start is a lot cheaper.

THE DATA PROTECTION ENFORCEMENT AUTHORITY, THE DPA ONLY COMES IN AT THE END OF THE PROCESS.

What counts for DPAs is that companies have done their data protection homework. Personal data should be properly protected, without DPAs spelling out each and every step controllers should take to ensure this. Accountability and privacy impact assessments are concepts that are meant to help controllers to take up their role in ensuring data subjects can trust their data is well protected.

ILLUSION OF PERSONAL DATA PROTECTION?

Eng. Wacław Iszkowski, Dr. T.S.
Polish Chamber of Information Technology and Telecommunications

I consider important to highlight in my essay that I represent here the telecommunication operators and Internet access and services providers. They gather TBs of personal data and incur that way quite significant costs of their management and protection. I represent as well the ICT companies which deliver ICT systems and programming tools. The systems and tools are meant to provide for the most effective personal data protection while offering profits to said companies.

This year we celebrate the 30th anniversary of adoption of the Convention for Protection of Individuals in reference to Automatic Personal Data Processing. It is worth remembering that by that time the Internet was yet to be launched. And the number of people understanding operation of computers was truly limited. Since than the European Commission and EU countries have embarked on legal and technical activities to keep pace with the personal data protection. They also wanted to provide for an increasingly fast development of ICT, the Internet, in particular.

Legal rules governing protection of personal data were introduced first by way of directive and then by way of national law. They impose on the companies which gather data concerning individuals the duty to protect content of relevant databases against unauthorized access. And compliance with said duty is expensive. The imperative objective here is the protection of individuals. The protection against ability to make them suffer moral or financial harm done based on the information obtained illegally by physical persons or legal entities. At the same time the rules to govern access of the special services to said data are being refined. Particularly those which describe behaviour and places of stay of natural persons. Data like those are collected by the ICT operators, supplemented recently by the bank and fiscal information. In the line of prevention and fight against terrorism, the services obtained access to such data. Access that is not controlled by the independent agencies for the sake of protection of confidentiality of the services actions.

At the same time campaigns addressed to the citizens are conducted covering the youngest ones who already commonly use the Internet. They are designed to encourage guarding of one's personal data, photos and other information. Said information should not be made available in the Internet without need. Regrettably, the effects of said campaigns are poor. Young internauts, and also the elder ones, boast of their photos and data at the social portals. And the information is often the intimate one. It is worth remembering that in the ICT systems, including the Internet applications serving ones, the data once recorded in are never forgotten. They are consistently gathered in consecutive backups. Instructed "forget" the system responds by just blocking a direct access to them. This does not mean that the data – including their copies in backups – are physically erased in an effective way.

But still it should be remembered that the information technology is not perfect. It fails to guarantee a full security of said data. The new systems and applications which are yet to be fully tested are introduced under economic pressure. They are prone to the "electronic break-ins" by the better

organized groups of hackers and crackers. The people like those often act jointly in criminal designs while sometimes also as individuals of the State services. One is thus justified to ask if there are practical and economically justified technical solutions facilitating a guaranteed protection of the personal data. Protection of the degree we all think of. In October 2007 (it was the 10th anniversary of establishment of the General Inspector of Personal Data Protection in Poland) I said in my appearance that *"Protection of the main personal data was an illusion"*.

This was met with general objection of the lawyers involved in protection of personal data. They said that the statutory provisions were legally sufficient for provision of a complete protection of personal data of every citizen. Now, four years later, I want to repeat that statement, more strongly this time.

ABILITY TO PROTECT EFFECTIVELY THE PERSONAL DATA IS AN ILLUSION. AND THE STATUTORY DEMAND OF THEIR PROTECTION – AS FOUND NOW IN THE ACT – IS NOT JUSTIFIED.

For the lawyers I want to add that I tell that as the IT technician – engineer for years now involved in development of the information technology. From the technical point of view there is no sufficiently effective solution which could be applied for an absolutely reliable protection of TBs of the gathered personal data. Burdening administrator of said data with legal obligations and penal liability makes just "calming down of the society". Making people think that the law provides for sufficient protection of their personal data. And this is not the matter if the data "flow out of some database" and the administrator is brought to justice. The matter is the whole sphere of privacy of every person living in our modern information society.

Let us see a number of examples:

1. In Brussels – the city of European Commission – people at a hotel copy both sides of ID and credit card. And the hotel is owned by an Arabian company.

2. Even the European Commission itself requires of the experts it employs their mailing of the copy of ID or passport. It is interesting to learn the legal ground of that request, and where they keep relevant copies, and for how long. And which General Inspector of Personal Data Protection proceeds with the required supervision.

3. Copying and scanning of ID and other documents makes now a prevalence. It is the practice of the visa offices of embassies, banks, travel offices, showrooms of operators, equipment rentals and many other places. The question is who takes guard of those paper copies, and their electronic versions?

4. It is a general practice now that the personalized city cards are issued in the cities. The cards present not only the photo and name but also the number according to the Universal Electronic System for Registration of the Population. And it was just an intervening by the General Inspector of Personal Data Protection that prevented said data being generally read in Warsaw by the terminal in every transport vehicle. Wonder what is the situation in other cities?

5. Armies of guards who protect even the insignificant institutions or real estates carefully write down, in notebooks mostly, the personal data of visitors. Who and how guards said

notebooks? This is not known even by the General Inspector, may be saved for the notebook of his or her registered office.

6. For the sake of our security the call centres eagerly identify us while recording of the call at the same time. And with our not accepting the recording we can only hang up. Our obtaining of even simple information is conditioned on the statement of the personal data.

7. Once recorded in the portal the profile – our personal data – stays there for good, even after we sign off. In addition "for our security" said portals record also our phone number or identities of our friends. And shareholders of the portals are American, Uzbek, Estonian, Russian, and other companies from all over the world. We certainly do not have to be present at said portals – but let us explain this to our children.

Many examples like these can be still presented. It is sufficient to look around to see how often we disclose or are forced to disclose our personal data in the European Union and off the European Union where we are out any control of their subsequent beings.

Aha, an important remark – discussing an investor from the USA, Uzbekistan, or Arabian or Russian company I do not have any ground to tell that with the potential access to our personal data they can use the same against us to a more significant degree than some EU smart fellow. But the one we are at least able to catch using European Arrest Warrant!

CONCLUSIONS

Let us assume that our main personal data – names, surname, photo and identification number are not subject to protection and can be collected everywhere when somebody decides that their collection is necessary. But then said somebody remains responsible for their protection and storage without necessity to notify accordingly the General Inspector of Personal Data Protection.

Remaining main data can be generally collected as well but still according to our consent given or not after the purpose of collection is explained. In such cases it is not allowed that relevant operation (service, sale, provision of information) is made depend on provision of data (e.g. the right to recording in contact with bank or operator – the voice is the personal data, as well).

In both above-mentioned cases the data collector should understand that he should protect collected data so that no harm or damage is done to their owner by their use. And the role of the General Inspector of Personal Data Protection in said protection can be minor.

One should legally ban copying or scanning of all official personal documents (ID, passport, driving license, etc.) save for the situations discussed in the Act. The documents are just for seeing and can be electronically read for verification of the holder data.

Public entities including special services are allowed to collect the personal data solely according to provisions of the Act which decide their relevant catalogue, purpose and time period of collection.

At the same time the right of the services to collect data from the private entities – telecommunication operators, banks – should be combined with necessary payment of a charge to said entities for said services (let us say – the price with discount). Current free-of-charge access to the data often leads to excessive demands.

The main personal data database of the citizens (PESEL database in Poland[1]) should be accessible free of charge for verification of personal data through inquiries if the personal data delivered to it are correct. Today access to such database is limited to just a few categories of entities. And each inquiry requires payment.

SENSITIVE PERSONAL DATA

Medical and other intimate personal data – sensitive according to provisions of the Act – may be collected only to relevant knowledge of the General Inspector of Personal Data Protection, and only by the entities stated in relevant Acts. The data must be absolutely, under threat of the penal liability, protected in an effective way, and are allowed to be stored just for a specified period of time. The data are much less numerous and are collected less frequently, and only in the well described situations. Thus their protection is more effective though still more expensive. There is no other option here because only single, even accidental; their making available to the public can bring about major troubles to their owner.

RIGHT TO FORGET[2]

One should still support attempts of Commissioner Viviane Reding to include in an EU Directive of the right to forgetting of data. The term being understood as blocking access to them and their copies after the purpose of their collection is no longer the case, or to request of their owner. Exceptions here are the data which must be stored according to the Act or according to the legal financial relations established with their owner.

Worth supporting here are also attempts of the Commissioner to make said provisions concerning forgetting of data become accepted also off the European Union jurisdiction. Supposedly, an assurance of acceptance of said provisions was given to the Commissioner from heads of Facebook, Google and Microsoft during meeting in DAVOS in January 2011. It would be nice if also relevant agencies in the USA, Russia, Israel, and other countries accept these provisions, and forget – block access – to our data collected when we cross their border - after expiry of their visas and when we leave said countries.

Retention period applicable to the data collected by entities for future needs of the special services should be determined statutorily to be 6 – 12 months at the most. Access to such data should be feasible for the services only in their search for the evidence concerning significant crimes. After lapse of the period the data, and the other ones which are not connected to the investigations in progress, should be forgotten through restriction of their accessibility. Relevant activities should be supervised according to a particular procedure by the General Inspector of Personal Data Protection and by the Human Rights Defender.

REQUEST ADDRESSED TO LAWYERS AND LEGISLATOR

It is required that the law is refined to facilitate more effective assertion of claims from natural persons and entities who using personal data held or collected illegally caused

financial damage or moral harm. In special cases, when the number of the harmed persons or the damage is significant, the right to the class action combined with obtaining of penal sanction and awarding of damages, should be vested in the Inspector of Personal Data Protection and the Human rights Defender. Now the law is of a minor effectiveness resulting from the known laziness of the judicial proceedings. The above-presented postulates are just a part of a different view of the problems of personal data protection. The view accepts the current rules of personal data protection and the proposed extensions. But it also introduces different solutions coming closer to the reality and technical feasibilities. The solutions which offer every citizen the freedom of choosing protection and availability of his or her personal data in a modern information society. All that combined with a stronger legal protection should his or her good be violated by somebody.

ENDNOTES

1 Citizen identification number in Poland

2 It should be known that in the ICT systems, including those serving the Internet applications, the data once written in are never forgotten, and are consistently collected in the consecutive backups. Instructed "forget" the system respond with just the blocking of their being directly accessible. This does not mean that the data – complete with their copies in the backups – are effectively physically erased.

THE STATE OF THE ART IN PRIVACY IMPACT ASSESSMENT

David Wright[1]
Trilateral Research & Consulting, London

ABSTRACT

This paper presents some findings from the PIAF project. PIAF is the acronym for a Privacy Impact Assessment Framework. The project, which began in January 2011, is being undertaken for the European Commission's Directorate General Justice. The first deliverable was completed in September. The paper provides some background on privacy impact assessment, identifies some of its benefits and elements that can be used in construction of a state-of-the-art PIA methodology.

INTRODUCTION

The European Commission is expected to issue its proposed revisions to the data protection framework later this year. It signalled some of the changes we can expect in its Communication of 4 November 2010. One of the changes concerns "an obligation for data controllers to carry out a data protection impact assessment in specific cases, for instance, when sensitive data is being processed, or when the type of processing otherwise involves specific risks, in particular when using specific technologies, mechanisms, or procedures, including profiling or video surveillance."[2]

Two months later, work began on the PIAF project. PIAF is the acronym for a Privacy Impact Assessment Framework. The project is being undertaken for the Commission's Directorate General Justice by a consortium comprising Vrije Universiteit Brussel (VUB), Trilateral Research and Consulting, and Privacy International. The objective of the project is to provide a review and analysis of privacy impact assessment methodologies in Australia, Canada, Hong Kong, New Zealand, the UK and US and to make recommendations for an optimised privacy impact assessment framework for Europe, i.e., we aim to take the best elements of existing PIA policies and practices, and commend those to European policymakers.

We have completed work on our first deliverable which can be found on the consortium's website.[3] The first deliverable reviews PIA policies and practices in the six above-mentioned countries plus Ireland as well as 10 case studies of PIA reports. The report also has a set of conclusions which identifies the benefits to organisations of undertaking privacy impact assessments and some of the best elements we have found in our review of existing policies and practices.

The PIAF report represents the state of the art in privacy impact assessment. To our knowledge, it is the most complete compendium and analysis of PIA methodologies, policies and practices yet compiled.

DEFINITION

There are various definitions of PIA, but we define a privacy impact assessment as a methodology for assessing the impacts on privacy of a project, policy, programme, service, product or other initiative and, in consultation with stakeholders, for taking remedial actions as necessary in order to avoid or minimise negative impacts. A PIA is more than a tool: it is

a process which should begin at the earliest possible stages, when there are still opportunities to influence the outcome of a project. It is a process that should continue until and even after the project has been deployed[4].

Although privacy impact assessment has been used in Australia, Canada, New Zealand and the United States since the mid-1990s, the methodology is a relatively new phenomenon in Europe. The UK Information Commissioner's Office published its PIA Handbook in December 2007 and a revised version in June 2009. It became the first country in Europe to publish a PIA guidance. Ireland became the second with the publication of its PIA guidance in December 2010.[5]

These two guidance documents, like those in Australia, Canada, New Zealand and the US, have some good points but also some shortcomings. Thus, Europe has the opportunity to build on the experience of others to develop a state-of-the-art PIA policy and practice. It can also take into account the RFID PIA Framework which was developed by industry and approved by the Article 29 Working Party in February 2011.[6]

While a privacy impact assessment is a methodology for identifying risks to privacy posed by any new project, product, service, technology, system, programme, policy or other initiative and devising solutions to avoid or mitigate those risks, it also offers several important benefits to organisations, their employees, contractors, customers, citizens and regulators.

Among them are the following:

BENEFITS

A PIA has often been described as an early warning system. It provides a way to detect potential privacy problems, take precautions and build tailored safeguards before, not after, the organisation makes heavy investments. The costs of fixing a project (using the term in its widest sense) at the planning stage will be a fraction of those incurred later on. If the privacy impacts are unacceptable, the project may even have to be cancelled altogether. Thus, a PIA helps reduce costs in management time, legal expenses and potential media or public concern by considering privacy issues early. It helps an organisation to avoid costly or embarrassing privacy mistakes.

Although a PIA should be more than simply a compliance check, it does nevertheless enable an organisation to demonstrate its compliance with privacy legislation in the context of a subsequent complaint, privacy audit or compliance investigation. In the event of an unavoidable privacy risk or breach occurring, the PIA report can provide evidence that the organisation acted appropriately in attempting to prevent the occurrence. This can help to reduce or even eliminate any liability, negative publicity and loss of reputation.[7]

A PIA enhances informed decision-making and exposes internal communication gaps or hidden assumptions about the project. A PIA is a tool to undertake the systematic analysis of privacy issues arising from a project in order to inform decision-makers. A PIA functions as a credible source of information. It enables an organisation to learn about the privacy pitfalls of a project, rather than having its critics or competitors point them out. A PIA assists in anticipating and responding to the public's privacy concerns.

A PIA can help an organisation to gain the public's trust and confidence that privacy has been built into the design of a project, technology or service. Trust is built on transparency, and

a PIA is a disciplined process that promotes open communications, common understanding and transparency. An organisation that undertakes a PIA appropriately demonstrates that the privacy of individuals is a priority for their organisation. It affirms that an organisation has addressed privacy issues and has taken reasonable steps to provide an adequate level of privacy protection.

An organisation that undertakes a PIA demonstrates to its employees and contractors that it takes privacy seriously and expects them to do so, too. A PIA is a way of educating employees about privacy and making them alert to privacy problems that might damage the organisation. It is a way to affirm the organisation's values.

A proper PIA also demonstrates to an organisation's customers and/or citizens that it respects their privacy and is responsive to their concerns. Customers or citizens are more likely to trust an organisation that performs a PIA than one that does not. They are more likely to take their business to an organisation they can trust than one they don't. We assume regulators are likely to be more sympathetic towards organisations that undertake PIAs than those that do not.

ELEMENTS IN GOOD POLICY AND PRACTICE

The extent to which an organisation can achieve these and other benefits depends on the elements that go into the construction of a PIA policy and practice. From our review of PIA in the seven aforementioned countries, we have identified various elements that should be included in a PIA framework for Europe. Among them are the following:

- *Roles – Who initiates a PIA and who approves it?*

A PIA policy should clarify who should initiate a PIA and who should approve it. Typically, responsibility for initiating the PIA should fall on the shoulders of the project manager. The organisation's privacy officer should provide guidance. The PIA should be signed off by a senior executive who is held accountable for its adequacy.

- *Threshold analysis – Is a PIA necessary?*

An organisation should perform a preliminary threshold analysis of every project to determine whether a PIA is necessary. Threshold analyses typically consist of a set of questions to help uncover potential impacts. Many PIA methodologies include a threshold analysis.

- *Clarity for whom the PIA is prepared*

Those undertaking a PIA should be clear for whom they are preparing it – e.g., for senior management, for the regulator, for stakeholders, for the public.

- *Process*

A PIA should be regarded as a process. It is not about preparing a report, although a report helps document the process. It is a process that should start when a project is in the early planning stages and should carry on throughout the project's life. New risks may emerge as the project progresses.

• *Scale and scope of the PIA*

The scale and scope of a PIA should generally be in line with the scale and scope of a project. A more elaborate PIA – and more resources for carrying it out – will be needed for a complex project.

• *PIA starts early*

The sooner a PIA starts, the better. It should start early enough so that it can influence the design of a project. It is useless if it is undertaken after all the decisions have been made.

• *Privacy, not just data protection*

The Commission has used the term "data protection impact assessment", but we hope that it will drop that terminology in favour of "privacy impact assessment". PIA is the terminology that has been used by all other countries, and we think that using the term DPIA risks sending the wrong message to organisations. Informational privacy is only one type of privacy. Roger Clarke and others have identified other types of privacy that are also important – privacy of the body, privacy of communications, privacy of location, privacy of behaviour. If industry and governments think the Commission's main or only concern is with data protection, informational privacy, then these other forms of privacy could be brushed aside.

• *PIA as part of risk management*

Most PIA guidance documents say that PIA should be viewed as part of an organisation's risk management practice. We agree. PIAs are about identifying risks and finding solutions. They should not be seen as somehow distinct from risk management, as an administrative burden.

• *Questions to identify risks and solutions*

All PIA guidance documents contain a set of questions to help project managers and those carrying out PIAs to identify privacy risks. Usually, the questions require more than a yes or no response; respondents must provide some details to support their yes or no. The responses to the questions often serve as the basis of the privacy impact assessment report.

• PIAs are only as good as the processes that support them

In its audit of PIAs undertaken in the Canadian government, the Office of the Privacy Commissioner (OPC) commented that how an organisation complies with the government's PIA policy presupposes the existence of some administrative structure to support the policy's objectives and requirements. The OPC said key elements of a sound infrastructure should include:

• Programs in place to inform staff and other stakeholders of the policy's objectives and requirements;

• Formally defined program responsibilities and accountabilities;

• The existence of a system to effectively report all new initiatives that may require a PIA;

- The existence of a body composed of senior personnel charged with reviewing and approving PIA candidates;

- The existence of an effective system of monitoring compliance with the PIA policy;

- Adequate resources committed to support the organisation's obligations under the policy.[8]

• *Training and raising awareness of employees*

Coupled with the above, and to embed PIA within its culture and practices, the organisation needs to install an ongoing employee awareness program, effectively raising the profile of PIAs and regulatory requirements for their performance with program managers and new hires. Creating general awareness of the policy requirements respecting privacy is often the first step towards ensuring that program managers fully consider the privacy impacts of their plans and priorities at the time an initiative is conceived.[9]

• *Mandatory PIAs*

Undoubtedly, a contentious issue is whether PIAs should be mandatory, as the Commission indicates in its Communication. PIA is already mandatory in Canada, the UK and the US, at least for government agencies. They are also mandatory for the private sector in certain other instances, for example, involving health care or biometrics. There is a strong case for mandatory PIA, as the Commission indicates, in projects involving sensitive data, surveillance and profiling. Unless they are mandatory, many organisations may not undertake them even though their projects, technologies or services have serious privacy impacts. Nevertheless, the logistics of mandatory PIA are not so straightforward. Mandatory PIA would need to be complemented by audits and, desirably, publication and stakeholder engagement.[10]

• *Engaging stakeholders*

The ICO PIA Handbook puts a strong emphasis stakeholder engagement and consultation. The ICO is of the view that if a PIA is undertaken solely from the viewpoint of the organisation itself, it is likely that risks will be overlooked. It therefore recommends that stakeholder perspectives are considered.[11] Australia's PIA Guide makes a similar point. It says "Consultation with key stakeholders is basic to the PIA process." It adds that a PIA should always consider community privacy attitudes and expectations. Affected individuals are likely to be key stakeholders, so wider public consultation is important, particularly where a lot of personal information is being handled or where sensitive information is involved. Public consultation also adds to community awareness about the project and can increase confidence in the way the project (and the organisation) is handling personal information.

• *Recommendations and an action plan*

It is not sufficient for a PIA report to simply make a set of recommendations. An action plan is needed to ensure those recommendations are implemented or, if not, some explanation given as to why some recommendations are not implemented. If PIA is viewed as a process, then the process should continue after preparation of the PIA report to ensure recommendations are implemented.

• *Publication of the PIA report*

Under the US E-Government Act of 2002, government agencies are obliged to publish their PIA reports unless it is necessary to protect classified, sensitive or private information contained in the assessment. Even in such exceptions, the organisation could redact the sensitive information. In Canada, agencies are obliged to publish somewhat detailed summaries, but publication of the full report is obviously better, as it will instil greater confidence that the organisation has identified the privacy risks and is adopting measures to counter those risks. The report creates another opportunity for gathering stakeholder views.

• *Third party audits and monitoring implementation*

In the first instance, the organisation itself is responsible for implementing the recommendations (at least, those with which it agrees). In some instances, the data protection authorities or privacy commissioners may need to monitor implementation. The utility of third party audits, such as those performed by the Government Accountability Office (GAO) in the US and the Office of the Privacy Commissioner in Canada show the utility of audits, including from the perspective of the organisation itself. Audits lead to improvements in PIA practice.

• *PIAs, state security and commercially sensitive issues*

State security and commercially sensitive information need not – should not – be legitimate reasons for not conducting a PIA. Where there are legitimate concerns about making those PIAs public, ways can usually be found to deal with the concerns – for example, through redaction of sensitive information, third-party audit, oversight by the data protection authority and the engagement of external stakeholders through non-disclosure agreements.

• *Accountability*

Accountability can arise from a requirement that a completed PIA be included in program and funding approval processes. Accountability for PIA completion can also be enhanced by mandatory reporting requirements. Notification and public disclosure are important instruments of accountability to the public. A senior executive at the board level should be accountable for the adequacy of a PIA.

• *Tying PIAs to budget submissions*

In Canada and the US, PIAs are tied to budget submissions. In Canada, government institutions must complete and forward a PIA to the Treasury Board of Canada Secretariat to accompany submissions for funding new programs and projects, and in the US, government agencies must include a PIA with submissions to the Office of Management Budget.

• *A central registry of PIAs*

One of the recommendations from the audit done by the Privacy Commissioner of Canada is that the government should create a central registry for PIA summaries, as has been done in British Colombia and Alberta. We view this as a good practice. It helps create a body of knowledge so

that project managers and assessors can learn from the experience of others. It is also useful for greater transparency and for simplifying the search process.

CONCLUSION

Our review of PIA methodologies and reports show that there are similarities as well as differences among the seven countries. Europe can benefit from their experience by drawing upon their best elements to create its own state-of-the-art PIA policy and practice. This paper has presented some of the elements that can be used to construct an optimised PIA.

For further information:

Wright, David, "Should privacy impact assessments be mandatory?", *Communications of the ACM*, Vol. 54, No. 8, August 2011. http://cacm.acm.org/magazines/2011/8

PIAF Deliverable D1, September 2011. www.piafproject.eu

Wright, David, and Paul De Hert (eds.), Privacy Impact Assessment, Springer, Dordrecht, 2012 [forthcoming]

ENDNOTES

1 The views expressed in this paper are those of the author alone, and are in no way intended to reflect those of the PIAF consortium. Comments on this paper are welcome and can be sent to david.wright@trilateralresearch.com

2 European Commission, A comprehensive approach on personal data protection in the European Union, Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, COM(2010) 609 final, Brussels, 4.11.2010. http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf

3 www.piafproject.eu

4 The word "project" is used in this paper in its widest sense, to include any technology, product, service, programme, policy or initiative that may impact upon privacy.

5 Health Information and Quality Authority, Guidance on Privacy Impact Assessment in Health and Social Care, Dublin, December 2010. http://www.hiqa.ie/resource-centre/professionals

6 The PIAF project does not include a review of the RFID PIA Framework which was published several months after our consortium submitted its proposal to DG Justice. A copy of the RFID PIA Framework can be found here: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_annex_en.pdf. The Art 29 Working Party's Opinion on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications can be found here: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_en.pdf

7 Health Information and Quality Authority, Guidance on Privacy Impact Assessment in Health and Social Care, Dublin, December 2010, p. 14.

8 Office of the Privacy Commissioner of Canada, Assessing the Privacy Impacts of Programs, Plans, and Policies, Audit Report of the Privacy Commissioner of Canada, Ottawa, 2007, p. 9.

9 OPC, 2007, p. 17.

10 For more on this issue, see Wright, David, "Should privacy impact assessments be mandatory?",Communications of the ACM, Vol. 54, No. 8, August 2011. http://cacm.acm.org/magazines/2011/8

11 ICO, PIA Handbook, p. 56, p. 58.

A TAILOR-MADE DATA PROTECTION FRAMEWORK FOR THE EUROPEAN POLICE OFFICE

Daniel Drewer
Head of the Data Protection Office of the European Police Office (Europol)

Europol supports Member States in the fight against organised crime and terrorism. In line with this specific mandate Europol operates a comprehensive and robust data protection system.

Europol's system is based on the same principles of data protection contained in the 108 Convention (of the Council of Europe), as well as the European Directive (95/46/EC), but tailor-made to the specific mandate and tasks of Europol and its operational needs.

The Europol Council Decision contains very detailed provisions on data protection and data security, which were further developed by

- the Council Acts related to the Rules applicable to Analysis Work Files,
- the Rules on relations with Third Parties,
- the Rules on Confidentiality, and
- strict conditions related to the processing of data for the purpose of determining the relevance of data.

These rules cover all Europol's processing operations within Europol's mandate to fight organised crime and terrorism.

This framework has functioned for over 11 years. About one hundred analysts process personal data at our headquarters on a daily basis.

What does this mean in practice?

We apply very strict time limits. All personal data must be reviewed at the latest after three years. Accuracy of data, therefore, is not only a goal for Data Protection Officers, but our analysts also have a vital interest that data contributions are up to date.

Every processing action on our system is logged for later verification of the legality of retrieval.

Sensitive data can only be processed under strict conditions and with the agreement of the supervisory authority.

Handling codes are used to ensure the marking of information with the applicable data protection safeguards. Classification levels are used to ensure that the relevant security measures are applied to the data.

Europol receives over two hundred data subject requests from individuals per year. Appeals against Europol's decision on the right of access can be submitted to the Joint Supervisory Body (JSB).

As soon as personal data is processed electronically, systems have to be accredited to ensure a baseline of data security.

Europol's data processing activities are monitored in-house by a Data Protection Officer who is independent in his judgement.

Last, but not least, compliance with data protection relies to a great extent on the quality and efficiency of its supervision. The JSB has the possibility to closely cooperate with national data protection authorities, which is of additional value when it comes to the supervision of systems operated by Europol, but with personal data still under the responsibility of Member States' national police forces. Since the start of Europol's activities in 1999 the JSB has conducted regular inspections and possesses a wide experience in the police sector.

This raises the question whether a future "one-fits-all" data protection regulation for the EU would be the best option for Europol. This is not about rejecting new obligations, but about the possible risk of lowering the level of data protection safeguards at Europol.

There is no discussion about the fact that fundamental principles of data protection should be fully applicable to all areas of EU competence, including police and judicial cooperation in criminal matters.

There should be careful consideration of the sensitive nature of the operational activities and specificities of data processing activities in the area of police cooperation.

This is particularly important in areas such as the legitimate grounds for processing of personal data, as consent plays no role in the context of the operational activities of Europol and for law enforcement in general. The mere fact that Europol is processing an individual's data in its databases could lead to ongoing national investigations being hampered. There is a need therefore to pay particular attention to and to create specific rules for the processing of personal data on such vulnerable data subjects as persons who are suspects in criminal investigations, victims and witnesses. Specific agreements are required for the transfer of data to third countries and there is a need to have data protection and data security safeguards regulated for Europol in one coherent set of rules.

Declaration 21 adopted with the Lisbon Treaty is particularly important for Europol. It reads: the Conference acknowledges that specific rules on the protection of personal data and the free movement of such data in the fields of judicial cooperation in criminal matters and police cooperation … may prove necessary because of the specific nature of these fields.

Post-Lisbon, Europol's tailor-made and complete set of data protection rules will remain essential for our activities.

THE INFLUENCE OF EUROPEAN DATA PRIVACY STANDARDS OUTSIDE EUROPE: IMPLICATIONS FOR GLOBALISATION OF CONVENTION 108

Graham Greenleaf[1]
Professor of Law & Information Systems, University of New South Wales

ABSTRACT[2]

Seventy-eight countries, from almost all regions of the world, have now enacted data privacy laws covering most of their private sectors. Enactment of laws outside Europe is accelerating. Before long, the majority of the world's data privacy laws will be found outside Europe. This geo-political change has implications.

First, by examining the most important differences between the two European privacy standards (the EU Directive and the Council of Europe Convention 108) and the two non-European standards (the OECD Guidelines and APEC Framework), it is possible to identify what can reasonably be characterised as 'European influences' on data privacy laws outside Europe. Examination of the current 29 national data privacy laws outside Europe shows that the 'European standards' have had by far the greater influence outside Europe, and this is increasing.

Second, the Council of Europe data Protection Convention (Convention 108) and its Additional Protocol are examined from the perspective of the possibility and desirability of their becoming a global international agreement on data privacy. It is argued that there are potential considerable advantages to both non-European and European states if Convention 108 (plus the Additional Protocol) were to become a global privacy agreement through accession of non-European states. However, for such globalisation to occur, the Council of Europe will have to settle and publicise appropriate policies on accession that are appropriate, transparent, and do not reduce European data privacy standards.

Europe has no reason to retreat from its privacy standards developed over forty years. The rest of the world is moving its way, and it should not compromise fundamental standards for the sake of compromise with powerful outliers, particularly the USA and China. Respect for their domestic prerogatives should not be confused with any need to reduce fundamental aspects of global data privacy standards.

ENDNOTES

1 Professor of Law & Information Systems, University of New South Wales. Australia. This paper was developed while the author was a Visiting Fellow at the AHRC-Script Centre, Faculty of Law, University of Edinburgh. An earlier version was presented to the International Data Protection Conference, Polish Data Protection Authority (GIODO), 21 September 2011, Warsaw. Parts of the paper are based on a chapter 'Global data privacy in a networked world', to be published in the I Brown (Ed) Research Handbook on Governance of The Internet, Edward Elgar Publishing, Cheltenham, 2012 (in press). Very helpful comments were provided by (in alpha order) Inês Antas Barros, Colin Bennett, Lee Bygrave, Magda Cocco, Robert Gellman, Marie Georges, Chris Hoofnagle, Christopher Kuner, Pablo Palazzi, Jörg Polakiewicz, Charles Raab, Daniel Solove, Blair Stewart, and Nigel Waters, but responsibility for all content remains with the author. Assistance with the Table in this paper is acknowledged separately with the Table. Comments are welcome to <graham@austlii.edu.au>.

2 This abstract is of an expanded version of the Conference presentation, for publication in International Data Privacy Law, Volume 2, Issue 2, 2012 http://idpl.oxfordjournals.org; a copy of this draft is at http://www2.austlii.edu.au/~graham but please cite the final version. You can find the whole essay in the Annex.

THE MODERNIZATION OF THE CONVENTION OF THE COUNCIL OF EUROPE FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA (ETS NO. 108): MOVING FROM A EUROPEAN STANDARD TOWARDS A UNIVERSAL STANDARD FOR DATA PROTECTION?

Jean-Philippe Walter
Deputy Federal Data Protection and Information Commissioner (Switzerland),
Chair of the Consultative Committee "Convention 108"

1. INTRODUCTION

The year 2011 marks the 30th anniversary of the Convention of the Council of Europe for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108). Throughout this year, it's an opportunity for us to review progress as well as look into the future. Since the adoption of the Convention, the world of information and technology have changed dramatically. Nowadays, information technology has been democratized; it is accessible to all and omnipresent, yet without being transparent. Without losing its centralizing dimensions, it became ubiquitous and multifunctional and each one of us has at least one computer or mobile phone. Information flows easily and is accessible from all parts of the world, but this does not mean that all citizens of the world enjoy the same rights and equal protection with respect to the ecosystem of the data concerning them and the existence of which they are generally unaware of.

If the objective of the Convention as set out in Article 1 remains valid, or becomes even more actual, it is advisable:

- First, to examine whether the current text of the Convention and its Additional Protocol meet the needs of modern data protection in order to guarantee the citizens of member countries of the Council of Europe the respect of their rights and fundamental freedoms and ensuring their control over the data concerning them in a most complex and globalized informational and communicational environment?

- Second, to see if and to what extent these texts are likely to be the basis of a binding universal standard for data protection.

In order to address these questions, we need to examine the highlights of the Convention and identify the improvements needed to meet the current evolutions.

2. THE STRENGTH OF THE CONVENTION

Among the highlights of the Convention, let me reiterate the following:

- The Convention is the reference text of many international and national texts, beginning with Directive 95/46/EC, which constitutes a development of the principles of the Convention.

- With the Additional Protocol, this is the first and only binding international document governing the protection of data. Up to now, 77 countries from 5 continents have adopted a law on data protection. Over half of these states are parties to the Convention. It has indeed been ratified by 43 of the 47 member states of the Council of Europe, including the 27 member countries of the European Union.

- It sets out the basic principles of data protection that are universally recognized and its binding legal standards are fully consistent with other legislation such as the OECD guidelines or even more so with the guiding principles of the United Nations.

- The Convention was written in a simple and general manner and follows an approach known as "technologically neutral", keeping the fundamental legal standards it contains up-to-date and enabling adjustment to technological developments without lowering the level of protection or exclude additional protection according to the needs and situations.

- It is horizontal in application, covering all automated data processing of the private and public sector, including in the field of police and justice.

- By harmonizing the right to privacy and the freedom of information (including the right to the free movement of data regardless of borders), it guarantees a high level of protection in accordance with the existing legal systems and ensures in principle the free movement of data between State parties while requiring (through the Additional Protocol) an adequate level of protection for the transfer to countries not party to the Convention.

- The Convention regulates the cooperation between the Parties and assistance to those affected regardless of their nationality or place of residence. It establishes a platform for multilateral cooperation through the Advisory Committee.

- Developed with the participation of States that are not members of the Council of Europe (United States, Canada, Australia and Japan), the Convention is not a strictly European text. It is open to accession by third countries, which gives it a universal potential.

3. NECESSARY ADJUSTMENTS

Although the provisions of the Convention and Additional Protocol remain relevant and are still fully applicable to different personal data processing, the fact remains that we must consider some adjustments to better meet the challenges of technological developments, their multifunctional uses and mass effects hanging over privacy and the right to data protection.

The Advisory Committee of Convention 108 has initiated this reflection last year and began work to modernize the Convention and its Additional Protocol. This work pursues three main objectives, namely:

- to meet the challenges relevant to the right to data protection and privacy resulting from the use of the information and communications technologies;

- to strengthen the implementation and monitoring mechanisms of the Convention;

- The working method that we follow - and this is the third objective - favours an open and multi-party approach. We want to involve not only all members of the Council of Europe, whether or not they are part of the Convention, but also third countries from all regions of the world to provide a better basis for the opening option of the Convention and to take into account the basic requirements for the protection of data that each legal system should be able to achieve. We obviously count on the contribution of the European Union and we also wish to integrate into the working process the private sector and civil society, including the NGOs as well as the authorities responsible for data protection. It seems indeed essential to emphasize a dialogue including all stakeholders in order to develop standards that are effective and accepted by all. Based on a preliminary report from the Research Center on IT, Law and Society at the University of Namur, the Council of Europe has launched earlier this year a public consultation to which we received over 50 responses from States, associations or professional bodies and representatives of civil society from around the world.

From the responses to the 30 questions, four major trends emerge that will guide the work of the Advisory Committee:

- First, the general, flexible, simple and pragmatic nature of the provisions of the Convention should be maintained and supplemented by more detailed sectoral laws on the basis of the recommendations of the Council of Europe.

- It is then necessary to ensure consistency and compatibility with the legal framework of the European Union.

- The technology-neutral character of the provisions of the Convention must be maintained.

- Finally, the universal and open nature of the Convention should be preserved and promoted. It is thus considered important for the text not to be too detailed in order not to compromise the international character of the text.

Based on the summary report prepared by the team of Namur, the Office of the Advisory Committee began considering the items that could justify modifications:

a) Object and purpose of the Convention

In relation to the object and purpose of Convention 108, we consider the need to strengthen the right to data protection, in particular by assigning it to Article 1 in a more affirmative way. In this sense, the agreement would guarantee individuals their right to data protection, namely the respect of their rights and their fundamental freedoms with regard to the processing of the personal data that concern them.

b) Definitions

In terms of definitions, an update seems necessary in particular concerning the concepts of file, processing and controller of the file. This is in particular to ensure greater consistency with more recent legislation including the European Directive.

c) Scope

As far as the scope of the Convention is concerned, there is unanimity among the respondents to support the fact that the Convention must continue to cover the private sector as well as the public sector, including the police and justice. Exceptions are possible but within the limits of the current Article 9. On the other hand, we must consider the possibility of incorporating an exception for so-called domestic processing. This is a difficult question because with the development of information technology and communications, including social networks, the domestic character of processing has taken new dimensions.

d) Basic principles

As far as the basic principles of data protection are concerned, a tendency emerged from the consultation, according to which these principles are sufficient to cover the different situations of personal data processing. However, we ponder the possibility of including more explicitly the principles of proportionality and data minimization. On the other hand, some skepticism emerges about the introduction of the "privacy by design" principle, which is the obligation to apply the principles of protection as early as the design of the equipment and applications, and the principle of "accountability" or reinforced liability, on the grounds that these aspects are already covered in part by the basic principles. Some favour the introduction of a requirement to the controller to perform a risk analysis on data protection and respect for private life prior to the collection and processing of personal data.

e) Lawfulness of processing

Currently the Convention does not develop the grounds that may justify the processing of personal data. Article 5 stipulates simply that the collection and processing have to be lawful. Without going into detail, some clarifications could be made regarding the grounds of legitimation of the processing. We refer in particular to consent and the law.

f) Sensitive data

As far as sensitive data as defined in Article 6 of the Convention is concerned, we believe in maintaining the current system and not to complete the list of categories of so-called sensitive data. It is nevertheless accepted that on the one hand a Contracting State may complete the list of sensitive data and on the other hand, according to the context of processing, it may be legitimate to strengthen guarantees to protect data even if the data are not by definition of a sensitive nature.

g) Data security

In terms of data security, we believe that it is appropriate to introduce the obligation to report security breaches. However, this obligation should be limited to serious and significant cases. The terms of these reports must also be defined. In addition, security must not only be passive, but develop into active obligations, including the obligation to design systems that make it possible to minimize the risk of data security and privacy breach.

h) Rights of data subjects

The rights of data subjects should also be strengthened in order to ensure them full control over their data and the respect of their right to human dignity and non-discrimination. These include reviewing the extent of the right of access and improve the information of those concerned. We also examine the introduction of new rights, including the right not to be subjected to an automated decision. At the heart of the debate is also the question of the right to oblivion, which remains a contentious issue. Instead of an actual right to be forgotten, some prefer the option of a right to object to processing, coupled with clarification on the obligations on limited data conservation and the right of rectification or deletion of data, already anchored in the Convention.

We also examine the need to strengthen sanctions and possible action and/or recourse for those concerned. While some believe that it is for the Contracting States to provide for sanctions and recourses, others would prefer to see the Convention establishing these sanctions, as well as the development of various forms of recourse and actions for those concerned.

i) International cooperation

International cooperation, expertise and the independence of data protection authorities, as well as the system of transborder data flows are also at the center of current debate and will require some adjustments in either the Convention or through recommendation. Thus the responsibilities and powers of the Advisory Committee could be strengthened with particular reference to the assessment of the level of protection provided by States wishing to adhere to the Convention and to the development of dynamic monitoring mechanisms. Its opinions should also be more binding on States parties.

j) Data protection authorities

As for data protection authorities, it is primarily about improving cooperation between them, especially to enable joint investigations, strengthening their powers and improving harmonization. The outlines of independence should also be specified.

k) Cross-border data flow

On the subject of cross-border data flows, the principle of adequate level is not questioned. On one hand this is about bringing closer section 12 and the Additional Protocol and, on the other, to consider new developments which, while guaranteeing a high level of data protection, facilitate the exchange of data without unnecessary obstacles. The Convention must continue to provide a sound base to allow the free flow of information between the Parties who, by their ratification or accession, provide sufficient guarantees of a high and more than adequate level of data protection. The notion of cross-border flows in relation to the Internet also deserves clarification.

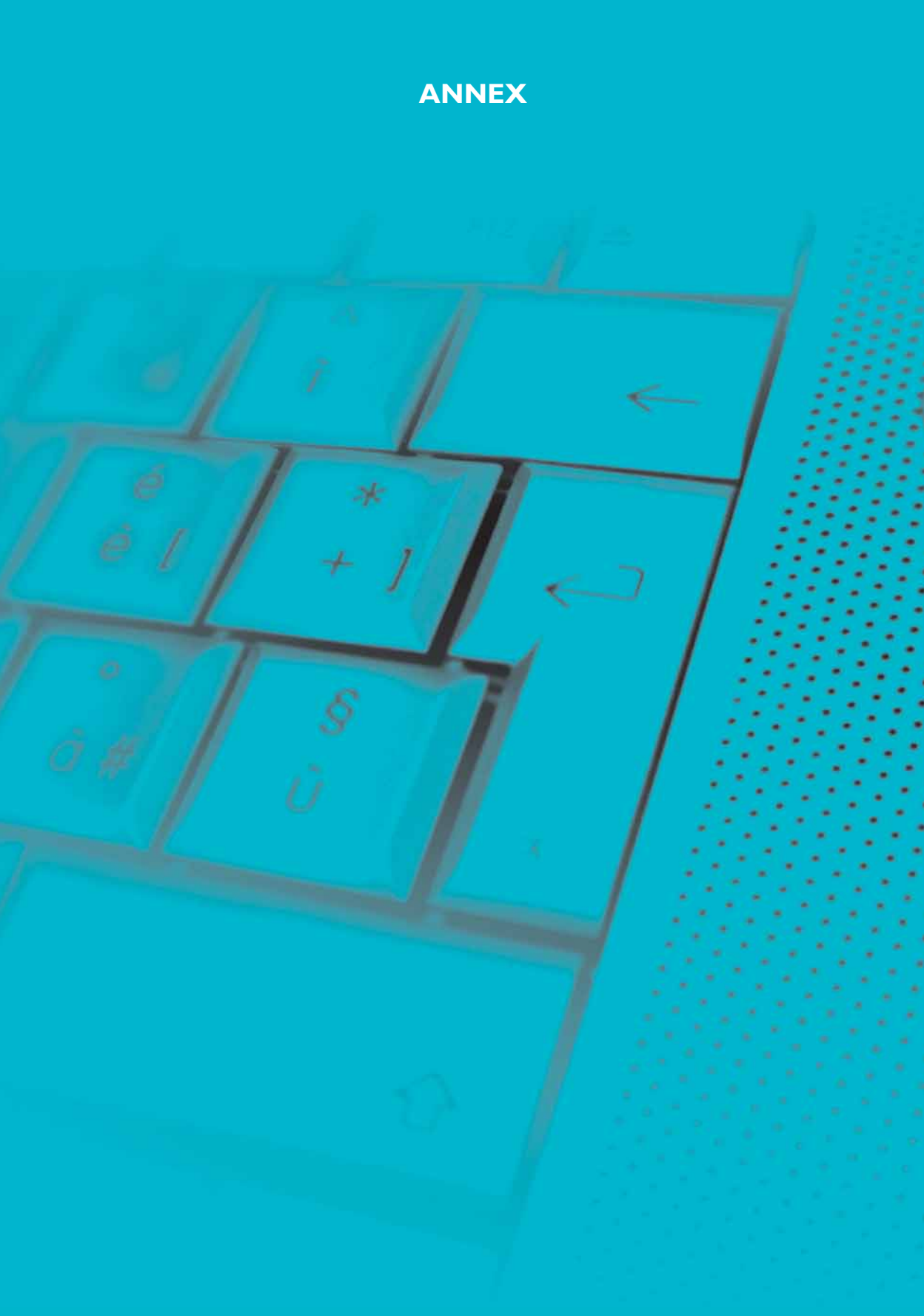
4. CONCLUSIONS

The task of modernizing the Convention and its mechanisms of implementation is one of the priorities of the Council of Europe and the Advisory Committee. The latter should be able to review a first draft at its next plenary session in late November. The objective is

to present to the Committee of Ministers a draft for adoption at the end of 2012. Meanwhile, the Council of Europe is strengthening its policy of worldwide promotion of the protection of data and of the Convention in particular. Membership of other States is indeed a way to strengthen data protection in the world while allowing data exchange and cooperation between the Parties. A first non-European country, Uruguay has been invited by the Committee of Ministers to join the Convention and this adhesion could become reality in 2011.

More than ever, Convention 108 and the Council of Europe play a central and fundamental role in the development of a universal right or standard for data protection. Convention 108 and its Additional Protocol, I believe, contain a unique potential to become the major standard of a universal law of data protection and offer joining third States an opportunity to be recognized as adequate. As the number of adhering states grows, we move towards an area of freedom, security and justice, ensuring the protection of personal data and people's rights beyond European borders. In this process of modernization, we must give priority to dialogue with all stakeholders, be open to different legal systems and be able to recognize their contributions in order to reach a strong and universal standard and to ensure maximum consistency between our different approaches to data protection and privacy. Beyond the norms and principles of data protection, we must also pay particular attention to implementation and think about reinforced collaborative structures with genuine powers, so that data protection can become truly effective and a reality. Intervening in a disorganized manner against companies like Google or Facebook can only weaken the impact of data protection in Europe and worldwide.

ANNEX



FROM THE PRINCIPLE OF ACCOUNTABILITY TO SYSTEM RESPONSIBILITY – KEY CONCEPTS IN DATA PROTECTION LAW AND HUMAN RIGHTS LAW DISCUSSIONS

Professor Paul De Hert
Vrije Universiteit Brussel (LSTS) & University of Tilburg (TILT)[1]

1. INTRODUCTION: WHO CARRIES WHICH RESPONSIBILITIES IN THE INFORMATION SOCIETY?

At *Think Privacy*, a public debate organized in the European Parliament on 28 January 2010, the following question was asked to the large audience: 'Who takes responsibility for his or her privacy: the government, the ICT companies or the Internet user, who distributes his personal details on social networking sites?' The question was raised after a presentation by Michel Walrave, professor at the University of Antwerp, presenting the results of research on teenagers' online self-disclosure, showing that young people are aware of privacy concerns but in practice do little to protect their privacy. [3] The public were first asked to vote on who was responsible, who then, and so on. The result of the vote is of no importance. What was striking was that the vote made an issue out of something that from a human rights perspective, allows for no such a choice (see below).[4]

The voting game, making responsibilities look like options, is often introduced by representatives of industry and business. '(Security as a consumer choice'). We tend to see this as a strategic move to avoid a proper debate about the allocation of responsibilities. The voting game is reminiscent of the resistance to attempts by the United Nations (UN) to motivate international companies to respect human rights when they operate in countries with weak legal structures.[5] International firms prefer the current status quo and to avoid certain answers to burning human rights issues.

In this contribution we will look at this UN debate, because it bears many parallels with our discussion about accountability in the information society (section 2). The *Protect, Respect and Remedy* scheme proposed by the UN Special Representative to the Secretary-General offers a solid framework for assessing the scope of duties that need to be taken care of in every human rights discussion about accountability. We then turn to European human rights law and its poignant answers regarding these responsibilities (section 3). Contrary to the international context of human rights protection, European human rights law with its insistence on positive duties to protect rights and freedoms such as privacy obliges every European state to take action whenever rights and freedoms are at stake. The state can do so by doing all the necessary work itself, or by making others take up their responsibilities (section 4-6). The concept of system responsibility is key to understanding the current accountability discussion in Europe. It is not only a moral, but also a legal concept, so do we believe, flowing from positive state duties in European human rights law (section 6). In some cases member states are mandated to implement new criminal law provisions (section 4).

The positive state duties are by no means vague (section 7-8). Judgments such as *Gaskin*, *Peck* and *I. v. Finland* are discussed with a view to understanding the concrete implications of the theory of positive human rights duties in the context of the information society (section 9-12). Through these judgments we learn a lot about the way a system of access to courts needs to be set out for victims of rights breaches in the information society. The legislator has a role in this, since he has to make access to justice possible. However, his responsibility goes much further. Applying the *Protect, Respect and Remedy* scheme we highlight the need to complement a scheme of remedies with pro-active regulation of the information society in order to avoid human rights violations. The contribution then considers how, with the EU Charter on Fundamental Rights and the series of amendments to the ePrivacy Directive, the European Union is showing the way (sections 13 and 15). These developments are elaborated with a consideration of how the debate around human rights and data protection in the face of consequential data processing technologies has developed and which problems it faces. It is demonstrated how a more nuanced understanding of responsibility allocation as well as human rights obligations also demands (and leads to) a more nuanced approach to the specificities of each technology (section 14).

2. RESPONSIBILITY FOR HUMAN RIGHTS VIOLATIONS BY MULTINATIONALS

2.1. Background[6]

The United Nations is, as a promoter of human rights in the world, committed to the issue of human rights and corporations.. In international human rights law states alone are responsible for complying with human rights legislation. Corporations are not (yet) regarded as having direct obligations. Consequently, it is the role of the nation states to oversee the conduct of corporations in their respective territories. In weaker countries, the conduct of rich and powerful multinationals, for several evident reasons, is not always easy to control.

Therefore, the United Nations aims to create an international initiative to support these weaker countries. One of the first United Nations initiatives to bring corporations in line with human rights was the UN Code of Conduct for Transnational Corporations.[7] This project, which began in the mid-seventies, sought an overall regulation of the activity of transnational corporations and included a consideration of their human rights impact. The idea behind such a code has never been formally adopted by the United Nations and the project was stopped in the early nineties. In 1998, within the UN Subcommittee for the Protection and Promotion of Human Rights, a (sub) group of experts was set up, which established the 'Norms on the Responsibilities of Transnational Corporations and Other Business Enterprises with Regard to Human Rights' (the *Norms*). This document represents a first attempt to establish legally enforceable human rights obligations for corporations and a move away from the traditional view that states have a primary responsibility for the protection and promotion of human rights. The *Norms* add to this the idea that companies have at least secondary responsibility in this regard.[8] On August 13, 2003, in Resolution 2003/16, the Subcommittee adopted the *Norms* unanimously. They were subsequently discussed in March 2004 by the UN Human Rights Commission,[9] where they were greeted rather coldly.[10] The main discussion point concerned the mandatory nature of human rights obligations for corporations created by the *Norms*.[11] Most Western states and most developing countries were, under pressure from the corporations, reluctant to impose legally enforceable human rights obligations on corporations. A solution to this deadlock was to

create yet another new initiative which consisted of appointing a Special Representative (John Ruggie, a US academic) with the task of examining the issue rights violations by transnational corporations again.[12] In 2008 Ruggie presented his report *Protect, Respect, Remedy*, containing a description of 'building blocks' to bridge the so-called governance gaps in this area.[13] Ruggie distinguishes three, different, but complementary, parts in his approach. First, the duty of the state to protect its citizens against human rights violations (Protect), second, the corporate responsibility to have respect for human rights (Respect), and third, the access to remedies when violations have occurred (Remedy).

2.2. 'State duty to protect', 'corporate responsibility to respect' and 'access to remedy'

Ruggie's first part deals with the duty of the State to protect individuals against human rights violations, including those committed by corporations. Ruggie returns to the classic idea within international human rights law making state protection the cornerstone of the legal system. The report emphasizes the importance for states to encourage and implement a corporate culture respectful of human rights. This requires a coherent government policy, greater cooperation with international bodies and initiatives, and special attention to conflict areas. It is emphasized that corporations can affect virtually all human rights.

The report then turns to the duty for corporations to respect human rights. What is needed in this discussion is to define the scope and content of the "responsibility" of corporations concerning human rights. A first obligation for companies is to operate in such a way that they comply with national laws, and generally avoid any human rights violations (do not harm). When, however a corporation operates in a country where no, or only minimal, human rights law exists, the corporation only complies with its responsibility to respect human rights if it acts with *due diligence*. This concept implies that diligent companies should ideally adopt and integrate a human rights policy, should carry out human rights impact assessments, and should subject their policies and activities to external audit and monitoring.

The third pillar of Ruggie's human rights programme deals with access to remedial measures or remedies. Although in many countries a great variety of remedies exist - legal and non-legal – the access to legal remedies is often inadequate and non-legal remedies tend to be underdeveloped. To be effective and credible, the legal remedies must conform to certain principles. Thus, these remedies need to be legitimate and accessible to all and the procedure should be predictable, equitable, transparent and consistent with internationally accepted human rights standards.

The inaccessibility of existing mechanisms can be due to the lack of knowledge about them. Victims of human rights violations are often not aware of what remedial measures exist or and where to find them. Even when they find their way, the results are far from promising due to the, often limited, powers and scope of the existing reparation mechanisms. To remedy these shortcomings, the report suggests the creation of a global ombudsman, empowered to receive and process all complaints regarding human rights and corporations centrally.

Responses to the *Protect, Respect, Remedy* report were positive. The Human Rights Council, member states, corporations and civil society, … all gave the report a warm welcome.[14] However, not all responses were equally positive. A group of NGOs requested that the Human Rights Council, in its new mandate, go beyond the Protect, Respect, Remedy framework, and also pay attention

to the liability of corporations for human rights violations. "In defining the scope of a follow-on mandate we therefore urge (…) to broaden the focus beyond the elaboration of the 'protect, respect and remedy'- framework, and to include an explicit capacity to examine situations of corporate abuse. A more in-depth analysis of specific situations and cases is needed in order to give greater visibility and voice to those whose rights are negatively affected by business activity and to deepen understanding of the drivers of corporate human rights abuses. Both elements should underpin the elaboration of the framework and proposed policy responses. For example, the modalities of corporate impunity and its impact on the enjoyment and protection of human rights need greater scrutiny as an integral part of the effort to identify solutions. A cornerstone of human rights is combating impunity. *To date the mandate has placed relatively little emphasis on the means of holding companies – including those that operate trans-nationally – to account. But for victims of human rights violations, justice and accountability can be as important as remedial measures*" (emphasis added)."[15]

2.3 SIX LESSONS FOR THE DEBATE ON THE INFORMATION SOCIETY

The above provides relevant elements for the debate about responsibility in the information society.

1. There is, as above, a tension between 'international players' and 'weak players' in the discussion about the digital world. Strong, untouchable (American) players such as Facebook, Intel, Microsoft and Google operate from Silicon Valley where data protection laws are inferior to European standards from whence they so incessantly and metronomically bombard us with ICT solutions that no defence is possible.

2. Also apparent in the debate about multinational companies and human rights is the argument about the alleged market distorting effects of government intervention. The preceding paragraphs show that resistance against mandatory norms, which are imposed on corporations, comes from both Western states and developing countries. The belief that greater protection for the citizen kills a climate of innovation seems rife amongst policy and decision makers who would prefer not to regulate or to render immune the 'vital forces of the economy.' In the context of the information society we recall that the E-Commerce Directive provides a favourable liability regime for access providers (who transmit information) and hosting providers (who also store information). This regime purposely differs from the ordinary civil and criminal liability regime. The favourable regulation was created to specifically to make sure not to overburden this type of service with too many responsibilities.[16]

3. The debate about multinational companies and human rights is not about whether corporations should commit themselves to respect human rights. We have seemingly and fortunately passed that phase. The debate is about the way in which corporations should show that commitment and, more specifically, whether there is a need for legally binding norms. Similarly, in the discussion about the Information Society, the debate no longer revolves around the question as to whether we are in need of human rights for the Internet or in need of values such as a 'safe and reliable ' Internet. The debate has moved on (in the right direction) and concerns questions such as: 'How are these values to be realised?' and 'Is there a need for "legally enforceable" rights or norms that determine who is primarily and secondarily responsible for potential problems?' The

question about liability is therefore legitimate. Without defining responsibilities, governance gaps remain.

4. Within the accountability paradigm several choices are possible. In the debate about multinational corporations and human rights, Ruggie's 'Protect, Respect, Remedy' scheme seems acceptable to most 'stakeholders.' However, some in the NGO world prefer to go one step further, especially when the responsibility of corporations is concerned. They advocate an 'upgrade' of corporate responsibility and a conversion from their respect-assignment into a protect-assignment. They advocate a shift from (mere) compliance to accountability.[17]

5. In the debate about multinational corporations and human rights, the weak (people in developing countries who 'choose' to work for multinational corporations, whatever the conditions are) are not held responsible for their choices and predicament. The existence of asymmetrical power relations allowing no freedom of choice for the weak is undisputed. Is it that different for a citizen in the Western information society? Are they capable of making the right choices when clicking and browsing? Research on the digital divide shows that each employee can be considered ICT illiterate five years after losing their job. The evolution is so fast that the loss of a lifelong learning environment is disastrous. Although it can be accepted that Internet users must have some responsibility, it seems unfair to make them the main responsible actor. Many Internet users are unaware of the small print privacy warnings and know absolutely nothing about invisible Internet protocols.

6. What the third building block of Ruggie's *Protect, Respect, Remedy* scheme brings up well is that citizens should not be approached in terms of 'personal responsibility ', but rather in terms of empowerment. If a citizen has responsibilities to bear, in a context where insecurity seems to be possible, then he or she should be given access to adequate legal and non-legal remedies ("access to justice"). In addition, the focus of awareness campaigns should not (exclusively) be on the individual's own responsibility, but rather on the existence of such remedies and remedial measures, with the level of support necessary to envisage facilitating agencies such as the Ombudsman. Meijer, a Dutch author, calls these kind of arrangements 'accountability arrangements'.[18] In the Third World in general there are very few of these arrangements. Meijers suggests a similar situation in the West regarding eGovernment: Governments are indeed setting up front offices, serving the citizen using multiple back offices, but when things go wrong these front offices are more than often legally untouchable as accountability structures still focus on back offices.[19] Hence, our duty is to focus the debate in the information society on clear accountability arrangements rather than proclaiming the death of privacy.

3. THE EUROPEAN HUMAN RIGHTS PERSPECTIVE ON RESPONSIBILITY IN THE INFORMATION SOCIETY

The European perspective on the liability and responsibility question is largely governed by the European Convention for the Protection of Human Rights (ECHR) (1950) interpreted and adapted to modern contexts by the European Court of Human Rights, sitting in Strasbourg and (to a lesser extent) by community law and the EU Charter for Fundamental Rights (2001) interpreted by the Court of Justice in Luxembourg. We note in passing other human rights texts such as the 1990 Convention on the Rights of the Child and the Additional Protocol to that convention,

which includes one specifically relevant provision stating that children have a right to privacy. However, in this contribution we will confine ourselves to Europe and especially to the progressive and encouraging work done by the European Court of Human Rights (ECtHR).[20]

Formally speaking, the European human rights text is as traditional as other international texts in the sense that the text is directed at member states and does not impose directly binding obligations to corporations or individuals.[21] However, the European Court has caused a breakthrough with the development of the doctrine of positive obligations.[22] This doctrine, - also recognised in comparable supra-national systems, but absent in others, e.g. U.S. constitutional law, was developed by the European Court with a view to evaluating government behaviour in complex cases.[23] Take for instance the case where the rights of an individual are not threatened by a specific concrete action on the part of a government official, but by the non-movement or inaction of the government. The doctrine allows the potential condemnation of the state for the failure to have taken appropriate action in line with their obligations to ensure the enjoyment of the right.

The doctrine has so far been applied in relation to many rights enshrined in the Convention (e.g. the right to life protected by Article 2, but its main applications so far concern the rights protected by Article 8 of the ECHR, .Article 8 ECHR recognizes the rights of the protection of privacy, family, communication and home. On the basis of the doctrine, this provision not only prohibits the state from interfering in the rights of citizens, but it also includes an obligation for state parties to adopt measures to ensure the effective enjoyment of the privacy right or any other right under Article 8 ECHR and to introduce specific provisions to prevent or punish the acts of individuals who would ignore or violate these rights.[24] Although this 'positive' duty is not expressed as such in the treaty, it has been inferred from it by the Court.[25]

The first Article 8 ECHR application of the doctrine was in the *Marckx* case (1979) and the *Airey* case (1979) on the right to family life and also the judgments *Rees* (1986) and *Gaskin* (1989) concerning the right to private life.[26] More recently, the doctrine of positive obligations was applied in the *Stjerna* case (the right to alter names)[27], the *Guillot* case (naming)28, the *Willsher* case (access rights)[29], the *López Ostra* and *Guerra* (environment) cases[30] and in the *Botta* case(disabled facilities).[31] We will come back to some of these cases *below*.[32]

In the *Botta* judgment, the Court clarified that it is up to the Court to decide if there is (or if there is not) such thing as a positive human rights duty and it will only acknowledge the existence of such a duty "when it considers that the measures requested by the person are directly and immediately linked with the private and family life of the person concerned."[33] In last instance it is therefore the Court's decision to determine whether a positive obligation exists or not.[34] It is therefore not possible to establish a precise index of positive duties, nor is it possible to determine in advance which initiatives a state needs to take to effectively respect private and family life.[35]

Decisive in developing this revolutionary doctrine was the 1979 *Marckx* ruling. In the Court's view, the right to respect of family life does not only result in a duty for the government (continued) to refrain from interfering in family life, but it also results in a positive duty. Because of the right to protection of family life, states should especially take those measures that are necessary to make this right possible. As such the existence of positive obligations in relation to family life implies that when states develop family law rules, these should not impede on the normal devel-

opment of family relationships, but, on the contrary, should provide the context to make their enjoyment possible.

In 1979 the Court ruled on the impossibility for Mrs. Airey to be able, on the basis of Irish law, to file for divorce. For the claimant this legislation constituted a breach of several fundamental rights. One was the fundamental right to the protection of privacy and family life. The Court saw no negative duty breach (the negative duty not to infringe), but discussed the case in terms of positive duties. Mrs. Airey's core complaint was not that Ireland had performed an act, but rather that it failed to act.[36] In the rest of the judgment, the Court then turned to the analysis of this positive duty. Should Ireland have altered its divorce laws to make them more flexible in light of contemporary human rights standards?

In identical terms and with reference to the *Airey* principles, the Court ruled in the *Gaskin* case (1989) that the refusal of UK authorities to give Gaskin access to a file on his childhood years is not to be understood as a violation of a negative duty. The British government officials did not really do anything detrimental with Gaskin's data, but simply refused him access. This cannot be considered as a violation of a negative duty. However, it can be possible to look at the facts as demonstrating non-compliance with a positive duty on the part of the British government to meet Gaskin's request.[37]

4. POSITIVE HUMAN RIGHTS DUTIES AND PROTECTIVE CRIMINAL LAW PROVISIONS

The standards set out by the European Court are high. States can even have a positive human rights duty to single out certain acts as crimes and the Court has accordingly extended the doctrine of positive state obligations to criminal law. Sometimes this doctrine implies that additional criminal legislation is necessary in a member state. Distinctive is *X and Y v. Netherlands* (1985),[38] concerning the application of the doctrine of positive obligations to the problem of protecting the public from sex crimes.[39] In this case the Court condemned the Netherlands, because its legislation did not allow the prosecution of someone who was sexually violent towards a mentally handicapped girl who had just turned sixteen.[40]

Marckx and *X and Y v. Netherlands* teach us that there are at least two kinds of positive obligations in European human rights law.[41] States need to take measures that make the exercise of fundamental rights possible,[42] *and* need to introduce specific provisions for the prevention and/or punishment of acts of individuals who ignore or violate basic rights or obligations.[43] This broad set of duties plays a role in *MC v. Bulgaria* (2003).[44] The Court found a violation of the treaty because M.C. – a victim of rape - was not legally protected in Bulgaria in a satisfactory way.[45] Not prosecuting in a case of rape is a violation of the positive obligation of a contracting state to protect its citizens against violations of their fundamental freedoms and rights through an effective legal system and to investigate complaints thoroughly.[46] From *M.C. v. Bulgaria* one can also infer a duty to reasonable and adequate criminal law making. [47]

To these duties (to enable enjoyment, to investigate certain complaints and to protect through criminal law), one must add the duty to ensure an effective remedy for human rights abuses as laid out in Article 13 ECHR. This right is considered a necessary complement to the other treaty rights. Citizens not only 'have' the regular rights (the right to privacy, to life, to freedom of expression etc.), but they also have the right to an effective remedy when these rights are violated.

5. RESPONSIBILITY AND ITS DISTRIBUTION AMONGST STAKEHOLDERS

This brief discussion of the Strasbourg machinery and the European doctrine of positive state duties to realize effective enjoyment of rights gives a new meaning to the old rule that the ultimate responsibility for human rights violations lies with the state. In a certain way the old rule applies more strictly than ever before: human rights violations by non-state actors can trigger state responsibility when certain positive duties have not been adequately met.[48] States have final responsibility for human rights violations within their jurisdiction. This responsibility is a source of specific duties. These duties relate to the three building blocks identified by Ruggie: Protect, Respect and Remedy. By creating a protective environment by making non-state actors directly accountable to human rights standards and by installing effective remedies for redress, states can defer this responsibility. Putting pressure on companies through administrative law or human rights law ('sharpening accountability, or increasing 'enforcement' on 'compliance'), creates liability immunity in Strasbourg. A legal system cannot guarantee that no human rights violations occur, but efforts need to be taken to prevent them and when they occur the system needs to be responsive.

A translation of these human rights duties to the information society context is not difficult. Of course not all the judgements discussed *above* relate to the information society, but at least in our view, enough guidance is given for states to take up their duties with regard to the Internet and other modern media.[49]

It is not only about non-interference, but about the full package: to protect, create respect and to remedy. More specifically, governments must protect their citizens against human rights abuses by companies and against abuses by other users on the Internet (first building block); ensure that companies respect their human rights obligations (second building block); and provide easily accessible remedies or remedial action (third building block).

Concerning the second building block, the government may choose (consciously or by not acting), to be lenient towards ICT companies and service providers, but this may amount to a neglect of the duty to protect and the government will then be held responsible in Strasbourg for possible human rights violations committed by third parties.[50] Alternatively a government may choose to distribute responsibilities by tying ICT companies and service providers to certain satisfactory standards. In the case of possible violations, the Strasbourg test would be less painful. Making private actors more accountable helps governments to respect contemporary human rights standards.

6. SYSTEM RESPONSIBILITY AS A LEGALLY BINDING ACCOUNTABILITY SCHEME

Calls for accountability fit well in a postmodern digital age where traditional power structures, such as oversight by parliament, are losing their importance and where complex and rapidly evolving global and technological processes often preclude solid and effective anticipatory regulation via legislation and government policy.[51] Meijers, who distinguishes between *liability* (limited, only relevant in disputes) and *responsibility* (all encompassing), correctly identifies a double accountability scheme for governments in the digital era. Next to the responsibility for their own services and actions, states now have broader *system* responsibility that extends to all use of ICT, regardless of by whom in any given society.

As regards the responsibility of use by the government for its own applications, accountability has a rather natural place - which does not mean that it is always provided. Through accountability arrangements, the inevitable uncertainties associated with the introduction of new systems can be dealt with, to a certain extent, by anticipating on an institutional level, that there will be problems and disputes. System responsibility (for technological developments outside its own organization), on the contrary, triggers a different kind of accountability. Now, the government is, as it were, on the side of the individual citizen in demanding the accountability of service providers in the ICT market. This is, seen from the government's perspective, a more difficult role than setting up accountability in their own processes.[52] This broadened role is ambitious and complex. It forces governments, amongst others, to take action in order to protect citizens against identity theft, to organise appropriate forums for conflict resolution and to introduce protective conditions for the freedom of expression in the light of the existence of actors on the Internet that have excessive social power.[53]

A human rights law analysis, like the one proposed in this paper, adds more body and colour to the important idea of system responsibility.[54] System responsibility is neither an ideal nor a virtue nor a voluntary option for the wise policy maker, but legally imposed starting point for regulation.[55] Part of the system responsibility consists of making actors such as internet companies comply with human rights standards. Governments simply *must* support citizens in demanding accountability. Governments are not directly responsible for every human rights violation in their jurisdiction, but they are obliged to ensure that through the efficient distribution of responsibility, responsibilities are covered.

7. POSTMODERN VAGUENESS AND LACK OF CLEAR ACCOUNTABILITY SCHEMES?

Meijer quotes many 'governance' authors announcing the end of traditional Westphalian state sovereignty and pointing out the failures of the traditional idea of 'government'. Developments in technology and globalisation undermine the essential traditional pillars (territoriality and the absence of a role for external agents) of Westphalian state sovereignty. The collapse of the nation state makes traditional law mechanisms obsolete. The question then arises as to whether law can still play a meaningful role in this context?

Most lawyers have never been able to fully understand that question. For them, law is an activity or a procedure, rather than a norm setting system, a process more than an institution or structure. Law in this view is to be compared with a signalisation system that attributes facts and events to persons or legal actors. By speaking the law and operating legal principles of attribution judges do no more than apply, construct and maintain a system of responsibilities.[56] All kinds of legal systems coexist within and outside of the state. Sometimes people have a choice and they can do legal forum shopping. Do we take this damage to a criminal court or to a civil court? Do we go to the Court of Justice in Luxemburg or do we stick to a national court. Law reinvents itself constantly. Leaving behind traditional and strict liability mechanisms from private law and tort law, Strasbourg seemingly develops a liability system that is modern in more than one way: If there is a complaint about a human rights violation in a certain state, then that specific state is accountable. Governments of European states will be held responsible in Strasbourg when their own actions amount to human rights violations, when inaccuracies or errors are found in their accountability arrangements or when there is no, or a careless, distribution of responsibility.

We contend that this human rights accountability system is a significant (but of course not sufficient) response to the alleged deficiencies of the classical Westphalian legal system.[57] Meijers discusses the fact that most Internet users do not understand the invisible protocols of the Internet[58], and that through the use of information technology the anatomy of decisions is obscured with the result that certain governmental acts are less open to contention.[59] Strasbourg simply shrugs its shoulders and turns to the one stakeholder that is always identifiable: 'the' government of a member state. It will be this government that will be held accountable for violations of privacy and other rights when scrutiny reveals that no satisfactory legislative or regulatory initiatives have been taken to protect these rights of the citizen or when insufficient accountability arrangements have been created in the light of the right to an effective remedy. How so postmodern vagueness and lack of clear accountability schemes?[60]

8. CONCRETE CONSEQUENCES OF SYSTEM RESPONSIBILITY

The story of globalisation and complex technological developments brought to us by serious scientists is one that politicians often play out strategically to shift away their system responsibility ('*Things are not in our hands, and the Americans do not listen!*'). Our human rights analysis gives a much more pressing account. The recognition of system responsibility in Strasbourg explains why there is, in Europe at least, no accountability without the sanction of liability.

The challenge is to understand how far these positive obligations to system responsibility stretch. In general the answer is *not too far*. The broader, state accountability, scheme is only triggered when positive duties are recognized, and European courts are prudent when recognizing extensive state duties. Too prudent, if we are to believe many authors that single out the limited extra value of the positive duty doctrine for citizens and vulnerable groups in particular. In an article from 2005, Olivier De Schutter highlighted the missed opportunities in the case law of the European Human Rights Court to provide for real protection and identified certain structural and institutional limitations to court procedures to further develop human rights law.[61] Too often judges prefer to work with open concepts and avoid more general statements that make duties concrete. The outcome of their cases is too closely linked to the immediate context of the claimant. More fundamental is De Schutter's observation that the 'binary' character (all or nothing) of the judicial function often leads judges to a hands-off approach.[62] Clearly we cannot entrust the difficult task to identify positive human rights duties to the judges alone.

The concrete shape of a privacy policy that a corporation is obliged to develop in the name of human rights will have to be determined using other sources, in particular by law. It is probably not fair to demand a high level of detail from Strasbourg. Understanding the full implications of our commitment to human rights is not the sole responsibility of the European Court. Human rights are primarily the responsibility of member states that recognise them.[63] It is the responsibility of our governments to think through the idea of negative and positive obligations in the context of the information society.[64] The European Court will only reluctantly position itself thusly, preferring to avoid substituting itself for elected authorities mandated to make certain choices depending on factors such as budgetary constraints. The Court will however look at the outcome of these deliberations to safeguard treaty rights that need to remain practical and effective.[65] The European Court is becoming more active and clear in recent judgments on the issue of positive state duties in the context of the information society. In the following, we will discuss

some of these important judgments. They will aid understanding as to the extent of the system responsibility that authorities should shoulder.

9. SYSTEM RESPONSIBILITY CONCERNING ACCESS AND PUBLIC PRIVACY: GASKIN AND PECK

Already in 1989, with the *Gaskin* case (which was discussed *above*), the Court had made perfectly clear that the theory of positive obligations was of a significant enough nature to alter our understanding of privacy obligations. The Court ruled that the act of not allowing access to a person's data violates the Convention. To have access to one's data is an aspect of the right to privacy that entails a duty to others to allow this access. In the name of privacy, access should be given, even when national law contains no explicit provision in this regard.

Does the foregoing mean that no national legal basis for the right to access rights needs to be created? Does recognition by Strasbourg of a (human) right to access make national legislation creating such an access superfluous? On the contrary, national governments should make policy in advance. The Strasbourg system is not meant to be a permanent backup system (see the principle of subsidiarity, *above*). The Court merely helps the member states to understand the scope of the rights agreed upon and to regulate accordingly.

It is useful to add to this the observation that the European Court is not to be compared with a regular constitutional court that is mandated to check the validity of legislation. A case can only be taken to Strasbourg when there is a concrete violation of rights and an individual claims status as a victim. A claim that there is a problem solely based on the observation that, for instance, national law does not regulate CCTV, would not be admissible in Strasbourg,[66] hence the obligation to wait for a real camera problem before going to Strasbourg.

Interestingly, for our understanding of the information society, this did not happen until late in the history of CCTV.[67] In the *Peck* case, CCTV-images were made of a suicide attempt in a public place. The images from these CCTV cameras were made available to journalists and shown on British television. The Court condemned this practice: Publication, through media outlets, of sensitive data is in this case a breach of Article 8 ECHR; the fact that the claimant was clearly recognisable on television and the publication of his picture in the press constitutes a violation of his right to privacy. The right was violated as the data subject did not give his approval, nor was he made unrecognisable.[68]

Peck is important because it removed the last doubts for certain stakeholders, who up until 2002 had been ignoring the human rights dimensions of CCTV. The judgment illustrates the broad meaning given by the European Court to the right to privacy. The view that everything we do in public is automatically unprotected is simply incorrect in Europe. The Court recognises the applicability of the right to privacy for acts outside the 'strict private sphere' and involves in its analysis, inter alia, the criterion of reasonable privacy expectations. Translated into the context of social networks, this means that our right to privacy is not lost forever because we share information with others, especially not if we have the expectation that the person(s) responsible for the social networking site handles our data responsibly.

10. SYSTEM RESPONSIBILITY CONCERNING SECURITY: *I. V. FINLAND*

In 2008, twenty years after *Gaskin*, a new dimension was added to the doctrine of positive obligations in the context of the use of personal data in *I v. Finland*.[69] The Court ruled that the security measures taken by a Finnish hospital - measures that when implemented properly could have guaranteed the right to respect for the private life of an HIV patient who worked at the same hospital - were inappropriate and found a violation of Article 8 of the ECHR.[70]

In its approach to the case, the European Court identifies some general principles relating to personal data. Medical information falls within the scope of Article 8 ECHR: "The protection of personal data, and specific medical information, are fundamental to the right of a person to respect for his / her private and family life." The Court also recognises that the most important - negative - object of Article 8 protection consists of "protecting individuals against arbitrary interference by public authorities", but at the same time emphasizes that there are positive obligations that may derive from the right to respect for one's private life. These obligations include the adoption of measures, which can ensure the right to respect for private life, even when these rules apply to relationships between individuals.[71] The Court observes that the protection of personal data, especially that of health data, is fundamental for the right to protection of privacy and family life on the part of the patient.[72] Such protection is not only crucial to respect the feelings and expectations of patient privacy ("the sense of privacy of a patient"), but also for patient confidence in the medical professions and health services in general.[73] Positive obligations concerning care for personal data do not merely serve individual interest. There is a general interest in protecting confidentiality. This duty may also be required from private persons.

After listing these general principles, the Court turns to the relevant Finnish law. Article 26 of the Finnish Data Protection Act ('the Personal Files Act 1987') requires the processor of personal data to take security measures and to ensure that only treatment personnel have access to files. Strict application of this provision would have been an effective protection under Article 8 ECHR and would have allowed the hospital to control the access ("to police strictly access to a disclosure of health records").[74]

In the Court's view there was no adequate security in place, which amounted to a breach of the Finnish Act *and* consequently to a violation of the ECHR. The taking of security measures by companies and institutions such as established in data protection legislation, does not constitute merely a moral or a simply legal obligation, but must be seen as a positive human rights obligation. Failure to comply with that requirement is therefore equated with a violation of the Convention. Further to the above violation: it was also found that there was neglect of the human rights duty to investigate.

In sum, what is needed, according to the Court, is practical and effective protection to prevent any possibility of unauthorized access. This protection was not given here.[75]

Dealing with personal data by individuals and institutions requires adequate security measures, with the purpose of guaranteeing the right to respect for private life. More generally, it can be said that by complying with existing legislation on data protection in the member states, the positive obligations which derive from the ECHR, are met. Returning to the

discussion about vagueness surrounding the theory of positive human rights duties (*above*), we note that the section in the judgment containing 'general principles' proves to us that the judgment is relevant for more than just this individual (very sad) case. This is not the only European judgment with a section devoted to general principles. In more and more judgments the Court opens with an analysis of the applicable general principles, which are then taken as guidelines.[76] This methodological rupture with traditional casuistic approaches of administering justice, aims to make possible further guidance to member states with a view to allowing them to adapt to the standards of the Convention as developed by the Court. In addition, we see in *I v. Finland* how the Court relies on data protection law and its extensive set of specific rights and duties. These are identified as positive human rights obligations. Data protection legislation is not mere legislation. It is warranted by our human rights! Data protection laws after *I v. Finland* can be considered as checklists for positive human rights obligations.

11. REMEDY AND FINANCIAL COMPENSATION CANNOT BE THE ONLY BUILDING BLOCK

In *I. v. Finland* one can discern additional guidelines related to positive state duties, this time with regard to the 'Remedy' building block. Not every legal redress system is good enough for a law abiding information society. Finland got a serious reprimand for its system. The claimant complained about the way in which compensation was handled in Finnish law.[77] She lost her data protection case because she failed to demonstrate a causal link between the deficiencies in access rules and the improper dissemination of information on her medical condition.

Lawyers recognise this situation. Damage is not enough in continental civil claims. Next to showing injury a person pretending to be a victim has to establish a causal link between the harm and actions or non-actions of third parties. The European Court is obviously not charmed by the stringency of Finnish civil law requirements. Placing such a burden on the shoulders of the claimant is unfair - the Court found: "To place such a burden of proof on the applicant is to overlook the acknowledged deficiencies in the hospital's record keeping at the material time."[78] If the hospital had carried out greater control of access to health information, for instance, by only giving access to those directly involved in the treatment, or by keeping a log book of all persons who had access to the data, then the claimant would have been in a less unfavourable position before the national courts.

In the information society where all processing of data leaves trails that can be checked on by the processor, it is unfair and contrary to the Convention to expect significant proof from the data subject, who does not control the computer but is simply being registered in it.

A feel for the practical obstacles faced by privacy victims is equally present in the Court's position with regard to the question of how compensation for the claimant should be calculated. In practice, this is a thorny issue for regulators. What is the harm if one is careless with how personal data is handled? Privacy victims seldom die. In the present case, a person lost her job and reputation, but very often the damage is less evident. What is the damage when Sony loses billions of *Play Station* users data (including credit card data) as happened in early 2011? Does it make sense to go to court immediately or does one need to wait until further damage (monetary loss by misuse of credit card data) occurs? Having sloppy security measures is clearly a data protection error, but is it enough to warrant claims for compensation?

We would argue yes, but the Courts are seemingly not ready to go along with this to any significant extent. *I v. Finland* does not answer all questions, but the Court does underline that the applicant is also eligible for reimbursement for non-pecuniary damage. The claimant had suffered non-pecuniary damage and therefore qualified for financial compensation. "Failure to comply with a security requirement is not compensated by simply adjusting their security measures, but requires financial compensation."[79]

The importance of *I. v. Finland* for the discussion about the establishment of the information society is still raised too little. Its paragraphs are rich and complete. The ideas and guidelines about compensation that we discussed *above* are followed by complementary statements about the limits of compensation possible from a human rights perspective. Indeed, after having recognized compensation for pecuniary and non-pecuniary damage, the Court continues its reasoning by declaring that the mere fact that national legislation allows for compensation after privacy suffered damage is insufficient. The government should ensure a practical and effective protection of this right. Providing a system of compensation (Ruggie's third building block) is therefore not enough. A society must do more work to achieve human rights standards. There should not just be legal settlement afterwards (when problems occur), but there should also be a clear set of guidelines in legislation and proper enforcement of these guidelines (to avoid problems). This does not mean that Ruggie's third building block is unimportant. A system of compensation for damages must exist and must be based on fair and accessible procedures. No unreasonable burden of proof should be placed on the shoulders of the claimant and monetary compensation should be provided.

12. IF COMPENSATION IS AWARDED THEN IT MUST BE BOTH REASONABLE AND SUBSTANTIAL

Let us dwell a little longer on the issue of compensation. Some on the business side or on the governmental side will object to the foregoing: Where is it heading if, for violations of rules on use of personal data, we also have to compensate for non-pecuniary damage suffered? What are the limits of such an obligation? For the European Court, such compensation needs to be reasonable or proportional. The requirement that the compensation for abuse and accidents with personal data has to be reasonable is developed in *Armonas v. Lithuania* (2008).[80] The facts of the case and the position of the Court are of such a nature that they give the daily reports in our newspapers about "accidents" with personal data (lost, press leaks, etc.) a special dimension. Armonas was married to L.A. who died on April 15, 2002. On January 31, 2001 Lithuania's largest newspaper reported about a so-called *Aids*-threat which was prevalent in the region. The front-page article mentioned L.A. by name and surname and identified him as an *AIDS* patient. The article also reported that he had two illegitimate children with a woman, G.B., also an aids patient. L.A. starts proceedings against the newspaper and is awarded a small compensation for violation of his privacy.[81] Lithuanian law places upper limits on compensation granted. Due to these restrictions in law the compensation could not legally exceed LTL 10,000 (about € 2,896) and L.A. (who died) received only very little compensation.

L.A.'s wife turned to the European Court with the complaint that her right to privacy had been violated because of the ridiculously low compensation that was granted to her husband, despite the recognition by the Lithuanian court that a violation of privacy had occurred. Such low compensation would not satisfy the requirements under Article 8 and 13 ECHR to provide an effective remedy.

Technically-speaking it was not certain that her case would stand up to scrutiny but the European Court declared the complaint admissible[82]. This is usually a sign of the willingness of the Court to take the case seriously. Again, the starting point for the Court is the idea that negative and positive obligations are incumbent on States. The latter may include obligations for the government to take steps to protect the privacy in relationships between individuals.[83] Proportionality is a central concept in assessing the scope of these obligations and in this case a fair balance had to be found between press freedom and the right to private life.[84, 85]

The publication of information on the health status of Armonas' husband did not contribute to the public debate and only served to fulfil the curiosity of particular readers. The balance in this case therefore weighs in favour of the individual right to privacy. The government has an obligation to ensure that this right can be enforced against the press. The Court attaches particular gravity to the assertion in the article that the staff of the local AIDS centre had confirmed the information on L.A.'s health status to journalists. This, according to the Court, could be discouraging for others to take a voluntary *AIDS* test. The protection of personal data in this sensitive context is of particular importance.

In theory such a protection exists through Lithuanian data protection law. Also, compensation was awarded to L.A. The question, however, is whether the amount of compensation was proportionate to the injury and to what extent the legal provisions restricting the compensation to a fixed (low) amount were in line with Article 8 ECHR. It is not for the European Court to require that member states impose heavy sanctions. The Court leaves certain discretion in hands of the state concerning the regulation of financial compensation. They can take the socio-economic situation of a country into account and have to prevent overly heavy restrictions on the press from resulting in the right itself being eroded. Imposing overly heavy sanctions on the press can have a chilling effect on press freedom.[86] However, in case of a manifest abuse of that freedom, as in the present case, the Court considered that the heavy legal restrictions on the compensation of victims and the subsequent low compensation amounts were not in line with the expectations people have in that area in accordance with Article 8 ECHR. Therefore, there was a violation of Article 8 ECHR and Lithuania was held accountable.[87]

The ruling *Armonas v. Lithuania* from 2008 indicates that not everything may be written in a newspaper. The lessons can be extended to other media such as the Internet. The distinction between the actual distribution of information as part of public debate on the one hand, and distasteful allegations concerning the private life of a person on the other is equally applicable. The government should protect its citizens against distasteful unwarranted allegations and citizens, bloggers or newspapers should refrain from publishing such information.[88] *Armonas* also contains a fine illustration of the positive state duty to protect human rights (such as the right to data protection) in an alert and appropriate way, if necessary through the imposition of sufficiently high compensations in case of infringements by publishers, advertisers and media companies.[89] Furthermore, this compensation needs to be proportionate to the suffered harm, and cannot be too low. States should set up their compensation system in such a way that restitution for harm is possible without an excessive burden of proof and there is no sham justice in the form of derisory compensation. An effective remedy as warranted by Article 13 of the Convention should be available, even when confined to cases with only mere moral harm resulting from a lack of respect for an individual's right to self-determination.[90]

In what follows, I will discuss the tasks of the legislator in the information society. It is clear from the above that our society not only needs to work on access to justice, but should also design and implement a system of legal protection and supervision in advance.

13. THE EU CHARTER: A CORNER STONE FOR SYSTEM RESPONSIBILITY

The EU Charter of Fundamental Rights, which was proclaimed on 7 December, 2000[91] and 14 December, 2007,[92] was made legally binding for member states via the Treaty of Lisbon.[93] This new human rights text not only repeats the contents of the ECHR, but also codifies new developments in human rights. Article 7 of the Charter provides us with the right to privacy, whilst Article 8 of the Charter goes a step further than the ECHR and recognises a separate right to the protection of personal data. The provision says that personal data should not only be protected but also that personal data must be processed fairly, that data must be processed for specified purposes (purpose binding), that personal data must be processed with the consent of the person or that personal data must be processed based on some other legitimate basis laid down by law. Article 8 of the Charter then goes on to grant each person access to data collected about them, a right to have this data corrected if needed and the right to be assisted by an independent controlling data protection authority (DPA) to oversee the compliance with the law.

Article 8 of the Charter can be understood as a corner stone for the regulation to be set up in Europe. It leaves no doubt about the need to protect *all* personal data and usefully recalls the existence of several important principles that govern all processing of personal data. In particular, the inclusion of the purpose limitation principle deserves credit. Its enforcement has very serious and widespread implications, for instance, for the work of the justice system and the police, for the actions of controlling employers and for social network providers that like to use their users' data for new purposes other than those for which the data were originally collected, preferably without any transparency or consent. This principle is poorly anchored in Asian and U.S. law, which creates a lot of confusion with regard to transnational transfers of data and shared security initiatives such as PNR and Swift. From a European perspective, there is thus little harm in emphasizing its importance in a high visibility text.[94] The same applies to another sore point in transatlantic relations, the question as to whether an independent supervisor, which would sanction and control the use of personal data, must be instated in a legal system.

The inclusion of these data protection rights and principles in the highest fundamental rights is not without significance, as the U.S. experienced recently when the European Parliament opposed access to SWIFT banking data due to lack of accompanying guarantees.[95]

14. WHY SPECIFIC LEGISLATION FOR BIOMETRICS IF WE HAVE DATA PROTECTION PRINCIPLES?

The necessity of regulating technologies to avoid human rights issues has always been disputed and indeed for a number of reasons. Today this position is losing momentum, but there remain voices opposed to the detailed regulation of specific technologies. One opinion is that there is already enough regulation. The argumentation is that the protection of personal data has the best chance of success on the basis of existing general data protection principles that apply to *any* technology that processes personal data. These principles - the right of access, rectification and erasure, the purpose limitation principle, etc. - are contained in a set of well know international and European documents and legal instruments: the OECD Guidelines[96], the Council of Europe's Data Protection Convention 108[97], the European Directive 95/46/EC[98] and Framework decision 2008/977/JHA.[99] The argument is then that we need no more. The general recognition that the already existing data protection principles apply to a new technology will do.

Surprisingly many advocate this view within and outside the EU. Within the EU this explains why no specific regulation has been elaborated concerning CCTV, although many citizens would agree with the view that this is consequential technology requiring more detailed regulation. Some seem to fear to be curtailed when more is done than just recognizing the applicability of very general principles to a specific technology such as CCTV.[100] Others from within the data protection community fear that new regulations will be accompanied by serious limitations to the general principles. More regulation would then mean less protection.[101]

Within both views the existence of general data protection laws is used to oppose data protection initiatives. The argument 'we do not need regulation' is traded in for the better sounding argument; 'we do not need extra and more detailed regulation'.

Sticking to the general principles when confronting new technologies disregards the particularities (in terms of human rights consequences) of each specific technology. An image, for instance, is different from a written document on a person and a fingerprint is different again. It is, moreover, contradicting the pivotal Article 5 of Directive 95/46/EC which contains the rule that member states should actually indicate, with precision, the conditions under which the processing of personal data is lawful. In the absence of specific legislation on new technological developments, with clear conditions and limitations, the fundamental principle of fair and lawful processing remains vague and difficult to enforce. One must only think of the wide variety of biometric applications that exist and how their application varies across different actors (from swimming pools to border checks). In this light, how do you materialize these general principles of data protection?[102] European data protection law has therefore a duty to itself to actively protect European human rights. To proclaim that the Internet is unsafe and that surfing on it is at your own risk is not an option. The biometrics case and the somewhat older CCTV case are examples of technological developments past their initiation phase where almost all countries as well as the EU have missed a beat by not taking up their human rights duty to regulate. None of the three building blocks are there.

In many of its legal instruments there is some attention given to the three building blocks. The EU legal instruments on new technologies such as the proposed regulation for a European processing of passenger data include the 'usual data protection rights' such as the right of access, rectification, and erasure. However they seldom include strict deadlines within which these requests must be met or fulfilled. Equally, these regulations mention, as a rule, a right to compensation and a right to judicial remedies for any breaches, yet the scope of these rights is left to the scrutiny of the national legislators. In practice the added value is very limited, since the absence of strict rules on the liability of the different authorities involved does not allow the competent judicial or administrative authorities to impose sanctions when necessary.[103]

The EU is, however, getting better at the regulation of other types of technologies and is increasingly living up to human rights expectations.[104] Governments actively regulate many aspects of these new technologies. In fact the model of regulation is increasingly becoming the model of regulation our society developed for traffic regulation. No detail is ignored and there are rules for cars, drivers, signs and rules, the pavement and lighting. The ultimate aspiration of traffic regulation is to have safe traffic. Courts will use civil law provisions to address governments when it appears that, for example, traffic signs are insufficient or accidents are happening as a result of inadequate road surfaces.

Comparing cyberspace with traffic is an elegant way to signpost the direction we must head: A safe and reliable, human rights-friendly information society with a government that has final responsibility and regulates and actively delegates responsibility. A good example is the data protection policy, which the EU pursues in the telecommunications sector. The example that will be discussed in the next section illustrates that Europe has never hesitated to materialise the "sacred principles of data protection," and to call risks and solutions by their true names. It is deplorable however, that the exercise has not been sustained across all technologies that have been launched in recent years.

15. AN ACTIVE APPROACH TO TECHNOLOGY: THE EXAMPLE OF THE EPRIVACY DIRECTIVE

Less than two years after the general Directive on the protection of personal data, the European Directive of 15 December 1997 concerning the processing of personal data and protection of privacy in the telecommunication sector was enacted with a view to complementing the general framework of 1995.[105] This specific regulation ensured the protection and confidentiality of personal data processed by telecom services and networks. The directive focused heavily on ISDN technology. The lack of harmonization in this field would have disturbed the creation of a single market in the field of telecommunications.[106] ISDN was therefore seen as an important prerequisite for the further development of the internal market. The directive gave citizens important safeguards (in the form of new explicit subjective rights), including the creation of member directories and the installation of detailed bill and call forwarding. The directive also included numerous other new telecommunications safeguards. Member states are required by the directive to ensure that the confidentiality of communications via the public telecommunications network and publicly available telecommunications is guaranteed.[107] New rights were created with regard to number identification and rules were incorporated with regard to sexual and other malicious 'breathing calls'.[108] A first ban was introduced for providers on telecommunications services preventing the sharing of subscriber data,[109] and a second ban concerned unsolicited spam. Automated calling systems for direct marketing were only allowed if subscribers gave prior consent.

The first ePrivacy Directive focused on public telecommunications networks (ISDN supported) and public digital mobile networks.[110] The Internet was neither named in the text of the directive, nor in the preamble. To address the challenges posed by the Internet, the European legislator replaced the 1997 regulation by an updated version in 2002.[111] This time the Internet and its challenges (cookies, spyware, malware and viruses) are clearly addressed to the benefit of the Internet user.

The story does not stop here. The 2002 ePrivacy Directive was again updated in 2009 to address further new developments.[112] The object of the update illustrates an attempt by the legislator to distribute responsibilities to certain stakeholders in the telecommunications industry and to make them shift from compliance to accountability.[113]

Firstly, the 2009 ePrivacy Directive obliges telecom companies to report security breaches of personal data (Data Security Breach Notification).[114] It is in fact a double obligation. There is the obligation to notify the competent authority of every security breach, regardless of whether there is a risk to individual users. The notification must contain a description of the consequences of the violation and of any measures taken or proposed to address the violation. There is also an obligation to report to the individual users and to inform them of "likely adverse effects" on their

personal data and privacy. Consideration could given to identity theft or fraud, physical harm, significant humiliation and loss of reputation.[115] Telecommunications companies are required to keep an inventory of breaches, in which facts, consequences and remedial measures are recorded.

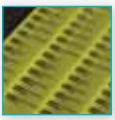
Secondly, there are new refinements in the rules about cookies, spyware, malware and viruses.[116]

A *third* measure concerns the ban on spam, which goes back to the first version of the 1997 Directive. Since many individuals do not normally take action against spammers (either because they cannot afford to file a lawsuit, or because the damage they suffer is too small to start a procedure), a collective instrument has been created: From now on it is possible for natural and legal persons who have a legitimate interest in fighting spam to take legal action against spammers. Providers of electronic communications who want to protect their legitimate business interests or the interests of their clients and consumer associations and trade unions, who represent the interests of people who have suffered spamming, can now contribute to a safer Internet! In addition, the new directive also allows Member States to issue specific sanctions targeted at providers of electronic communications who contribute to spamming through negligence.

Finally (and *fourthly*), the 2009 Directive focuses on strengthening certain enforcement mechanisms. National data protection authorities should be empowered to prohibit further actions by persons or firms breaching the provisions of the Directive (prohibition order).

All three building blocks, identified by the UN Rapporteur, come beautifully together in this reform package. The road to justice is facilitated by better notification of security breaches, by enabling public interest groups to initiate legal actions and by making prohibition orders possible. Towards ICT companies and other relevant stakeholders, one can observe a change in approach. Mere compliance is refined and translated into real accountability: There must be an active policy towards the government and citizens (notifications), a safe final product (free from cookies, spyware, malware, viruses and spam) and sanctions are possible against the negligent offering of internet services.

The above illustrates the way forward. Responsible legislatures should set up a system that prevents human rights violations. They can do this by distributing certain responsibilities to stakeholders in the field. Their performance needs to be closely monitored by governmental authorities and access to justice needs to be made possible by a range of practical steps of which we have given numerous examples in this piece. At the moment, the EU is involved in a review process of the general data protection directive of 1995 and similar outcomes are to be expected in the years to come.



16. GENERAL CONCLUSION

In this contribution we have discussed the concept of the system responsibility of the government in the information society. This responsibility for 'the whole' exists with regard to the protection of personal data, but it of course also exists with regard to many other human rights sensitive areas such as the fight against identity fraud and the protection of media pluralism. Exploring these domains needs to be the object of further scientific contributions.[117]

The responsibility, that we have discussed, is moral (legislators should pick up signals coming from society and act upon them, not merely giving in to economic stakeholders) *and* legally enforceable in accordance with human rights standards, legislation and jurisprudence.

Positive human rights obligations bring with them the obligation that the state should actively act against violations by government officials and individuals and has to take positive steps to ensure the enjoyment of fundamental rights. This requires supervision ,legislation and policy-making. Policy makers must rely on criminal law when they are confronted with serious crimes. Tightening unclear penal provisions, introducing new penal provisions and using police and the judiciary cannot be ruled out. System responsibility often assumes distribution of responsibility. As has been done in the area of telecommunications, the relevant actors in society must be forced to take their share of responsibility and to respect the human rights expectations of citizens, notwithstanding proportional constraints. If this distribution is unbalanced or there is no distribution at all, then the government is ultimately responsible to the European Court in Strasbourg.

The assumption that European human rights law furnishes our governments with too few practical guidelines is unwarranted. In the area of data protection, the Court has developed general principles, which are applicable in more and more cases. To a lesser extent the same is true in the fight against identity fraud and the protection of media pluralism. Member states can put these principles to work and start evaluating the adequacy of existing remedies and compensation systems. The relevance of *I. v. Finland* (judgment of July 17, 2008) for the discussion of the establishment of the information society has not received sufficient attention. The judgment of the European Court of Human Rights states explicitly that the mere fact that national legislation allows for compensation is inadequate, and that there is a need for a practical and effective protection of personal data through legislation and enforcement. Providing a system of compensation based on fair and accessible conventional procedures is important, but insufficient. A full human rights abiding structure that both protects and develops (better: encourages development) is required and this operation is increasingly urgent. The information society has been around since the nineties and governments have already had the time to act appropriately.

This contribution began with a comparison between two debates, the first on the information society and the second on respect for human rights by multinationals in 'weak' countries. In both debates, there is a strong undercurrent against regulation and government intervention, and governance gaps are being covered up, created or supported, either in the name of the newness of the technology or in the name of the need for economic development in poor countries.[118]

Within the responsibility paradigm several choices exist. Ruggie's *Protect, Respect, Remedy* scheme indicates well the indispensable basic building blocks. Whenever the theme of accountability is addressed, all three blocks have to be considered for the sake of an integrative approach. The author of this contribution has not been able to temper his fascination for the third building block, the classical legal idea of remedy. However classical it may be, its relevance remains high. Too many public and private initiatives are launched and regulated from only one perspective, the perspective of the organism that takes the initiative. Seldom are initiatives looked at from 'the back end', from the perspective of the citizen that needs to be informed about his rights and from the perspective of the supervisory authority (judge or administrative authority) that needs to safeguard the fundamental right to an effective remedy. With Ruggie's threefold scheme and his insistence on 'real' access to justice and real transparency the above trap is avoided.

Public authority has an important role to play in every integrative approach to accountability. It is up to governments to develop an efficient remedy system. Post-legislative scrutiny of key legal instruments adopted in the past should become the norm. A 2009 House of Lords' report with regard to

surveillance contains several recommendations for specific actions by governments that can be repeated here by way of illustration.[119] Some of the questions that need to be addressed are the following: Do these instruments contain clear guidance on necessity and proportionality? Is priority given to citizen-oriented considerations? Can the safeguards and restrictions placed on surveillance and data handling be improved? Are design solutions incorporated? Can the introduction of a system of judicial oversight for surveillance carried out by public authorities be foreseen? Are individuals who have been made the subject of surveillance to be informed of that surveillance, when completed, where no investigation might be prejudiced as a result? Is compensation available to those subject to unlawful surveillance by the police, intelligence services, or other public bodies acting under the powers?

Partly, these recommendations can be grouped together with state obligations to *protect* through effective regulations and effective enforcement (building block). Again a task for public authorities. In the 'Evidence' gathered by the House of Lords for its report on surveillance, that massive violations of security and privacy were not followed by appropriate sanctions was deplored: "When banks dump personal data in outdoor rubbish bins, in direct contravention of the Act, their punishment is to sign a form saying they won't do it again. When the identities of staff at Network Rail and the Department of Work and Pensions are stolen from a compromised HMRC portal to defraud the tax credit scheme, HMRC escapes unpunished".[120] Improving the legal framework with regard to cybercrime, review of the data protection directive and more effective enforcement of privacy rules are rightly on the EU agenda.

With regard to the second building block ('respect'), some favour a more stringent approach turning a duty to comply into a more active duty to prove that one is concerned and contributes to the protection of certain rights. The development should be applauded from a human rights perspective. Those who have power have to be held accountable. An information society that works, allowing providers, who do not see problems in unsafe and unregulated information services, is becoming less defensible. Citizens cannot be held responsible for a system where the government is not playing its role and forgets or refuses to hold relevant actors accountable. That is not how system responsibility works. The author of this contribution is aware of attempts to 'sell' more accountability in exchange of fewer formalities and less stringent data protection requirements on other fronts. From such a perspective, 'more accountability' seems to be instrumental for a kind of politics of good intentions ('something went wrong but I am not responsible since I actively embraced data protection'). We recall that our legal system seldom considers good intentions and motifs, but does look at behaviour and consequences. Ethically it is important to embrace the active incorporation of human rights values, but legally there would be a flaw in system responsibility if no governmental reaction followed from damage caused.

ENDNOTES

1 Thanks to Dara Hallinan for many comments on earlier versions.

2 Although a lot of current attention focuses on the need to reform EU law, in particular data protection law, and on the need to enhance the duties of data processors to put data protection principles in practice, our paper ends with a long discussion on remedy and swift and accessible legal procedures, a building block that is often neglected in current discussions. We underline however that 'system responsibility' and comprehensive accountability implies that all three parts are equally important.

3 See www.dataprotectionday.eu.

4 Clearly, many think the question is not as simple, since the "open question of final responsibility" keeps returning in public discussions (luckily the answers are not always put to the vote). Even from a human rights perspective the argument can be made that this issue is not simple – particularly with the uncertainty as to the application of norms onto data environments. However the complexity can be reduced by taking European human rights case law as guiding principles as will be done below.

5 On resistance by transnational firms against control, see J. Tully, 'The Unfreedom of the Moderns in Comparison to Their Ideals of Constitutional Democracy', *The Modern Law Review*, Volume 65, 2002, Issue 2, pages 204–228, in particular p. 222.

6 This section borrows from my work with Karen Van Laethem, in particular P. De Hert & K. Van Laethem, 'Ondernemingen als nieuwe dragers van mensenrechtenplichten?', in J. Wouters & C. Ryngaert (eds.), *Mensenrechten. Actuele brandpunten*, Leuven-The Hague, Acco, Reeks Wereldvisie n°. 5, 2008, pp. 159-178 and K. Van Laethem & P. De Hert, '*Protect, Respect, Remedy*: Het beleidsplan van de Verenigde Naties voor mensenrechten en ondernemingen', *Wereldbeeld*, Vol. 34, n°. 153, 2010/1, pp. 11-18. See also Chris Jochnick & Nina Rabaeus, 'Business and Human Rights Revitalized: a New UN Framework meets Texaco in the Amazon', *Suffolk Transnational Law Review*, 2010, Vol. 33, Issue 3, pp. 413-437.

7 General Assembly, December 21, 1990, http://www.un.org/documents/ga/res / 45/a45r186.htm.

8 UN Sub-Commission on the Promotion and Protection of Human Rights, *Norms on the responsibilities of transnational corporations and other business enterprises with regard to human rights*, 55th session, 26 August 2003, E/CN.4/Sub.2/2003/12/Rev.2.

9 This Commission has now been replaced by the Human Rights Council.

10 UN Commission on Human Rights, *Report to the Economic and Social Council on the Sixtieth Session of the Commission*, Resolution 2004/116, E/CN.4/2004/L.11/Add.7 (2004).

11 It is important to realize the difference in composition of the Sub Commission, which is comprised of 26 independent experts, and the Human Rights Commission in which 53 government representatives take part. This particular composition shows the extended political character of the Human Rights Commission, in contrast to the Sub-Commission. This factor could be one of the underlying reasons for the 'failing' of the Norms.

12 UN Commission on Human Rights, Human Rights and Transnational Corporations and Other Business Enterprises, 61st session, 15 April 2005, Resolution 2005/69, E/CN.4/2005/L.87 (2005).

13 See Special Representative to the Secretary-General on Business and Human Rights, *Protect, Respect and Remedy: A Framework for Business and Human Rights*, 7 April 2008, A/HRC/8/5 (2008). 1. Ruggie has released more on his framework since 2008. In March 2011 the final report on the Guiding Principle for the 'Respect, Protect, Remedy framework were released. Available at http://www.business-humanrights.org/media/documents/ruggie/ruggie-guiding-principles-21-mar-2011.pdf

14 For instance the British National Contact Point of the Organisation for Economic Cooperation and Development (OECD) makes us aware of the concept of due diligence of the SRSG in a human rights complaint

against a corporation. In addition the International Organization of Employers (IOE), the International Chamber of Commerce (ICC) and the Business and Industry Advisory Committee (BIAC), amongst others, accept the policy framework as guidance. Finally also non-governmental organizations (NGO's), such as Amnesty International also recognise the importance of Ruggie's work.

15 *Joint NGO Statement to the Eight Session of the Human Rights Council*, 19 May 2008, http://www.hrw.org/en/news/2008/05/19/joint-ngo-statement-eighth-session-human-rights-council.

16 See. Art. 12 - 15 of Directive 2000/31/EC of the European Parliament and the Council of 8 June 2000, concerning certain legal aspects of the services of the information society, more specifically electronic commerce in the internal market, *Official Journal,* L 178/1 of 17 July 2000. The directive is very lenient toward intermediaries, particularly with regard to the existing rules on criminal and civil liability in different countries. This directive aims to guarantee the free movement of information society services between Member States without internal borders. More freedom and confidence in electronic commerce is key. The text provides a horizontal (which is the same for all jurisdictions) limitation of liability for ISPs. It concerns Articles 12 to 14, which safeguard the service provider from liability for information on websites, which becomes available via its access service; when they are just a hatch (mere conduit), when they only stores those pages briefly when it is about frequently sought information (caching) or when they temporarily holds information about another (hosting). See critically, A. Lucas, 'La responsabilité civile des acteurs de L'internet', *Auteur&Media*, 2001, n°. 1, pp. 42-52.

17 Compliance means (only) that an organisation meets the rules, which are imposed from the outside or the inside. These are seen as a burden, which is borne grudgingly, but not as a trigger to create an asset-driven policy, whereby processes are adjusted. Accountability as proven trust needs to be contrasted with compliance as blind trust. In a scheme of accountability it is possible for the person involved to prove good behaviour because he or she took active, assignable steps to achieve a certain 'good.' See for a broader definition (over-broad) of compliance: De Vries H. & W. Janssen, 'Compliance als kans', Ego. *Magazine voor informatiemanagement*, 2010, vol. 9, n°. 3, pp. 11-15.

18 A. Meijer , 'Overheidsverantwoordelijkheid in het informatietijdperk: een pleidooi voor het creëren van genormeerde experimenteerruimte', D. Broeders, C. Cuijpers & C. Prins (eds.), *De staat van informatie*, WRR-verkenning 25, Amsterdam, Amsterdam University Press, 2011, pp. 97-132 (via http://www.wrr.nl/content.jsp?objectid=5657).

19 Idem.

20 All the judgments of the Courts are available via http://www.echr.coe.int/echr.

21 Only states can be judged in Strasbourg for alleged violations of the treaty. Complaints against corporations and individuals are inadmissible. Those have to be taken to national courts, but this presupposes that there is a judge, a sound legal system and a system based on human rights legislation.

22 P. Van Dijk, 'Positive Obligations Implied in the European Convention on Human Rights: Are the States Still the Masters of the Convention?', in M. Castermans-Holleman, Fr. Van Hoof & J. Smith, J. (eds.), *The Role of the Nation-State in the 21st Century. Human Rights, International Organisations and Foreign Policy. Essays in Honour of Peter Baehr*, The Hague, Kluwer Law International, 1998, 17-33.

23 J-F. Akandji-Kombe, 'Positive Obligations under the European Convention on Human Rights: A guide to the implementation of the European Convention on Human Rights', *Human Rights Handbook Series*, No. 7, 2007, http://echr.coe.int/NR/rdonlyres/1B521F61-A636-43F5-AD56-5F26D46A4F55/0/

DG2ENHRHAND072007.pdf. For a full explanation of the development and current status of the doctrine of positive obligations under the ECHR, including its application to other rights.

24 J.-L. Renchon, 'La Convention européenne et la régulation des relations affectives et familiales dans une société démocratique' in P. Lambert (ed.), *La mise en oeuvre interne de la convention européenne des droits de l'homme*, Brussels, Ed. du jeune barreau de Bruxelles, 1994, pp. 98-102.

25 See more in detail C. Russo, P. Trichilo & F. Marotta, 'Article 8, § 1' in *La Convention européenne des droits de l'homme. Commentaire article par article*, L.E. Pettiti, E. Decaux & P.H. Imbert (eds.), Paris, Economica, 1995, p. 308.

26 ECtHR, *Paula and Alexandra Marckx v. Belgium*, judgment of 13 June 1979; ECtHR, *Johanna Airey v. Ireland*, judgment of 9 October 1979, § 32; ECtHR, *Mark Rees v. United Kingdom*, judgment of 17 October 1986, § 36; ECtHR, *Graham Gaskin v. United Kingdom*, judgment of 7 July 1989, § 42. Also see ECtHR, *Johnston v. Ireland*, judgment of 28 December 1987. See R. Lawson, 'Positieve verplichtingen onder het EVRM: opkomst en ondergang van de faire balance-test' (deel 1), *NJCM-Bulletin*, 1995, n°. 5, 559-567.

27 In the *Stjerna* case the Court explains in an unusually clear way the difference between positive and negative obligations. The refusal of the Finnish government to allow Stjerna to change his name did not constitute an interference with his fundamental right to private and family life and the theory of the positive obligations should therefore be applied. It would be interference, according to the Court, if the government would force Stjerna to change his name (ECtHR, *Stjerna v. Finland*, judgment of 25 November 1994, § 38). About this aspect of the judgment: Lawson 1995: 743-746.

28 ECtHR, *Marie-Patrice Lassauzet and Gérard Guillot v. France*, judgment of 24 October 1996.

29 ECtHR, *Willsher v. United Kingdom*, judgment of 9 April 1997.

30 ECtHR, *Gregoria López Ostra v. Spain*, judgment of 9 December 1994, § 58; ECtHR, *Guerra v. Italy*, judgment of 19 February 1998, § 60.

31 ECtHR, *Botta v. Italy*, judgment of 24 February 1998.

32 *Op. cit.* note 20, pp 36-48, for a full description of these cases, their relevance and the application of the doctrine of positive obligations in relation to the protection of private and family life.

33 ECtHR, *Botta v. Italy*, judgment of 24 February 1998, § 34.

34 We can conclude, based on the previous decisions, that a violation of the rights contained in Article 8 ECHR is possible: - when the state interferes in these rights – when an abstention or a non-action on the part of the state ignores the rights recognised in the provision - when abstention on the part of the state gives the opportunity to third parties to ignore the discussed rights. See G. Cohen-Jonathan, *La Convention européenne des droits de l'homme*, Paris, Economica, 1989, p. 375

35 Moreover, it is necessary to specifically examine whether there is a link between a possible positive obligation and the complaint of the subject which invoked the allegation of violation of fundamental rights.

36 "The Court does not consider that Ireland can be said to have 'interfered' with Airey's private or family life: the substance of her complaint is not that the State has acted but that it has failed to act. However,

although the object of Article 8 is essentially that of protecting the individual against arbitrary interference by the public authorities, it does not merely compel the State to abstain from such interference: in addition to this primarily negative undertaking, there may be positive obligations inherent in an effective respect for family life (see the above-mentioned Marckx judgment)" (ECtHR, *Johanna Airey v. Ireland,* judgment of 9 October 1979, § 32).

37 ECtHR, *Graham Gaskin v. United Kingdom*, judgment of 7 July 1989, § 41.

38 ECtHR, *X and Y v. The Netherlands*, judgment of 26 March 1985. One day after her sixteenth birthday, Y was sexually abused by the son of the director of the residence for the mentally handicapped, where she stayed. After a decision not to prosecute by the public office, her father (X) went to court claiming that a crime had been committed; 'deliberate inducement of minors to sexual abuse' (Art. 248*ter* Dutch Criminal Code). The Arnhem Court declared the case inadmissible because, pursuant to the Criminal Code only the victim may lodge a complaint and for people under sixteen, legal representation is provided. In Strasbourg, father and daughter claimed that there had been a violation of Article 8, 3, 13 and 14 ECHR. With regard to Article 8 ECHR, they argued that for a young girl such as Y., only criminal protection is sufficient and that states have a positive duty to create sufficient legal protection through criminal law.

39 ECtHR, *X and Y v. The Netherlands*, § 23. The 'effective respect' for private life implies, the Court held, that the state has a positive obligation to take measures to ensure privacy, even in the sphere of relations between individuals.

40 ECtHR, *X and Y v. The Netherlands*, § 27. The right to respect for private life requires member states to take measures in criminal law to protect sexual integrity. There is a margin of appreciation left to states regarding their policy to combat sex crimes and aggression, but as in this case, a civil law protection does not satisfy and is simply not enough. Additional criminal law protection is needed for serious violations of sexual integrity.

41 Renchon, *l.c.*, pp. 98-102.

42 See ECtHR, *Paula and Alexandra Marckx v. Belgium*, § 31.

43 See ECtHR, *X and Y v. The Netherlands*, § 23.

44 ECtHR, *M.C. v. Bulgaria*, judgment of 4 December 2003.

45 The facts did not lead to the punishment of the offender due to certain legal difficulties. Because the alleged victim could not prove that she resisted the sexual acts, the accused were not criminally convicted The applicant stated that in the summer of 1995, when she was fourteen years old, two men raped her. She volunteered to go along with three vague acquaintances in a car to a disco, but the men then took her to a pond, allegedly for swimming. The first rape happened there. Frightened and embarrassed the girl had not the strength to resist. Subsequently she went with the men, back to a house where a second man raped her. In his own words, she cried and begged to stop, but offered no physical resistance. When her mother found her the next morning in that house, she brought her to the hospital where it was found that she had had sexual intercourse. The men did not deny this, but claimed that the intercourse was voluntary. Eventually it ended in a lawsuit, whereby the men were acquitted. The judge found no evidence that the girl was violently forced to have sex, since there was no evidence that she resisted.

46 The Court reproached that the Bulgarian courts, in the absence of direct evidence of rape, did not reconstruct the circumstances of the crime and did not evaluate the credibility of the contradictory statements from which possible indirect evidence of absence of consent could be inferred. The report of the Bulgarian researchers showed that the Bulgarian judges did not rule out that the girl did not consent, but that they, because of lack of evidence of resistance, did not want to conclude that the perpetrators had understood that she did not consent. The Court stated explicitly that in rape cases there is an obligation to focus the investigation on the question of consent, and from that perspective to investigate all the relevant facts and circumstances. It should also take into account the special vulnerability and specific psychology of young victims. According to the Strasbourg judges, the Bulgarian government failed to fulfil the public duty to offer effective criminal law protection against rape and sexual abuse. Consequently, the Court concluded that Articles 3 (right to protection against inhuman treatment) and 8 (right to privacy) ECHR were violated.

47 In Bulgarian law, rape is only punishable when there is evidence of resistance by the victim. Simply not agreeing is insufficient. The text of the Bulgarian criminal provision on rape requires no evidence of physical resistance, but the requirement is 'read into' the provisions by the courts. For the European Court this state of affairs does not meet the European standards requiring states to criminalise and effectively prosecute non-consensual sexual acts, even if the victim did not physically resist. The Court bases this interpretation, amongst others, on the evolution of criminal law in this area in most European countries, as well as on the law of the International Criminal Tribunal for former Yugoslavia. In particular, Article 8 ECHR provides for measures to regulate relations between individuals. Particularly severe violations of fundamental values and privacy cannot be settled by legal protection, which is not based on criminal law. In this context criminal law is the only appropriate government measure. See paragraph 150: "Positive obligations on the State are inherent, in the right to effective respect for private life under Article 8; these obligations may involve the adoption of measures even in the sphere of the relations of individuals between themselves. While the choice of the means to secure compliance with Article 8 in the sphere of protection against acts of individuals is in principle within the State's margin of appreciation, effective deterrence against grave acts such as rape, where fundamental values and essential aspects of private life are at stake, requires efficient criminal-law provisions. Children and other vulnerable individuals, in particular, are entitled to effective protection." (see ECtHR, *X and Y v. the Netherlands*, judgment of 26 March 1985). In combination with the investigation and enforcement duties based on article 3 ECHR, the Court decided that: "States have a positive obligation inherent in Articles 3 and 8 of the Convention to enact criminal law provisions effectively punishing rape and to apply them in practice through effective investigation and prosecution" (ECtHR, *M.C. v. Bulgaria*, § 153.)

48 Of course, when there is no human rights problem or conflict, then no positive state duties come into play. If one were to imagine that the information society was human rights neutral, then nothing would need to be done. The well known popular mantras about self-regulation by industry could then be made heard.

49 Additional evidence for this statement will be given with the discussion of judgments such as *Gaskin*, *Peck* and *I. v. Finland* below.

50 If it does not turn ICT firms into policemen, it will have to police them individually.

51 A. Meijer , *l.c.*, p.101 and following.

52 Idem, p. 111 and following.

53 Idem, p. 98 and 106.

54 Meijer, a non-legal scholar that has guided us considerably with his work on responsibility, seemingly downplays the legal dimension of this broader notion of responsibility.

55 In Strasbourg's human rights perspective, the government is made responsible for not responding appropriately to human rights violations under its jurisdiction. Strasbourg, therefore, takes care of the legal leap from responsibility for its own disputes to 'system responsibility'.

56 See Gutwirth S., De Hert P. & De Sutter, L., 'The Trouble with Technology Regulation: Why Lessig's 'Optimal Mix' Will Not Work', in R. Brownsword & K. Yeung (eds.), *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes*, Oxford University Press, 2008, pp. 193-218; De Sutter, L. & Gutwirth, S., 'Droit et cosmopolitique. Notes sur la contribution de Bruno Latour à la pensée du droit', *Droit et Société 56*-57, 2004, pp. 259-289.

57 This contribution by no means wants to open the globalization discussion. It however strikes us that authors such as Tully and Kreide, both elaborating constructive proposals to strengthen the legitimacy of contemporary norm setting procedures, highlight political legitimacy and participation, but ignore 'simple' legal responses, such as the Strasbourg system discussed here, which strengthen rule of law legitimacy. See J. Tully, *l.c.*, pp. 204–228 and Regina Kreide, 'The Ambivalence of Juridification. On Legitimate Governance in the International Context', *Global Justice: Theory Practice Rhetoric*, 2009, Issue 2,

58 A. Meijer , *l.c.*, p. 107.

59 Much of what is involved in legal protection, is the unravelling of decision-making processes, to determine whether the process of the practice has been meticulous in all phases. Such process is much more difficult to verify when automated processes are involved, because then, how the system was designed must be tested. This can be a rather difficult, abstract, and meaningless exercise.

60 Again we remind the reader that additional evidence for this statement will be given with the discussion of judgments *Gaskin*, *Peck* and especially *I. v. Finland* below.

61 O. De Schutter, 'Reasonable Accommodations and Positive Obligations in the European Convention on Human Rights', in Lawson, A. & Gooding, C. (eds.), *Disability Rights in Europe: From Theory to Practice*, Oxford, Hart, 2005, pp. 35-64

62 More than often judges restrain themselves because of the scarcity of societal resources. If a judge accepts a claim, it will often be at the expense of other necessary government functions (O. De Schutter, *l.c.*, pp. 42-43). De Schutter refers to the work of Lon Fuller who developed the idea of poly-centrality: certain disputes are inherently incapable to be judged by courts because they hide complex issues and interests that are interlinked. See L Fuller, 'The Forms and Limits of Adjudication', *Harvard L Rev*, 1972, Vol. 92, p. 353 and further.

63 This is consistent with the view that the European human rights system is based on the so-called subsidiary principle. This principle states that the protection of the rights enshrined in the Convention is primarily a matter for the member states. They should ensure an effective protection and redress possibility when protection somehow fails. The European system only plays a complementary role and will only be visible when the national authorities do not, or insufficiently, devote themselves to their duties. Cf. J. Vande Lanotte & Y. Haeck, *Handboek EVRM: Deel I Algemene beginselen,* Antwerp, Intersentia, 2005, pp. 179-180. The principle is not explicitly reflected in the European Convention on Human Rights, but rather inherently present.

64 Compare with ECtHR, *Armonas v. Lithuania*, judgment of 25 November 200 § 46: "The Court agrees with the Government that a State enjoys a certain margin of appreciation in deciding what 'respect' for private life requires in particular circumstances (see *Stubbings and Others v. the United Kingdom*, judgment of 22 October 1996, §§ 62-63; ECtHR, *X and Y v. the Netherlands*, § 24). The Court also acknowledges that certain financial standards based on the economic situation of the State are to be taken into account when determining the measures required for the better implementation of the foregoing obligation."

65 ECtHR, *Armonas v. Lithuania*, § 38: "The Court reiterates that, as regards such positive obligations, the notion of respect is not clear-cut. In view of the diversity of the practices followed and the situations obtaining in the Contracting States, the notion's requirements will vary considerably from case to case. Accordingly, this is an area in which the Contracting Parties enjoy a wide margin of appreciation in determining the steps to be taken to ensure compliance with the Convention, account being taken of the needs and resources of the community and of individuals (see ECtHR, *Johnston and Others v. Ireland*, judgment of 18 December 1986, § 55). The Court nonetheless recalls that Article 8, like any other provision of the Convention or its Protocols, must be interpreted in such a way as to guarantee not rights that are theoretical or illusory but rights that are practical and effective (see *Shevanova v. Latvia*, judgment of 15 June 2006, § 69)."

66 A citizen or group cannot go to Strasbourg as a result of absence of a legal regime for technology when there is no identifiable, concrete human rights problem. This is what happened when the Belgian League for Human Rights went to Strasbourg to challenge the lack of specific regulation concerning CCTV in Belgian legislation. The complaint was declared inadmissible. See European Commission on Human Rights, *Pierre Herbecq and Ligue des droits de l'homme v. Belgium*, Decision of 14 January 1998, requests n°. 32200/96 & 32201/96, *J.T.D.E.*, 1998, pp. 67-68.

67 ECtHR, *Peck v. United Kingdom*, judgment of 28 January 2003.

68 The British government had unsuccessfully invoked Article 10 ECHR. The defence was that an effective legal protection against the violation of the right to privacy by the media was a threat to press freedom. The Court, however, does not agree. The Court considers that "the Council, and therefore the media, could have achieved their objectives by properly masking, or taking appropriate steps to ensure such masking of the applicant's identity".

69 ECtHR, *I. v. Finland*, judgment of 17 July 2008. See Jari Råman, 'European Court of Human Rights: Failure to take effective information security measures to protect sensitive personal data violates right to privacy – I v. Finland, no. 20511/03, 17 July 2008', *Computer Law & Security Report*, 2008, volume 24, nr. 6, pp. 562-564

70 Between 1989 and 1994 the applicant worked as a nurse on the eye diseases ward in a public hospital in Finland. Since 1987 she had regularly visited the 'contagious diseases' department in the same hospital as she had been diagnosed with HIV. After working for three years in the hospital she started to suspect that her colleagues knew about her illness. At that time employees of the hospital had free access to information on patients and their health. At her request, this situation was put right by only allowing the staff members responsible to have access to their patients' records. Further, the claimant was registered under a false name and under a new unique number. In 1995, however, her contract was not renewed. In November 1996, the claimant complained to the County Administrative Board about misuse of her personal data. She asked to be allowed to see who was able to access her information. The responsible official claimed that this was impossible claiming that the system only showed the five most recent consultations and the consulting department, not the person who had consulted the file. In addition, this information had been removed when the file was put back in the archive. The complaint of the claimant was therefore dismissed. Afterwards, the archive of the hospital was adjusted in such a way that it became possible to

identify the person who had consulted the patient data. A series of civil proceedings, which were brought before the District Court and Court of Appeal by the claimant against the authority which was responsible for monitoring the hospital, were all rejected because the claimant could not prove that her data had been consulted illegally. An appeal to the Finnish Supreme Court was also rejected, whereupon the claimant brought the claim to the European Court of Human Rights. In Strasbourg the claimant argued that the Finnish Supervisory Authority had failed in its obligation to set up a system in which patient records could not be used illegally, which she considered to be contrary to Article 8 of the ECHR. According to the claimant the requirement for retrospective monitoring is essential to respect this right. The Finnish government replied that the national legislation adequately protects patient data and that "systems which are developed in hospitals that make the record keeping of patients possible, can only work properly if detailed instructions are given to staff, when they respect high moral standards, when there is supervision and when the staff respect professional secrecy." In this case, it would not have been possible, according to the Finnish government, for the hospital to create a system whereby the authenticity of every request could be controlled in advance, since access to the data was often required immediately and urgently.

71 ECtHR, *I. v. Finland*, § 36.

72 ECtHR, *I. v. Finland*, § 38.

73 ECtHR, *I. v. Finland*, § 38.

74 ECtHR, *I. v. Finland*, § 40.

75 ECtHR, *I. v. Finland*, § 47.

76 Lawson & L. Verheij, 'Kroniek van de grondrechten 2002' *Nederlands Juristenblad*, 2002, Vl. 77, n°. 10, (pp. 513-523), p. 514

77 In this regard, she does not only complain about a breach of Article 8 ECHR, but also of Article 6 and 13 ECHR

78 ECtHR, *I. v. Finland*, § 44: "The Court notes that the applicant lost her civil action because she was unable to prove, on the facts, a causal connection between the deficiencies in the access security rules and the dissemination of information about her medical condition. However, to place such a burden of proof on the applicant is to overlook the acknowledged deficiencies in the hospital's record keeping at the material time. It is plain that had the hospital provided greater control over access to health records by restricting access to health professionals directly involved in the applicant's treatment or by maintaining a log of all persons who had accessed the applicant's medical file, the applicant would have been placed in a less disadvantaged position before the domestic courts. For the Court, what is decisive is that the records system in place in the hospital was clearly not in accordance with the legal requirements contained in section 26 of the Personal Files Act, a fact that was not given due weight by the domestic courts."

79 "The Court finds it established that the applicant must have suffered non-pecuniary damage as a result of the State's failure to adequately secure her patient record against the risk of unauthorised access. It considers that sufficient just satisfaction would not be provided solely by the finding of a violation and that compensation has thus to be awarded. Deciding on an equitable basis, it awards the applicant EUR 8,000 under this head" (ECtHR, *I. v. Finland*, § 47).

80 ECtHR, *Armonas v. Lithuania*. judgment of 25 November 2008.

81 There is insufficient evidence for the extramarital relationship so that triggers compensation, the local court held, but there was no reason to give compensation for the other facts: the information on the extramarital relationship and health status were not made known intentionally.

82 It was not clear whether further action was possible for the family of the original victim of a possible violation of a treaty right. The Court responded positively about this. The Court finds that the claimant may apply to the European Court as a victim. The Court had previously held that a case would be inadmissible if it were to declare the substance of the matter too closely linked to the deceased and untransferable to the heirs. However in this case this was not the case. Following the publication of the article the family was forced to move and also the national courts had ruled that the article had limited the communication ability of the family. The article therefore had a negative impact on both the applicant and her child. The argument of the Lithuanian government that the applicant was not a victim anymore, because the national judge had already ruled a violation of her private life and compensation had been awarded, was dismissed. This does not affect a possible classification as victim"Where Does The Quote Start Here?.

83 ECtHR, *Armonas v. Lithuania*, § 36.

84 ECtHR, *Armonas v. Lithuania*, § 37.

85 To better balance both rights at stake, the Court distinguished, with regard to the freedom of the press, between distributing factual information as part of a public debate on the one hand, and distasteful allegations concerning the private life of a person on the other (ECtHR, *Armonas v. Lithuania*, § 39). Turning to the right to protection of privacy, the Court observes that the right is there to encourage people in their development. The protection offered goes far beyond the family circle and includes a certain social dimension of individual privacy (ECtHR, *Armonas v. Lithuania*, § 39). Privacy as a fundamental right was therefore found to be undoubtedly applicable to this case.

86 ECtHR, *Armonas v. Lithuania*, § 47.

87 ECtHR, *Armonas v. Lithuania*, § 47.

88 The main findings of *Armonas* about the protection of persons in the media were already present in another famous case, this time from the Court of Justice in Luxembourg: Case *Bodil Lindqvist* on 6 November 2003. However *Armonas* enlightens us further than *Lindqvist* about how to make the balance between the protection of privacy and protection of press freedom and expression, especially through the important distinction between the distribution of factual information as part of a public debate on the one hand, and distasteful allegations concerning the private life of a person on the other. See Court of Justice, *Bodil Lindqvist*, case C-101/01, judgment of 6 November 2003 via http://eur-lex.europa.eu. In this judgment the Court of Justice judged the electronic publication of personal data on a website on the Internet in the context of Directive 95/46/EG concerning the data protection of natural persons. The case concerned a volunteer in a protestant church community in Sweden, who on their own initiative had developed web page and had disseminated names, telephone numbers and information about their proceedings and hobbies, not just about her but also about her colleagues. In addition, she mentioned that one of her colleagues had injured her foot and was on sick leave.

89 See D. Voorhoof, 'Commercieel portretrecht in België', in Dirk Visser, Richard van Oerle, Jaap Spoor (eds.), *Commercieel portretrecht*, Amsterdam, Uitgeverij deLex, 2009, (pp. 145-165), p. 155 with a discussion of *Armonas v. Lithuania* and similar judgments.

90 See in addition to *Armonis* also ECtHR, *Reklos & Davourlis v. Greece*, judgment of 15 January 2009,§ 47.

91 European Parliament, the Council and the Commission, 'Charter of the Fundamental Rights of the European Union', *Official Journal*, C 364 of 18 December 2000, pp. 1-22 (http://eur-lex. europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2000:364:0001:0022:nl:pdf).

92 European Parliament, the Council and the Commission, 'Charter of the Fundamental Rights of the European Union (2007/C 303/01)', *Official Journal*, C 303, 14 December 2007: pp. 1-16 (http://eur lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2007:303:0001:0016:nl:pdf). The Treaty of Lisbon provides the Charter with binding power by taking up giving it a status by which it obtains the same legal power as the Treaties This was the reason that the Charter was proclaimed a second time in December 2007.

93 Treaty of Lisbon of 13 December 2007 to change the Treaty concerning the European Union and the Treaty of the establishment of the European Community, signed in Lisbon, *Official Journal*, C 306, 17 December 2007, pp. 1-231 (http://eurlex.europa.eu/joHtml.do?uri=oj:C:2007:306:som:nl:html). The Treaty came into force on 1 December 2009.

94 About the lack of purpose limitation principle in the law of the United States, see De Hert and Bellanova 2008.

95 V. Pop, 'Ripples of discontent as MEPs reject US bank data deal', *EUobserver*, 2010 via http://euobserver.com/9/29455/?rk=1

96 OECD-Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data, 23 September 1980 in Guidelines governing the protection of privacy and transborder data flows of personal data, Paris, OECD, 1980, 9-12; International Legal Materials, 1981, I, 317.

97 Treaty of Strasbourg: Convention for the protection of individuals with regard to automatic processing of personal data, Council of Europe, January 28, 1981, European Treaty Series, nr. 108; International Legal Materials, 1981, I: 422.

98 Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 concerning the protection of natural persons in relation to the processing of personal data and concerning the free traffic of those data, *Official Journal*, L 381 of 23 November 1995.

99 Framework decision 2008/977/JHA of the Council of 27 November 2008 about the protection of personal data which are processed in the context of police and criminal justice cooperation in criminal cases, *Official Journal*, L 350, 30 December 2009, pp. 60-71.

100 British Security Industry Association, 'Memorandum by the British Security Industry Association (BSIA)' in House Of Lords, Selected Committee on the Constitution, *Surveillance: Citizens and the State*, HL Paper 18-II, 2nd Report of Session 2008-2009, Volume II: Evidence, pp. 392-394

101 See P. Hustinx, 'Evidence', in House Of Lords, Selected Committee on the Constitution, *Surveillance: Citizens and the State*, HL Paper 18-II, 2nd Report of Session 2008-2009, Volume II: Evidence, pp. 166-171, p. 171 (rejecting specific regulation for Radio Frequency Identification.

102 About the lack of regulation on biometrics see E. Kindt & L. Müller (eds.), *The privacy legal framework for biometrics*, Fidis, May 2009, D13.4. 134p. (via http://www.fidis.net/fileadmin/fidis/deliverables/new_deliverables3/fidis_deliverable13_4_v_1.1.pdf). P. De Hert & A. Sprokkereef, *The Use of Privacy Enhancing Aspects of Biometrics. Biometrics as a PET (privacy enhancing technology) in the Dutch private and semi-public domain*, 2009, Tilburg, Tilt, Report produced with the funding of Alliantie Vitaal Bestuur, 50p. (http://www.uvt.nl/faculteiten/frw/onderzoek/tilt/frw/reportpets/sprokkereef.pdf)

103 A. Brouwer, 'The EU Passenger Name Record (PNR) System and Human Rights: Transferring Passenger Data or Passenger Freedom?', *CEPS Working Document* No. 320, 2009: 26-27

104 See L.C. Baldor, 'Experts say US must do more to secure the Internet', The Associated Press, February 23, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/02/23/AR2010022304211.html:. "Comparing the digital age to the dawn of automobiles, analysts said more government regulations may be the only way to force the public and private sectors to adequately counter cyber threats. They compared the need for new oversight to regulations for seat belts and safety equipment that made the highways safer."

105 Directive 97/66/EC of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunication sector, *Official Journal*, L 24 of 30 January 1998: 1-8. About this Directive: F. Cuny, 'Commentaire de la directive européenne du 15 décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications', *Dr. l'Inf. & Tél.*, 1998, n°. 2, pp. 62-67; R. Roy, ,Geänderten Entwurf der EG-Richtlinie zum Datenschutz in digitalen Telekommunikationsnetzen', *R.D.V.*, 1995, n°. 2, pp. 52-57.

106 ISDN stands for Integrated Services Digital Network.

107 Art. 5 Directive 97/66/EC.

108 Art. 8 Directive 97/66/EC. The directive gives each subscriber the possibility of free per-call caller ID blocking (with the possibility to turn it off), so he remains anonymous. Also, each subscriber has the ability to block certain incoming numbers. In some cases calls may unblocked: for example with heavy breathing calls, as part of a criminal investigation and calls relating to certain emergency services (art. 9 of Directive 97/66/ EC).

109 Art. 6 Directive 97/66/EC. Some data are allowed to be stored and sold, but in that case the subscriber has the right to resist, in the sense that he must agree to the sale.

110 Art. 3 Directive 97/66/EC.

111 Directive 2002/58/EC of the European Parliament and the Council of 12 July 2002 concerning the processing of personal data and protection of privacy in the electronic communication sector (Directive concerning privacy and electronic communication), *Official Journal*, L 201, of 31 July 2002, pp. 37-47

112 Directive 2009/136/EC of the European Parliament and the Council of 25 November 2009 for amendment of Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services; Directive 2002/58/EC concerning the processing of personal data and protection of privacy in the electronic communication sector and regulation (EC) n°. 2006/2004 concerning cooperation between the national bodies responsible for enforcement of consumer protection laws, *Official Journal*, L 337, 18 December 2009, pp. 11-36.

113 The ePrivacy Directive is a specific directive and the new measures focus primarily on the providers of electronic communications such as telecommunications companies and Internet service providers. Given the growing interdependence between the I (information) and C (communication) from ICT this is already a substantial group within the information society. There is also the expectation that a number of new measures from the ePrivacy directive will be generalised in the forthcoming review of the general directive of 1995, so they will apply to everyone processing personal data, including those outside the telecommunications sector.

114 An "infringement in relation to personal data" is broadly defined as "a breach of security leading to the accidental or unlawful destruction, alteration, unauthorized disclosure of or access to personal data transmitted, stored or otherwise processed in connection with the provision of a public electronic communications in the Community ".

115 In its notification to the user, the provider has to at least state the nature of the infringement, the relevant contact information and suggest measures to alleviate the potential negative consequences of the violation. The individual user does not need to be notified if the provider shows to the competent national authority that he has protected the information with technical protection measures that make the data unintelligible to unauthorized parties. If the provider decides not to inform individual users but the national competent authority considers that the infringement may have an adverse effect on individual users, it can force the provider to inform individual users. This authority may also issue instructions on the circumstances in which notification is required, their format and how the notification should be done.

116 Some of the imperfections of the 2002 ePrivacy Directive have been eliminated in the new regime. Amongst others, the scope of the ban is extended. Under the old system this was limited to the situation where the access and information storage on the user devices was done through electronic communications. It was not clear whether the scheme was applicable to the situation where cookies, spyware and the like ended up on the user device through software ended up on external storage media (such as CD-ROMs and USB sticks) or downloads. To ensure that these would also fall within the scope, the words "through the use of electronic communications" were deleted.

117 See P. De Hert, 'Systeemverantwoordelijkheid voor de informatiemaatschappij als positieve mensenrechten verplichting', in Dennis Broeders, C. Cuijpers & J.E.J. Prins (eds.), *De staat van informatie*, WRR-verkenning 25, Amsterdam, Amsterdam University Press, 2011, pp. 33-95

118 See the declaration of State Secretary of Economic Affairs in his letter to the Chairman of the House of Representatives, 30 May 2008, *the House of Representatives*, Conference year 2007–2008, 31200 xiii, nr. 57.

119 House of Lords, Selected Committee on the Constitution, *Surveillance: Citizens and the State*, HL Paper 18-I, 2nd Report of Session 2008-2009, Volume I: Report, pp. 107-108

120 "Memorandum by the Open Rights Group" in HOUSE OF LORDS, Selected Committee on the Constitution, *Surveillance: Citizens and the State*, HL Paper 18-II, 2nd Report of Session 2008-2009, Volume II: Evidence, pp. 433-435, p. 433

THE INFLUENCE OF EUROPEAN DATA PRIVACY STANDARDS OUTSIDE EUROPE: IMPLICATIONS FOR GLOBALISATION OF CONVENTION 108

Graham Greenleaf[1]*,*
Professor of Law & Information Systems, University of New South Wales

1. INTRODUCTION: THINKING GLOBALLY

International agreements, 'European' standards

International agreements concerning data privacy have contributed a great deal to the development of consistency of national data privacy laws. From the start of the 1980s the non-binding OECD privacy Guidelines (OECD, 1980) and the first binding international agreement, the Council of Europe data protection Convention (CoE, 1981 - the *Convention for the protection of individuals with regard to automatic processing of personal data*), both embodied privacy principles with many similarities but not identical substance, and expressed in somewhat different language.

From the mid-1990s the European Union's data protection Directive (EU, 1995) embodied a set of privacy principles consistent with, but somewhat stronger than, those in the OECD and CoE agreements. However, the Directive added much stronger enforcement requirements, including establishment of an independent DPA and a right to have disputes heard by the courts. Unlike either of the earlier agreements, it also required limitations on data exports to countries outside the EU which did not have 'adequate' privacy laws (discussed in more detail later). The standards set by the Directive have become recognised as the strongest standard for data privacy in an international instrument. The Convention also now has an Additional Protocol (ETS No 181 – CoE, 2001) requiring data export limitations and supervisory authorities, so as to better align it with the Directive.

This paper considers the implications of these two key European privacy standards – Council of Europe Convention 108 (and its Additional Protocol) and the EU Directive – for countries outside Europe. But their implications for European countries are also changing.

The real world of data privacy laws: 78 countries and growing

In 'Global data privacy laws: Forty years of acceleration' (Greenleaf, 2011) the question 'How many countries now have data protection laws?' was answered with '76', but the answer is now '78' since Costa Rica adopted a data privacy law in September 2011, and Vietnam's new consumer protection law (containing a privacy code) came into effect in July 2011. The unexpectedly high answer (the conventional answer was a somewhat vague 'about sixty' or perhaps 'more than sixty') has considerable implications for European privacy standards.

In the abovementioned analysis and its accompanying Table, a country is only considered to have a 'data privacy law' if it has a national law which provides, in relation to most aspects of the operation of the private sector, a set of basic data privacy principles, to a standard at least approximating the OECD Guidelines, plus some methods of statutorily-mandated enforcement (ie not only self-regulation). Countries that have national public sector laws but no comprehensive private sector laws (only the USA and Thailand are known) are therefore excluded. Almost all the 78 jurisdictions have laws which also cover their national public sectors (the only exceptions being Malaysia, Vietnam and India), possibly by different legislation to that covering the private sector. Therefore, there are 75 countries providing comprehensive coverage of both their private and public sectors. Almost all of these jurisdictions provide in their legislation for a Data Protection Authority (DPA), a separate institution with responsibility for the data privacy legislation, although these vary greatly in name, functions and degree of independence from other government authorities. Chile, the Kyrgyz Republic, India, Japan, Vietnam and Taiwan are the few remaining exceptions with no DPA.

The total number of new data privacy laws globally, viewed by decade of enactment, shows that their growth is accelerating, not merely expanding linearly: 7 (1970s), 10 (1980s), 19 (1990s), 32 (2000s) and 10 (1.75 years of 2010s), giving the total of 78. In the first 21 months of this decade 10 new laws have been enacted (Faroe Islands, Malaysia, Mexico, India, Peru, Russia - more accurately, brought into force – Ukraine, Angola, Vietnam and Costa Rica), making this the most intensive period of data protection developments in the last 40 years. By region, the distribution of laws is in order: European Union (27); other European Countries (22); non-European countries (28) (Asia (8); Latin America (7); Sub-Saharan Africa (6); North Africa and Middle East (3); Australasia (2); North America (1); Caribbean (1); Central Asia (1); and Pacific Islands (0)). There are Bills or proposed Bills for new data privacy laws in many countries, including Brazil, Ghana, South Africa, Thailand, the Philippines and Singapore. At the current rate of growth, there may be more than 80 data privacy laws by early 2012.

Europe's data privacy laws will soon be outnumbered

The 22 European separate jurisdictions which are not EU member states but do have data privacy laws are: Albania; Andorra; Azerbajain; Bosnia & Herzegovina; Croatia; Faroe Islands; FYROM (Macedonia); Gibraltar; Guernsey; Iceland; Isle of Man; Jersey; Liechtenstein; Montenegro; Moldova; Monaco; Norway; Russia; San Marino; Serbia; Switzerland; and Ukraine. So there are a total of 50 European data privacy laws. There is little room for expansion within Europe: Armenia, Georgia, Turkey and Belarus are the only remaining European states without data privacy laws.

Most expansion of data privacy laws is now occurring outside Europe. There are now 29 data privacy laws outside Europe (see the Table following), more than the number of countries in the EU. In a few years, when the total of countries with data protection laws is likely to pass 100 (assuming the current rate of 5 or 6 new laws per annum, almost all from outside Europe), Europe as a whole will be in the minority of countries with data privacy laws. This geopolitical fact has considerable implications for both the Directive and Convention 108.

The outliers: The influence of the USA and China

The two major exceptions to the development of comprehensive data privacy laws, in terms of global political and economic influence, are the USA and China. The economic and political power

of both counties requires special consideration in any assessment of global data privacy developments. However, the increasing isolation of their positions must also be recognised. Most other countries that do not have (or clearly plan to have) data privacy laws have relatively limited global influence although some (eg Indonesia and Nigeria) have substantial populations. In Latin America, Africa, and Asia, a steady expansion in the number of countries adopting data privacy laws seems likely. In the Middle East and Central Asia, such laws are starting to emerge. Most of the rest of the world is increasingly adopting a generally consistent set of principles and establishing a DPA as part of the enforcement mechanism, as is demonstrated in the next part of this paper. Other countries that have previously taken an approach similar to the USA are changing course: Mexico, Malaysia and Peru have enacted laws which are both OECD and EU-influenced, with a DPA; Singapore and the Philippines are likely to do similarly (Greenleaf, 2011). Japan and Taiwan have not yet adopted a DPA, but have enacted otherwise extensive data privacy laws. US-sponsored APEC-supported alternatives which might have impeded the spread of strong data privacy laws in Asia and Latin America largely appear to have failed. There is nothing occurring in the rest of the world which represents a coherent alternative to the spread of European-influenced data privacy standards, or even coherent resistance (except in the USA) to the adoption of such standards.

The USA's standards are fundamentally lower than Europe's

The USA has many privacy laws and some effective enforcement, but no comprehensive privacy law in the private sector, nor much prospect of one, despite periodic calls for one from major companies and Bills introduced into Congress. It is not the case that the USA does not have any standards for private sector data privacy, but they must be inferred from many scattered pieces of sectoral legislation, the absence of any significant legislation in many sectors (just as important), some State constitutional protections, and the common law. Concerning the last of these, the USA's privacy torts, despite their fame, are only capable of sporadic contributions to data privacy (Solove, 2004: 57-62). A recent report (Hoofnagle, 2010) asserts that 'the US approach is incoherent, sectorally-based, and … legislative protections are largely reactive, driven by outrage at particular, narrow practices'. 'In [Federal] statutory law, privacy rights are found in the criminal code, the civil code, evidentiary law, family law, property law, contracts, and in administrative regulations. No single overarching statute even attempts to unify these interests in the diverse contexts in which "privacy" is used to frame some value'. The Federal Trade Commission (FTC) has gradually adopted the broadest role (though still in relation to only the parts of the private sector where it has jurisdiction, under its authority to counter 'unfair trade practices', particularly online misrepresentation concerning the purpose of collection of personal information and assurances of data security. But its reach is limited to ensuring that companies keep the promises they make in their privacy policies or otherwise (Solove, 2004: 73) and (though rarely used) unfairness cases. However, as Hoofnagle says, even within its limited ambit, '[i]t is important to note that the FTC has adopted a more limited set of fair information practices than international authorities. The agency is concerned with notice, choice, access, security, and accountability'. Hoofnagle summarises the other main gaps in the privacy principles adopted across US laws as follows: 'US privacy law typically allows businesses to use personal information for different purposes, including for marketing, without the data subject's consent. This is because the sectoral system leaves many businesses unregulated… Just a handful of laws create explicit purpose limitations'; and 'US privacy law generally does not have limitations on collection of personal information. Collection limitation runs counter to the notion of most enterprises, which attempt to collect as much information as possible in transactions'. The protection of privacy-affecting marketing as 'free speech' goes beyond

what is accepted in many other countries. Although the Federal *Privacy Act* (1974) applied most of the pioneering HEW principles of 1973 to the federal public sector, including the 'purpose limitation' principle that information collected for one purpose should not be used or made available for other purposes without consent (Regan, 2008: 56), little of the main subsequent legislation applying to the private sector has applied this principle (Regan, 2008: 57-60; Solove, 2004: 67-72). The result is a patchwork of inadequate laws that, in any event, 'only cover a small geography of the database problem' (Solve, 2004: 71).

There is therefore an arguable case that, even if all of the USA's existing sectoral laws (including FTC protections and privacy torts) were consolidated into one Act, and even if that Act was extended to the whole of the private sector, the standards it would embody would fall short of European standards in fundamental respects. The lack of general application of purpose limitation principles makes it questionable whether the USA has even complied with the OECD guidelines in relation to its private sector. The lack of laws limiting collection to the minimum data required for a legitimate purpose is a further difference from fundamental European standards (at least on paper: criticism of weak enforcement is justified). US data privacy laws enacted in the USA may be weaker on these points than European laws not only as a matter of fact, but also as a matter of constitutional necessity. This is because the First Amendment to the US Constitution is likely to make it unconstitutional for the federal government to impose some restrictions on disclosure, use and collection of personal information by the private sector (and perhaps by the States). Regan argues that any US privacy legislation is likely to be challenged in the courts, including 'on the basis of First Amendment grounds that any information, including that about individuals, should flow freely and without government restriction' (Regan, 2008: 51). Hoofnagle, however, considered that since US West v FCC (1999) held that opt-in consent restrictions on secondary use of telephone records violated commercial free speech rights (with which another circuit court has disagreed), subsequent court decisions 'have consistently upheld data-protection-style privacy laws against First Amendment challenges' (Hoofnagle, 2010: 7). Other scholars had taken a more negative position that the First Amendment protects a right to gather information (Froomkin, 2000: 1508), questioning the correctness of the Supreme Court's decision in *Reno v Condon* which upheld a federal law limiting access to personal information in the drivers' licence databases maintained by the fifty states. Hoofnagle's more positive assessment has now been made very doubtful by the U.S. Supreme Court's recent decision in *Sorrell v. IMS Health Inc.*, 131 S.Ct. 2653, 2672 (2011), which found that a state law that prohibited the sale of information on doctors' prescribing habits to marketers for drug companies violated the First Amendment (Julin, 2011). In relation to the Do-Not-Track bills currently before Congress, it has been argued that the principles of this case 'strongly suggest that any such legislation would run afoul of the First Amendment' (Julin, 2011), but other more narrow readings of the decision are also possible. The full scope of constitutional limitations on the possibility of data privacy laws in the USA is clearly not yet settled, but it seems that they are a significant if uncertain limitation (perhaps an example of a 'known unknown'). It is beyond the scope of this paper to demonstrate the scope of either the actual or potential limits on US data privacy laws, but it is important to state that there is a arguable case that US privacy standards have both actual and inherent limitations which place them at odds with fundamental aspects of European privacy standards.

These limitations do not mean that the USA lacks privacy standards or privacy innovations. In recent years there has been a profusion of innovative state laws in areas such as data breach notification and laws to limit effects of identity theft. Nor does it lack examples of effective enforce-

ment. The high financial settlements often imposed by the Federal Trade Commission (FTC) on the basis of sectoral laws on deceptive practices amount to around US$40 million in fines (Hoofnagle's estimate), which is still not a substantial amount given the revenues of the companies concerned, but the concomitant damage to reputation may be far more substantial. R E Smith (2011) gives a succinct but lengthy catalog of where US laws have pioneered particular privacy protections, often with laws that are stronger than elsewhere. These laws are significant, but don't add up to anything like a comprehensive data privacy law, or a coherent alternative set of policies to protect data privacy.

The main point being made here is that the USA's exceptional position should not be confused with a schism in global approaches to data privacy. Increasingly, the position is that the USA is the only significant outrider attempting to defend providing data privacy protection by a patchwork of sectoral laws (with significant limits to their principles arising from circumstances which may be unique to the USA) and no national DPA as a key means of enforcement. The USA is best seen as a country with a unique, largely isolated and sometimes inconsistent approach to data privacy, with some key standards weaker than is common in the rest of the world (particularly limits on collection, secondary use, disclosure and data exports). But it also often provides international innovation in relation to some principles (eg data breach disclosure, and other aspects of security) and in the deterrent effect of draconian examples of enforcement, particularly by the FTC. However, the USA does not provide an alternative paradigm for data privacy that deserves an undue amount of respect simply because of its economic and political power.

These differences are amplified by the core role it plays as the host or provider of numerous Internet-based personal information services which have global reach. The attempt to make US-based services accommodate the data privacy approaches of most other countries will continue to be one of the defining features of global privacy developments for years to come. Similarly, attempts by US companies and the US government to use their combined economic and political influence to limit development of data privacy laws in other countries will continue to be important, but may now be on the wrong side of history.

The rest of the world has to accept that there are some aspects of US domestic law on data privacy which are unlikely to change, but that does not constitute a reason for reducing international privacy standards in fundamental ways in order to accommodate or compromise with the inherent or deliberate weaknesses of American privacy protection. That would merely be capitulation.

China's direction is unknown

China is the other major power where there is little sign of a national data privacy law covering the private sector (Greenleaf, 2011a). In 2006-7, an EU-style draft *Personal Information Protection Act* was under consideration, covering both the private and public sectors, but this no longer seems to be favoured, and the Informatics Committee of the State Council considering it has been abolished. Instead, in recent years a profusion of different types of laws have been enacted. These give only partial coverage: the Seventh Amendment to the *Criminal Law* (2009) criminalised a wide range of disclosures of personal information and the obtaining of same; the PRC *Tort Liability Law* (in force 2010) includes a right to privacy (隐私权) in its list of protected 'civil rights and interests', but without defining further what is meant; data privacy provisions have been included in sectoral laws and guidelines in 2009/10 the fields of money laundering, medical records, insurance, consumer protec-

tion and credit reporting; various Provinces have also enacted local data privacy codes, particularly in consumer law; and the Ministry of Industry and Information Technology (MIIT) Standardization Administration of China (SAC) has issued draft non-enforceable 'Guidelines for Personal Information Protection' (2011). These initiatives are piecemeal and incoherent. If they are eventually replaced or supplemented by a national data privacy law, China may well influence developing countries and China's trading partners. But no-one knows the direction China will take.

2. THE INFLUENCE OF 'EUROPEAN STANDARDS'

for data privacy have been influential? How can we measure that? Can we identify the causes of influence, or only the effects?

The distinctiveness of the Directive

With a very small number of exceptions (Israel, public sector laws in some OECD countries, New Zealand) data protection laws outside Europe post-date the 1995 Directive (or at least post-date its draft form in the early 90s) and were therefore open to its influence at their inception. In some cases revised laws (eg Taiwan, South Korea, New Zealand) have added new elements influenced by the Directive.

To argue that a law outside Europe is influenced by the EU Directive of 1995, rather than by the preceding developments of the OECD Guidelines or the subsequent development of the APEC Privacy Framework, it is first necessary to identify those elements which are found in the Directive (and in some cases also in Convention 108) but are not required by the OECD Guidelines or the subsequent APEC Framework (in general, a weaker version of the OECD Guidelines: Greenleaf, 2003, 2009c). The following list of the ten most significant differences between the European instruments and the OECD/APEC instruments is not comprehensive but is indicative of the higher standards that one or both embody (informed in part by Bygrave, 2008, 19-38):

1. Requirement of an independent Data Protection Authority as the key element of an enforcement regime (EU Directive, and Additional Protocol to Convention 108);

2. Requirement of recourse to the courts to enforce data privacy rights (EU Directive, Convention 108 and more explicitly the Additional Protocol to Convention 108);

3. Requirement of restrictions on personal data exports to countries which did not have a sufficient standard of privacy protection (defined as 'adequate') (EU Directive, and Additional Protocol to Convention 108);

4. Collection must be the minimum necessary for the purpose of collection, not simply 'limited' (both EU Directive and Convention 108);

5. A general requirement of 'fair and lawful processing' (not just collection) (both EU Directive and Convention 108); where a law outside Europe adopts the terminology of 'fair processing' and a structure based on other obligations being instances of fair processing, this is both indicative of influence by the Directive, and makes it easier for the law to be interpreted in a way which is consistent with the Directive;

6. Requirements to notify, and sometimes provide 'prior checking', of particular types of processing systems (EU Directive)

7. Destruction or anonymisation of personal data after a period (both EU Directive and Convention 108);

8. Additional protections for particular categories of sensitive data (both EU Directive and Convention 108);

9. Limits on automated decision-making, and a right to know the logic of automated data processing (EU Directive);

10. Requirement to provide 'opt-out' of direct marketing uses of personal data (EU Directive).

Other 'European' elements could be added to this list, for example the right to prevent further processing, but the above choice has been made on the basis that these are the ten most important distinguishing elements. None of these ten elements is required, or even recommended, by the OECD Guidelines or APEC Framework. The as-yet incomplete APEC CBPR initiative may include some of these elements, but is irrelevant as influences are not retrospective. It is plausible to argue that non-European laws including a significant number of these ten elements are 'primarily influenced by the EU Directive'.

In order to be comprehensive, the same analysis would need to be made for the influences of each of the following (i) the elements that are distinctive to the APEC privacy framework (discussed later); (ii) the elements shared by the OECD Guidelines and the Council of Europe Convention 108 (which account for much of the similarities of all data privacy laws, but are not analysed in this article); and (iv) the elements in national privacy laws which are not found in any of these international agreements.

Influence of the 'European standards' in the 28 laws outside Europe

A systematic analysis of the effect of European privacy standards outside Europe requires the analysis of the (currently) 28 privacy laws outside Europe to determine the extent to which the ten factors above are found in those laws, and this is attempted in the following Table.

This Table only indicates correlations between the contents of a national law and the suggested 'European' elements. The question of causation, whether the provisions found in the Directive or Convention 108 either directly or indirectly caused (or more accurately, influenced) the adoption of a similar provision in a non-European law, can only be answered by detailed national studies (in the domains of legal history, politics or sociology) of the influences brought to bear in the enactment of particular legislation. An a-historical analysis such as is provided by this Table can only give rise to plausible hypotheses which invite further investigation and evidence. At best, we could argue that if the correlations are strong enough, they might give rise to a presumption that European influence is involved, rebuttable by further investigation.

In some cases, national laws are more strict than the European requirements, and this is still counted as providing the European element by going beyond it. For example, South Korea requires

consent for all data exports, with no automatic right to export data to 'adequate' jurisdictions. Korea also requires consent (ie 'opt in') for any direct marketing uses of personal data. On the other hand, just because the right words are used does not mean a provision is present: the Indian Rules refer to 'sensitive' information, but do not in fact prescribe a class of information to be given more extensive protection, so this does not count.

In some cases, provisions in laws have not yet been brought into force, but these have still been counted in this analysis. For example, Hong Kong has a data export provision not yet in force. Malaysia has not yet appointed a Privacy Commissioner under its legislation. Some assessment for the Table are matters of interpretation and opinion: for example, whether New Zealand law has the requisite type of data export provisions, or the requisite limits on automated decision-making, are matters of interpretation, but I have followed the approach taken by the Expert Report on New Zealand accepted by the Article 29 Committee.

The more correlations there are between a law and the European elements, indicated by the number (0-10) in the final column, the more it is suggestive of a conscious influence of the Directive in a particular country. For example, the score of 9 for Macau is no surprise, given that it is known to be based on the Portuguese law. The score of 9 for South Korea is perhaps more surprising, given that its law is not known to be based closely on that of any particular European country, although German law has had some influence.

The Table, and the total scores for a country, do not say anything much about whether a country's law is likely to be regarded as 'adequate' by the European Union. Adequacy assessments take into account different factors, and do not only consider the formal law, but also its implementation in practice. The question of whether a country's law makes it appropriate for that country to accede to Convention 108 is also a quite different question to which different standards apply (see discussion later). It seems to be common sense that it would be more profitable to investigate (from the perspectives of potential adequacy or potential accession) a country whose law shares nine of these European elements, rather than one whose law only shares a couple of them. However, it is quite possible that a law with a high number of 'European' elements might also have broad exemptions to its principles, and major deficiencies in its enforcement procedures, so the Table and its numerical summary also cannot be simply equated with the 'strength' of a data privacy law.

Table: Indicators of European influences on non-European data privacy laws

This table lists the 29 known data privacy laws outside Europe as at October 2011[2].

Jurisdiction	Key Act	Latest	Region	1	2	3	4	5	6	7	8	9	10	Ttl
Peru	Law on Protection of Personal Data	2011	Latin Am	√	√	√	√	√	√	√	√	√	√	10
Uruguay	Law on the Protection of Personal Data	2008	Latin Am	√	√	√	√	√	√	√	√	√	√	10
Burkina Faso	Law on Protection of Personal Information	2004	Africa	√	√	√	√	√	√	√	√	√	√	10
Senegal	Act on the Protection of Personal Data	2007	Africa	√	√	√	√	√	√	√	√	√	√	10
Morocco	Data Protection Act	2009	M.East/N. Af	√	√	√	√	√	√	√	√	√	√	10
Angola	Lei da Protecção de Dados Pessoais	2011	Africa	√	√	√	√	√	√	√	√	√	√	10
Argentina	Personal Data Protection Act	2000	Latin Am	√	√	√	√	√		√	√	√	√	9
Macau SAR	Personal Data Protection Act	2007	Asia	√	√	√	√	√	√	√	√	√		9
South Korea	Data Protection Act	2011	Asia	√	√	√	√	√	√	√	√		√	9
Mauritius	Data Protection Act	2004	Africa	√		√	√	√	√	√	√	√	√	9
Costa Rica	Protección de la Persona frente al tratamiento de sus datos personales	2011	Latin Am	√	√	√	√	√	√	√	√		√	9

Jurisdiction	Key Act	Latest	Region	1	2	3	4	5	6	7	8	9	10	Ttl
Benin	Loi sur la Protection des données personnelles	2009	Africa	√	√	√	√	√	√	√	√		√	9
Cape Verde	Loi N° 133/V/2201 du 22 janvier 2001	2001	Africa		√	√	√	√	√	√	√	√	√	9
Colombia	Data Protection Law	2008	Latin Am	√	√	√	√	√	√	√	√			8
Tunisia	Law on the protection of personal data	2004	M.East/N. Af		√	√	√	√	√	√	√		√	8
Taiwan	Personal Data Protection Act	2010	Asia		√	√	√	√		√	√		√	7
Malaysia	Personal Data Protection Act	2010	Asia	√		√		√	√	√	√		√	7
Canada	Personal Information Protection and Electronic Documents Act	2002	North Am	√	√		√	√		√	√		√	7
Hong Kong SAR	Personal Data (Privacy) Ordinance	1995	Asia	√	√	√	√		√	√			√	7
Australia	Privacy Act 1988	2001	Australasia	√		√	√			√	√		√	6
New Zealand	Privacy Act 1993	2010	Australasia	√	√	√	√			√		√		6
Kyrgyz Rep.	Law on Personal Data	2008	Central Asia		√	√		√		√	√	√		6
Mexico	Federal Law on the Protection of Personal Data Held by Private Parties	2010	Latin Am	√	√	√		√			√			5
India	s43A Rules, Information Technology Act 2000	2011	Asia		√	√	√			√				4

Jurisdiction	Key Act	Latest	Region	1	2	3	4	5	6	7	8	9	10	Ttl
Israel	Privacy Protection Act 1981	1981	M.East/N. Af	√	√	√							√	4
Bahamas	Data Protection Act	2003	Caribbean	√						√			√	3
Japan	Act on the Protection of Personal Information	2003	Asia								√			1
Chile	Privacy Law	1999	Latin Am			√								1
Vietnam	Law on Protection of Consumers' Rights	2011	Asia		√									1
Totals				22	23	25	21	20	16	24	25	13	20	

Key to numbered columns of 'European' elements:

1. Has an independent Data Protection Authority (DPA);

2. Allows recourse to the courts to enforce data privacy rights;

3. 'Border control' restrictions on personal data exports to overseas countries;

4. Collection must be the minimum necessary for declared purposes;

5. General requirement of 'fair and lawful processing';

6. Requirements to notify DPA, and provide 'prior checking' of some processing systems;

7. 'Deletion': Destruction or anonymisation of personal data after a period;

8. Additional protections for particular categories of sensitive data;

9. Limits on automated decision-making (incl. right to know logic of automated processing);

10. Requirement to provide 'opt-out' of direct marketing uses of personal data.

What we can see from the Table is that of the 29 African, Latin American, Asian, Australasian, and other jurisdictions with data privacy laws, all jurisdictions except four (Japan, Bahamas, Vietnam and Chile) have at least four of the ten 'European' elements. Nineteen of the 29 have 7 or more elements, and 13 of the 29 have at least nine of the ten elements. This last group is geographically diverse, including Peru, Burkina Faso, Argentina, Macau, Morocco, Angola, South Korea and Mauritius. I suggest this leads to quite a strong inference that European privacy standards have been, either directly or indirectly, influential in all of these Latin American, Asian, African and Australasian

countries except the four with 3 or fewer where the influences are minor. The influences are modest (a score of 4) in Israel (a 1981 law that pre-dates the Directive and is a contemporary of the Convention) and India (a set of rules inserted into another Act).

All the ten 'European' elements of data privacy laws identified above are found in at least 13 data privacy laws outside Europe: the least common features are limits on automated decision-making (13/29) and requirements for prior checking of some systems (16/29). Some are commonplace, for example specialist data protection agencies (22/29); 'border-control' data export restrictions (25/29); additional protection for sensitive data (25/29); deletion requirements (24/29). Some elements also appear in unexpected places (eg 'fair and lawful processing' in Malaysia). The average number of times each feature appears is 20.9/29 instances, so on average each 'European' feature is present in over two thirds (almost three-quarters) of all non-European data privacy laws.

Of course, it is logically possible (although quite implausible) that these 'European' elements have been independently invented, time and again, in non-European states. More realistically, Raab (2010) explains some of the likely patterns of influence in his study of the complex interactions between European data protection authorities and policy-makers in non-European countries with similar linguistic backgrounds, such as the Ibero-American Data Protection Network (RedIPD) and the Association of Francophone Data Protection Authorities (AFAPDP). There is also a lusaphone network. Only fully detailed studies of the history of data privacy laws in particular countries, such as the country studies in Rule and Greenleaf (2008) can properly answer questions about influences. In three countries examined there, outside the networks considered by Raab, Australian and Hong Kong laws showed evidence of influence by the EU Directive. The study of the then Korean law did not (though factors such as data export restrictions were present), but the 2011 revised Korean law shows stronger EU influence (Greenleaf, 2011a). Bennett and Raab's analysis of the emergence of data privacy laws up to 2005 (2006, Ch 5) also sees significant influence of the Directive both in Europe outside the EU and in non-European laws, but not to the extent identified here.

On the basis of what is shown in this Table, which is consistent with expert but impressionistic knowledge of the contents of these laws, we can say that outside Europe, something reasonably described as 'European standard' data privacy laws are becoming the norm in most parts of the world with data privacy laws. This trend is most noticeable in Latin America, with Costa Rica recently joining Argentina, Colombia and Uruguay with EU-style laws, and Mexico with a law with both EU and OECD influences. All the recent laws in West and North Africa show strong EU influence. In the last two years, revised laws in Taiwan and South Korea have moved further in the EU direction, as have new laws in India and Malaysia (while also showing influences of the OECD Guidelines). Macau's law is derived directly from the Portuguese law. Japan, Hong Kong, New Zealand (likely to soon be the second Asia-Pacific country after Canada found to be 'adequate') and Australia (where protracted law reform processes should strengthen its law) all have laws which show EU influences to some degree. Nowhere in the new Asia-Pacific laws is there any strong evidence of APEC influence, even Vietnam where the influence is more clearly from the OECD than from APEC (see later, and generally Greenleaf, 2011a and articles cited therein for evidence for specific countries).

Although more evidence of causation is desirable, it is an entirely plausible (and in my view, correct) hypothesis that the EU Directive is the most significant overall influence on the content of data privacy laws outside Europe, and that its influence is gradually strengthening, partly because of the desired of non-EU countries to have their laws recognised as 'adequate', but also because

of the their aspiration that their laws should be recognised as providing the highest international standard of privacy protection.

The adequacy mechanism and 'border control'

The 'adequacy' mechanism in the Directive, and perceptions of it outside Europe, have been one (but only one) of the means by which the influence of European standards has been felt. The EU's 'border control' approach is to require member states to limit data exports unless 'adequate protection' can be demonstrated at the receiving end (EU Directive Articles 25, 26). In summary '[t]he effect of a Commission adequacy finding is that personal data can freely flow from the 27 EU Member States and the three EEA member countries to that third country without any further safeguard being necessary. However, the exact requirements for recognition of adequacy by the Commission are currently not specified in satisfactory detail in the Data Protection Directive' (EU Commission, 2010, 2.4.1). There is a further problem that different EU Member States make different judgments on adequacy.

As yet, the EU has only made 'adequacy' decisions in relation to nine jurisdictions as a whole (Andorra, Argentina, Canada, Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, and Jersey), some of which are of little economic or political significance. Uruguay and New Zealand will soon be added to this list, following positive findings by the increasingly pragmatic Article 29 Working Party (Greenleaf and Bygrave 2011). It is arguable that Colombia, Mexico and Peru also have adequate laws (Palazzi, 2011). South Korea and India could each put forward a case after their 2011 reforms, as could Taiwan (with more difficulty), and Hong Kong and Australia might do so after their legislatures complete their reform processes (see generally Greenleaf, 2011a). The new laws in Africa resemble the EU Directive in their principles, so arguments for adequacy would hinge largely on issues of effective enforcement. For European countries that have acceded to both Convention 108 and the Additional Protocol, an adequacy finding is not needed.

There could be significantly more adequacy findings outside Europe if the EU was more pro-active and more transparent about its processes. Where the EU has made positive adequacy decisions it has publicised the reasons, but where it has considered 'applications' from other countries but concluded that their protections were not yet adequate, it has not generally publicised the reasons for these negative conclusions. There has therefore been much less information available about what does and does not constitute 'adequacy' than is desirable. Individual European countries do not seem to have blocked particular data exports very frequently since the Directive has been in force, thus reducing the impact of the adequacy requirement. However, whether these has been less blocking of data exports than occurred during the 1980s and early 1990s (when there seemed to be quite a lot) needs empirical verification. There has also been considerable criticism of whether EU countries live up to their own standards, including assertions of considerable inconsistency and non-enforcement by EU members in relation to the data export provisions (Bygrave 2010, p 197).

Despite the slow pace of the EU in making and publicising assessments, the desire to eventually obtain an 'adequacy' finding from the EU, or in a more amorphous form, to have one's law regarded as of the highest international standard (that the EU Directive is considered by many to embody) has been a significant influence on the development of laws outside Europe (as discussed above).

Outside Europe, 'border control' data export limitations are found almost all (25/29) data privacy laws in all regions, though their strength varies a great deal, and they are not yet in force in the laws of Malaysia and Hong Kong. So anyone who wishes to criticise the EU for wanting to 'impose its standards on the rest of the world' had better level the same accusation at the rest of the world.

The strengthening Directive (and the Convention)

Fifteen years after 1995, the EU's promotion of its standards is growing stronger, although it is not without critics. After reviewing the EU's current data privacy legal framework through conferences, consultations and commissioned reports (including Korff and Brown, 2010), the EU Commission has concluded that 'the core principles of the Directive are still valid and that its technologically neutral character should be preserved', although it should be strengthened in various ways (EU Commission, 2010, 1), as discussed in Greenleaf (2011). The European Commission is intent on expanding the global influence of its standards, and in fact seems to see them as 'universal principles' (EU Commission, 2011, 2.4.2):

Data processing is globalised and calls for the development of universal principles for the protection of individuals with regard to the processing of personal data. The EU legal framework for data privacy has often served as a benchmark for third countries when regulating data privacy. Its effect and impact, within and outside the Union, have been of the utmost importance. The European Union must therefore remain a driving force behind the development and promotion of international legal and technical standards for the protection of personal data, based on relevant EU and other European instruments on data privacy.

Furthermore, it is intent on strengthening both the Principles and the enforcement mechanisms of EU data privacy (EU Commission, 2010). 'The Lisbon Treaty provided the EU with additional means to achieve this: the EU Charter of Fundamental Rights - with Article 8 recognising an autonomous right to the protection of personal data - has become legally binding, and a new legal basis has been introduced allowing for the establishment of comprehensive and coherent Union legislation …'. The aim is to ensure 'that the fundamental right to data protection for individuals is fully respected within the EU and beyond' (EU Commission, 2010, 1). The final two words indicate the significance for the rest of the world.

Outside Europe, some of the emergent international data privacy norms that the Commission is considering (such as data breach notification, the 'right to be forgotten' and 'data portability'), and other innovations, have already started to be incorporated in laws or legislative proposals. The USA has to some extent led the way with the development of data breach notification rights, but these are also now incorporated in the data privacy laws of Taiwan and South Korea (Greenleaf, 2011a, 2011e), and in proposed legislation in Australia (Greenleaf and Waters, 2010). South Korea also has an explicit 'no disadvantage in case of refusal' rule, requiring provision of services, with no extra costs, where data privacy rights are exercised. Australia has since 2001 had a specific principle requiring the option of anonymous transactions wherever this is feasible, whereas the EU's proposals for stronger data minimisation are not this explicit. Genetic data is already explicitly protected in India's new law. These examples are only from the Asia-Pacific, but similar ones may well be found in Latin America and Africa. Because of innovations like these at the national level in APEC economies, the EU Commission's proposals are unlikely to increase divergence in data privacy standards around the world in the long term. If they widen the gap between EU and APEC principles, that will only make APEC more irrelevant.

3. INTERNATIONAL AGREEMENTS OUTSIDE EUROPE

Some international data privacy agreements outside Europe will be significant, but probably not the one that usually comes to mind.

APEC's over-rated Framework and inchoate CBPR

From the start of its development in 2003 the APEC (Asia-Pacific Economic Cooperation) Privacy Framework (APEC 2005) has been the only significant international attempt to break the influence of the EU Directive. APEC has 21 member 'economies' in Asia (including China but not India, and overlapping the Council of Europe by inclusion of Russia), the Americas (including the USA) and Australasia. Through its Framework, which is not legally binding, APEC advocated an alternative approach which falls short of the 'European' standards set primarily by the EU Directive in four respects: (i) its set of principles can be described as 'OECD Lite' (Greenleaf, 2004), weaker than the Directive or most regional laws, and with no additions of value (Greenleaf 2008); (ii) a complete absence of any obligations to enforce the principles by law (self-regulation unsupported by legislation is acceptable for APEC), or even a recommendation for legislation; (iii) no complementary obligation of free flow of personal data in return for adoption of basic standards (at best, an encouragement of development of mutually-acceptable cross-border privacy rules (CBPR) by companies); and (iv) an 'Accountability' principle which is an incoherent substitute for data export limits (see later). However, the APEC processes have stimulated regular discussion of data privacy issues between governments in the region, and more systematic cooperation between DPAs in the region on cross-border enforcement.

The APEC Privacy Principles (Part III of the Framework) contain three Principles which it can be argued are not explicitly found in the two European instruments: 'Preventing Harm' (Principle I); 'Choice' (Principle V); and 'Accountability' concerning data exports (Principle IX). While it can be argued that these are not valuable additions to sets of privacy principles (Greenleaf, 2008), the separate question relevant to this paper (and as asked above about the 'European' principles) is whether these three 'APEC Principles' have had any influence on the development of national privacy laws, particularly those outside Europe. The short answer is that their influence appears to be minimal. New Zealand had a provision (not a Principle) which could be recognised as 'preventing harm' before the APEC Framework existed, and Canada had an 'accountability' principle relevant to data exports. Vietnam has none of the 'APEC trio', although otherwise it joins Japan as the least 'European' of Asian laws. There are possible future influences coming from law reform reports and Bills ('accountability' in Australia or New Zealand) but these might not become legislation. The Mexican law does include a version of the APEC 'accountability' principle. The 'choice' principle is not explicitly included in any national data protection principles, and it is difficult to assess whether it is impliedly and diffusely implemented anywhere. Perhaps other examples can be found, but it seems clear that, compared with the widespread influence of the distinctive aspects of the 'European' principles, the distinctive APEC principles have gained little traction.

The APEC approach was initially enthusiastically supported by at least the USA, Australia, Canada and Mexico, and acquiesced in by other countries. However it has failed to establish an alternative paradigm for data protection: almost no evidence of adoption of its principles in legislation in the region; little increase in self-regulatory initiatives (there are privacy seals in Mexico, Vietnam and Japan, but they are of questionable value); and a faltering CBPR initiative (Greenleaf, 2008; Waters,

2008, 2011, 2011a). New laws in the region are influenced more by the EU Directive than by the APEC Framework, as discussed previously.

APEC's attempt at establishing a regional form of cross-border privacy rules (CBPR) with national endorsement seems to be on the verge of collapse, crippled by the lack of enforcement mechanisms in some jurisdictions, the opposite problem of stricter legal requirements in others, and a general decline in interest in involvement by most APEC economies (Waters, 2008, 2011). Attempts are still being made at APEC meetings to finalise governance of the whole scheme. However, it is necessary to distinguish the APEC CBPR initiative for a number of reasons: (i) it does include elements not found in the APEC Framework (eg a requirement that CBPR be underpinned by local legislation); and (ii) it is possible that it could have some future effectiveness. However, those factors are not directly relevant to the argument in this paper, which is primarily about what has influenced non-European laws up until now: influences cannot be retrospective.

Even the best global analyses of data privacy developments still tend to accord too much significance to the APEC Framework as a brake on European influence (eg Bennett & Raab, 2006; Bygrave, 2008, 2010). It is more likely that APEC will be seen as a dead-end: why pay attention to non-binding guidelines that no-one follows and (probably) CBPR rules that have almost no implementation?

While this paper emphasises the points of difference or distinction between the 'European' and 'non-European' (OECD and APEC) international agreements, and takes the view that those differences are very significant in substance (Greenleaf 2008) and that Europe should not 'trade down' in order to achieve some global consensus, other commentators argue that the differences are much less significant in substance (Waters, 2008) and therefore tend to be more optimistic about a possible global consensus. It is beyond the scope of this paper to reconsider all of those arguments. However, what is unarguable is that there is a great deal of common ground between the European and non-European principles, and this commonality helps to explain the remarkable overall consistency of the world's 76 national data privacy laws (and many sub-national laws as well).

The ECOWAS data protection Act

The Economic Community of West African States (ECOWAS), a grouping of fifteen states under the Revised Treaty of the ECOWAS, agreed to adopt data privacy laws in 2008, and then adopted a *Supplementary Act on Personal Data Protection within ECOWAS* (ECOWAS, 2010). This supplement to the Treaty specifies the required content of such data privacy laws, influenced very strongly by the EU Directive, and that each state must establish a data protection authority. As noted earlier, four ECOWAS states have enacted such laws (Benin, Burkina Faso, Cape Verde, and Senegal), and a Bill is before Parliament in Ghana.

Other regional agreements on data privacy

ASEAN (the Association of South East Asian Nations) has a much weaker agreement among its eleven members to increase their data privacy protection by 2015 (Connolly, 2008; Munir and Yasin, 2010), but three have legislation in progress (Thailand, the Philippines and Singapore), and one has legislated (Malaysia). In Latin America the four Mercosur countries have agreed to establish Guidelines, but they are not completed (Palazzi, 2011). The prospects for a 'regional bloc' of consistent data protection laws, similar to what has occurred in Europe, seem strongest in West Africa. It is

possible, though less immediately likely, that such developments could also take place in other African sub-regions, South-East Asia or Latin America, although not in the Asia-Pacific as a whole or the APEC sub-set of countries.

4. COE CONVENTION 108 AND ADDITIONAL PROTOCOL: A GLOBAL AGREEMENT?

Council of Europe (CoE) Convention108 (the *Convention for the protection of individuals with regard to automatic processing of personal data*) Articles 5-8 are a set of data privacy principles that, while stated briefly, do contain versions of most of the elements we now recognised as core data privacy principles. Many of the principles are similar to those found in the OECD Guidelines due to cross-influences between the drafters of the two instruments. However, the Convention contains few of the enforcement mechanisms now regarded as essential.

The 2001 Additional Protocol (ETS 181) to the Convention adds a commitment to data export restrictions, to an independent data protection authority, and to a right of appeal to the courts, and therefore brings the standards of the Convention approximately up to the same level as the Directive (thus showing how the Directive has also influenced other international instruments: Bygrave, 2010).

Forty-three CoE member States have ratified the Convention, and have data privacy laws (see the Table in Greenleaf, 2011 or the CoE accessions page). Armenia, Turkey and the Russian Federation have signed but not ratified the Convention. San Marino has done neither. However, Russia does now have a data privacy law (in force 2011). Armenia, Georgia and Turkey are the only Council of Europe Member State not to have enacted a data privacy law. Belarus is not a Council of Europe member because of human rights concerns, and the Vatican (Holy See) is not a member because it is not a democracy. The UK and other countries have acceded to the Convention on behalf of their self-governing territories.

Thirty-one European countries have also ratified the Additional Protocol (see the Table in Greenleaf, 2011 or the CoE accessions page). Twelve countries that have ratified the Convention (plus three territories on whose behalf the UK acceded to the Convention) have not ratified the Additional Protocol, but in almost all cases that does not matter because they are EU member states, or their laws have been found 'adequate' by the EU, and they have already have the same obligations as the Additional Protocol would impose.

Accession by non-CoE countries to Convention 108

Article 23(1) has provided for accession by non-member States since 1981:' … the Committee of Ministers of the Council of Europe may invite any State not a member of the Council of Europe to accede to this convention by a decision taken by the majority provided for in Article 20.d of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the committee'. However, the Committee of Ministers had not invited a State to accede for the first quarter-century of the Convention's life.

The world's privacy and data protection Commissioners at their 27th International Conference in Montreux, Switzerland (2005) gave this aspect of Convention 108 a wake-up call when they agreed on a concluding 'Montreux Declaration' which issued a number of challenges to global

organizations and national governments. One was their appeal 'to the Council of Europe to invite, in accordance with article 23 [of Convention 108 on data protection] … non-member-states of the Council of Europe which already have a [sic] data protection legislation to accede to this Convention and its additional Protocol.' Article 23 had lain dormant while the CoE concentrated on obtaining accessions to Convention 108 from all of the European members of the CoE. The Secretary General took note of the Declaration and expressed his willingness to promote the Convention internationally.

In March 2008 the Consultative Committee of the Convention (T-PD) at its 24th annual meeting, considered accession of non-Member States under Article 23. According to its minutes (CoE 2008):

> 53. Lastly, the representative of Switzerland recalled the final declaration of the Montreux Conference of Privacy Commissioners in 2005, which had called the Council of Europe to "invite, in accordance with article 23 of the Convention for the protection of individuals with regard to automatic processing of personal data, non-member states of the Council of Europe which already have data protection legislation to accede to this Convention and its additional Protocol". He considered that now would be a good time for the Council of Europe to issue such an invitation, as these accessions could be a step towards a much called-for universal right to data protection which is becoming all the more important in today's world of borderless telecommunication networks. They would also contribute to reinforce the Council of Europe's visibility in this area.
>
> 54. The T-PD agreed and therefore recommended that non-member states, with data protection legislation in accordance with Convention 108, should be allowed to accede to the Convention. It invited the Committee of Ministers to take note of this recommendation and to consider any subsequent accession request accordingly.

The Committee of Ministers at its 1031st meeting on 2 July 2008 (CoE 2008a), meeting at Deputy level, made the following Decisions:

> 1. took note of the T-PD's recommendation that non-member states with data protection legislation in accordance with the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) should be allowed to accede to this convention;
>
> 2. agreed to examine any accession request in the light of this recommendation;
>
> 3. instructed the Secretariat to disseminate information about the convention;
>
> 4. took note of the abridged report of the 24th plenary meeting of the T-PD as a whole, as it appears in document CM(2008)81.

From mid-2008, non-European accession to the Convention therefore became possible as a matter of practicality. However, '[t]he Council of Europe never really promoted the Convention outside Europe. It was only in December 2009 that the EU's Stockholm Programme explicitly called for the promotion of Convention 108 worldwide' (Polakiewicz 2011). This promotion is now underway. Uruguay 'may become a party later this year' (Polakiewicz 2011).

The CoE is actively involved in discussions with other states, some of which have indicated informally their interest in acceding. But whether the CoE is likely to succeed in turning Convention 108 into a global convention is still an open question, on which this article is intended to shed some light.

Global conventions originating from Europe are not unprecedented, and some other Council of Europe Conventions are open to ratification by non-Member State. For example, the *Cybercrime Convention* has been ratified by the USA, and signed by three other non-European states (South Africa, Japan and Canada). Accession is now being promoted vigorously by the CoE and other parties, and countries like Australia have passed legislation to enable accession.

The standards required by Convention 108, and 'modernisation'

How high is the standard of data privacy that non-European states must meet in order to accede to the Convention and the Additional Protocol (both are required, as discussed below). It is necessary to consider both data protection principles and how they are enforced. The Convention applies to automated processing of personal data, but parties may extend its application to other categories of data. The Convention was amended in 1999 (Council of Europe, 1999) to allow the European Communities to accede.

First, concerning principles, Articles 5-8 of Chapter II set out Convention 108's data protection principles in what Bygrave (2008) rightly describes as 'broad brush fashion'. Most of the work is done by Article 5 (Quality of data) which requires that:

> Personal data undergoing automatic processing shall be: 1. obtained and processed fairly and lawfully; 2. stored for specified and legitimate purposes and not used in a way incompatible with those purposes; 3. adequate, relevant and not excessive in relation to the purposes for which they are stored; 4. accurate and, where necessary, kept up to date; 5. preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.

Other than that, all that Chapter II includes are familiar principles requiring 'appropriate' data security (Article 7), and rights to ascertain the existence of personal files, to access them, and to correct them (Article 8). There is also a provision for 'sensitive' data in Article 6: 'Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life [or criminal convictions], may not be processed automatically unless domestic law provides appropriate safeguards.' The Convention applies to both public sector and private sector organisations. Application to non-automated data is optional.

These are not very high standards for a data protection law to meet. Even so, the ease of compliance is increased by Article 9 which allows derogation from these principles (except the security principle) where

> such derogation is provided for by the law of the Party and constitutes a necessary measure in a democratic society in the interests of: a. protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences; b. protecting the data subject or the rights and freedoms of others.

As Bygrave notes 'these principles were hardly ground-breaking at the time of the Convention's adoption' over 25 years ago. They are even more modest today. Nevertheless, they are a basic set of data privacy principles. The OECD Guidelines are similar but even they are stronger on some points (eg provision of notice; application to non-automated files).

'European standards' also requires accession to the Additional Protocol

The Convention neither prevents nor requires data export restrictions to States which are not parties to the Convention and do not have similar data privacy laws, but does allow them under some circumstances (as do the OECD Guidelines). Convention 108 only requires in Article 12 that its parties 'shall not, for the sole purpose of the protection of privacy, prohibit or subject to special authorisation transborder flows of personal data going to the territory of another Party'. In other words, it guarantees free flow of personal data between parties to the Convention because they have adopted a minimum required standard of data protection. Article 12 also allows restrictions on data exports to other parties in limited circumstances (concerning (a) specific classes of data where the other party does not provide equivalent protection, and (b) where necessary to avoid transfers resulting in onward transfers via a party to a non-party with no similar data protection laws). However, the party wishing to so limit data exports to another party must lodge a derogation to that effect.

The Additional Protocol to Convention 108 in 2001 altered this situation and makes provision for data export restrictions mandatory. Once a party to the Convention also becomes a party to that Protocol, it is required to 'provide for the transfer of personal data to a recipient that is subject to the jurisdiction of a State or organisation *that is not Party to the Convention* only if that State or organisation ensures an adequate level of protection for the intended data transfer' (Article 2 – italics added). The main effect of this provision is that it makes Convention 108 more closely aligned with the EU Directive by adding a data export restriction in similar terms ('adequate protection'), though expressed in simpler terms. However, by the italicised words, this data export limitation requirement does not apply to transfers to other parties to Convention 108. If they are a party to the Convention, then that is the end of the matter as far as the Convention is concerned (though it might not be the end of the matter for countries bound by the Directive). It is therefore important that the standards for accession be kept high: otherwise parties to the Convention will be forced to allow exports of personal data to countries with low privacy standards.

There are further reasons why it is essential that countries only be allowed to accede to Convention 108 if they also agree to accede to the Additional Protocol. At least in theory it is not necessary for a non-European country to have a data export restriction provision in its law in order to accede to Convention 108. This only becomes necessary if the non-European country wishes to accede to the Additional Protocol. This may have important implications, because it means that those non-European countries without data export restriction provisions would still obtain the benefit of free flow of personal data from any countries that had also acceded to the Additional Protocol, unless each of those countries lodged a derogation in relation to it under Article 12(3)(b). In other words, data export restrictions are not required as part of the meaning of 'adequate level of protection' under Convention 108, even if they are required as part of the Directive's notion of adequacy.

Concerning enforcement standards, Convention 108 is vague about the sanctions and remedies that the laws of State parties must provide to enforce these principles. It only provides that 'Each

Party undertakes to establish appropriate sanctions and remedies for violations of provisions of domestic law giving effect to the basic principles for data protection set out in this chapter' (Article 10). It does add that a person must 'have a remedy' of access or correction rights under Article 8, but that does not add anything to Article 10. In short, Convention 108 by itself does not say anything about whether individuals must have a right of individual action to enforce rights, or access to the Courts. It is consistent with it that all enforcement of data protection laws could be by criminal sanctions or administrative remedies. There is no right provided by the Convention of individual complaint against a State party to any Court or other body, so there is no effective method in the Convention itself by which individuals can test whether a party's implementation of the principles are sufficient, or its enforcement methods are 'appropriate' (as required by the Convention). Recourse to the European Court of Human Rights is a separate remedy, but one only available to Europeans.

The Additional Protocol to the Convention also deals with this deficiency by requiring that parties to it 'shall provide for one or more authorities to be responsible for ensuring compliance' in its domestic law, and sets out requirements of independence, ability to investigate complaints, to 'hear claims', and to bring matters before a Court or to its attention (Article 1). It also requires that the decisions of supervisory authorities 'may be appealed against through the courts'. It does not require a single data protection authority. These standards would be met by many data protection laws outside Europe, though (for example) Australia's federal data protection law would currently fall short of this last requirement, as there is no general right of appeal against decisions of the Privacy Commissioner.

From this brief discussion, it should be clear that, taken together, Convention 108 and the Additional Protocol provide a set of standards roughly equivalent to those found in the Directive, and called in this article 'European standards', but Convention 108 by itself does not any longer count as 'European standards'. This is particularly important in relation to the data export requirements. The Council of Europe is at present undertaking a process to 'modernise' the Convention. If this 'modernisation' were to significantly weaken the standards currently found in the Convention plus Additional Protocol, then this would undermine, and probably make void, most of the arguments presented in the following parts of this article concerning the benefits of non-European accession.

Problems with the procedures and standards for accession

The procedures for accession by non-member states to Convention 108 have not been well-publicised, and even now do not cover all important issues. A September 2011 'Note of Information' on the topic by the Treaty Office of the Council Secretariat (CoE 2011), updating earlier publications, can be paraphrased as follows:

1) In principle, the Committee of Ministers may take the initiative of inviting a non-member State to accede to a Convention, but it is customary for the non-member State to request accession in a letter (from their foreign minister) addressed to the Secretary General of the CoE.

2) Before putting the matter on the Committee agenda, the Secretariat usually informally ascertains opinion among member States' delegations. For Convention 108, unanimous

agreement of all 43 member states who have ratified the Convention (as yet) is required. Formal requests for accession are examined by the Committee or by one of its rapporteur groups.

3) Once there is an agreement in principle within the Committee to give a positive reply to a request, it instructs the Secretariat to consult the other non-member States which are Parties to the Convention (none as yet), giving them a time-limit for the formulation of objections, usually two months.

4) In the absence of objections, the decision to invite the non-member State is (usually) taken at the level of the Ministers' Deputies. The Secretariat General then notifies the State concerned of the invitation to accede to the Convention.

5) Prior to acceding to Convention 108, the State invited has to take the 'necessary measures' to ensure that its domestic law allows the Convention to be implemented ('to give effect to the basic principles for data protection set out in this chapter').

6) The instrument of accession is to be deposited with the CoE in Strasbourg, or delivered by diplomatic courier. The Convention enters into force in relation to the State after three months on the first of the next month.

7) States are also 'asked' to accept the 1999 Amendments to Convention 108 which allowed the European Union to accede to the Convention, as those amendments require unanimous agreement.

8) Convention 108 has a consultative committee of experts (T-PD) which monitors its application by the States Parties.

While this Note is helpful, it does not address the following five major issues still to be resolved in relation to non-European accessions. All of these must be resolved before the implications of accession for non-European states, and for better global protection of privacy, are clear.

First, the Committee of Ministers needs to determine (or clarify in a public document) that there cannot be non-European accessions except to both the Convention and Additional Protocol, and not to just the Convention alone. The main disadvantage to non-European countries could be that, if the Committee of Ministers allows countries outside the EU to accede to the Convention with laws of low standard, or without acceding to the Additional Protocol as well, this could result in an obligation (at least on non-EU countries) to allow data exports to countries with sub-standard laws. Allowing accession to the Convention alone will drastically undermine European privacy standards, and is likely to create untenable inconsistencies between the Convention and the Directive. Georges (2011, para 83) refers to 'the Committee of Ministers' decision of 2 July 2008 to encourage (non-Member) States having an adequate standard to accede to Convention 108 and its Additional Protocol', and also assumes in further recommendations to the Consultative Committee that the Convention and the Additional Protocol should be treated as a package. The CoE Secretariat has also advised (personal communication, 5 October 2011) that a requirement to accede to both instruments reflects the Consultative Committee and Secretariat position. It would be important to reflect this key decision in the above Note and in a consolidated publication stat-

ing all of these policy decisions. It appears therefore that this key policy position has been resolved correctly, but it still needs to be stated explicitly in explanatory documents.

Second, the Committee needs to determine the standard by which an assessment is made of whether a country meets the standards for accession to the Convention (and Additional Protocol). The standards for accession are not specified in Article 23, but Article 4 requires that '[e]ach Party shall take the necessary measures in its domestic law to give effect to the basic principles for data protection set out in [Chapter II of Convention 108]', by the time of ratification. The 'Note of Information' discussed above does not elaborate on what this standard means. It cannot be a merely formal assessment of what a country's law says on paper. Otherwise, countries like Angola or Malaysia which have laws including a DPA, but have not yet appointed one, would appear to be compliant when in fact they are not. Similarly, India has on paper an apparently strong credit reporting law in force, but it has never been implemented or observed by anyone, including the regulator or the credit bureaus. Because of its previous focus on European accessions, the Convention 108 Consultative Committee has up until now been dealing with 'normal countries': democracies in Europe, and all of them within the jurisdiction of the European Court of Human Rights (ECHR). But some of the countries with data privacy laws outside Europe are not 'normal countries', and none of them are within the ECHR's jurisdiction. So the Consultative Committee must exercise extra vigilance to ensure that 'laws on the books' are not merely shams. The EU's approach requiring assessment that a law actually delivers 'a good level of compliance', 'support and help' and 'appropriate redress' must be something close to what should also required for a CoE assessment of what is required for accession.

The standard to the applied should not be exactly the same as that which the EU Commission would apply in determining whether a non-European country's law was 'adequate', but it should be similar in most respects. The key difference is that the Council of Europe should be primarily concerned with how strong is the protection of non-European law from the perspective of the citizens of that country. No particular weight being given to the interests of Europeans, if it is intended that Convention 108 is to become a neutral, global convention. However, when adequacy assessments are made, the Article 29 Committee quite correctly allows more flexibility in the application of the Directive's standards concerning aspects of a country's law which are not likely to have any significant influence on the protection of European data subjects (Greenleaf and Bygrave, 2011).

While the standards of the Directive and the Convention should be slightly different, it remains to be seen in practice if Convention 108 accession becomes something of a 'short cut' to an EU adequacy finding for non-European countries because it is an 'international commitment' that a non-European country has entered and therefore relevant under Article 25 of the Directive. The process might also work in reverse, with the Council of Europe taking into account and giving appropriate weight to a prior adequacy finding for a country (and the WP 29 Opinion on which it is based) when considering requests by non-European states to accede to the Convention and Additional Protocol. But while 'fast tracking' of countries that have prior adequacy assessments might be reasonable (Michael, 2008), it should not be automatic. As a practical matter, it would be desirable if the European Commission and the Council of Europe could find a cooperative mechanism by which they could take each other's findings into account in order to expedite their own. It also remains to be seen whether non-European countries will be satisfied to obtain one or other of an adequacy finding or Convention 108 accession, or whether they will want both.

Third, there needs to be clarification of the procedure which is to be followed by the Council of Europe bodies in making such an assessment, and which parties will be involved. Georges (2011) has proposed to the Consultative Committee detailed procedures by which applications for accession could be assessed, including a major choice of modalities between a 'peer assessment' by representatives of existing member states, or a 'committee of independent experts' with requirements of expertise and independence. However, her recommendations do not fully deal with the question of what 'to give effect to the basic principles' should mean (question 2 above). She does recommend that the Consultative Convention Committee be empowered to give an opinion on conformity when instruments of ratification are deposited or when accession requests are examined by the Committee of Ministers. This would mean it would play a role similar to the Article 29 Working Party under the Directive.

Fourth, and most difficult, is the problem that there is a lack of mechanisms for citizens of countries outside Europe to enforce the Convention, including their inability to take cases to the European Court of Human Rights because the European Convention on Human Rights is a closed convention to which non-European states cannot accede (Michael, 2008; Polakiewicz 2011). Perhaps the UN human rights mechanisms for individual 'communications' under ICCPR Article 17 could play a role in relation to non-European countries that are parties to Convention 108 and also to the Optional Protocol under the ICCPR. But that could only apply to some countries. Perhaps the Consultative Committee could be empowered to accept 'communications' from individuals, civil society organisations, or businesses who wish to complain that a party to the Convention is not observing its terms. This would not be comparable to taking a case to the ECHR, but better than nothing. Otherwise, all the Consultative Committee or the Council of Ministers can do is resort to persuasion or public criticism of recalcitrant countries. The answers are not obvious, but they need to be addressed if Convention 108 is to become genuinely global and to give individuals outside Europe genuine means of redress. Otherwise it will remain too biased in favour of the interests of Europeans to be genuinely global. Perhaps the current review of the Convention could take up this issue.

Fifth, there needs to be some procedure to test whether a member state does adhere to its commitments over time, and some sanctions which can be triggered if it does not (somewhat similar to an adequacy assessment being revoked). Georges (2011, para 98) proposes establishment of a periodic review mechanism such as is found in areas like anti-corruption. It is possible that post-ratification assessment of compliance could be dealt with without need for an amendment to the Convention, by such means as a Committee of Ministers' resolution (a separate legal instrument), which non-member states would have to accept upon accession. The current Convention 'modernisation' process, endorsed by the CoE Ministers of Justice in November 2010, has as one of its aims to strengthen the Convention's follow-up mechanism (Polakiewicz 2011), and the interests of non-European states and their citizens need to be kept firmly in mind as part of this process.

All of these issues need to be addressed by the Council's Secretariat in a comprehensive document concerning accession by non-member states if they are to obtain understanding of, and support for, the advantages of accession by the states concerned, and by business and civil society organisations.

The Parliamentary Assembly of the Council of Europe has recently (October 2011) made similar Recommendations to some of the above points: that reform 'should not lower the established protection'; that the Parties should 'establish a mechanism for monitoring compliance'; and that

the CoE should encourage ratifications by non-member States (CoE Parliamentary Assembly Recommendation 1984, 2011). The accompanying Resolution makes it clear that 'any global initiative should be based on Convention No 108 and its Additional Protocol', and not on the Convention alone (CoE Parliamentary Assembly Resolution, 1843, 2011, para 11).

The first example of non-European accession: Uruguay

At its 1118th meeting on 6 July 2011 the Committee of Ministers under Convention 108 decided to invite Uruguay to accede to the Convention, on the basis of an Opinion provided to it by the Convention's Consultative Committee, and it is expected it will do so by the end of 2011. The process that led to this decision sheds light on the first three issues discussed above.

The Opinion of the Consultative Committee (CoE TP-D 2011) explains that in this case the delegations of the 43 members of the Consultative Committee (the current parties to the Convention) were provided with Uruguay's letter requesting accession, its legislation, and the Opinion of the EU's Article 29 Working Party in relation to Uruguay's request for a finding of 'adequacy' of its law by the EU, which Opinion had been published in 2010 (EU WP29 2010). Fourteen of the 43 delegations replied positively to confirm that in their view Uruguay had taken the necessary measures in its domestic law to give effect to the basic data protection principles of Convention 108 (Bosnia and Herzegovina, Cyprus, the Czech Republic, Estonia, Finland, Hungary, Italy, Latvia, "the former Yugoslav Republic of Macedonia", Monaco, Slovenia, Sweden, Switzerland and the United Kingdom). No delegation objected. The Consultative Committee then adopted its Opinion supporting accession through written procedure.

The Consultative Committee's Opinion takes only two pages to detail that Uruguay's legislation does contain provisions which (on paper) cover all the elements to give effect to the basic data protection principles of Convention 108, but does not directly provide any information to demonstrate that these provisions have any effect in reality or deliver meaningful privacy protection to Uruguayan citizens. However, the Opinion stresses ('wishes to underline') the EU WP29 Opinion that found Uruguay's law adequate. That WP 29 Opinion contains 20 pages of detailed analysis of Uruguay's law and how it satisfies the EU's requirements, and is based on a much longer expert report obtained by the European Commission and further interaction between the Commission and the Uruguayan government. In particular, concerning the reality of enforcement, the WP29 Opinion says:

> "Furthermore, the LPDP [the Uruguayan law], as shown below, includes specific regulations in relation to investigation, inspection and sanctions, and the DPDP establishes specific regulations for certain procedures to be brought before the URCDP [the Uruguayan DPA] and, particularly, for registering processing and authorising international data transfers.
>
> The Working Party wishes to state that evidence has been provided by the URCDP of performance of these powers in a range of information provided during the analysis of data protection adequacy detailed in this document."

A reading of the WP29 Opinion leaves little doubt that, as a matter of reality and not merely of legislative form, Uruguay's data protection system meets the requirements of Convention 108 and the Additional Protocol. Therefore, although the Consultative Committee Opinion could not in

itself be seen to give much reassurance that Uruguay had an effective system of data protection, when taken together with the WP29 Opinion, as was possible in this case, it can be seen to provide sufficient assurance.

If however there are doubts in respect of a candidate for accession, or a lack of information about the real extent of protection, then the Consultative Committee, when requested by the Committee of Ministers to give an opinion, could appoint members or experts to prepare such an opinion, including by if necessary carrying out a fact-finding mission to the country in question. This has already happened in the past in respect of other CoE conventions, notably in the criminal law field (Polakiewicz 1999, 35-36). Presumably a practice similar to that adopted by the EU could also be followed, where the Commission obtains an expert report and the WP 29 Opinion draws on and refers to that expert report (as it does in its Opinion on New Zealand).

At least the following implications for future assessments of candidates for accession can be drawn provisionally from this first example concerning Uruguay:

(i) The Committee of Ministers will obtain an Opinion from the Consultative Committee (T-PD) (though it is not obliged to), putting T-PD into a position similar to the EU's Article 29 Working Party.

(ii) EU WP 29 Opinions will be utilised to support a Consultative Committee Opinion.

(iii) The standard applied by the Consultative Committee is not yet clear, but in the case of Uruguay the availability of the WP29 Opinion meant there was assurance that the law did not exist merely on paper, but did provide substantive protection.

(iv) There is no assurance, or requirement, in any of the documentation that Uruguay will adopt the Additional Protocol as part of its accession (issue 1 above), which is a considerable weakness in the process, although probably not as a matter of reality in this instance.

Implications and advantages of accession for non-European states

To summarise the previous discussion, Convention 108 Article 12 always allowed in principle for non-European states to accede to the Convention (and thus to the Additional Protocol as well), by invitation of the Committee of Ministers under the Convention. But the Committee never issued any such invitations, and there was no means of applying. However, in 2008 the Committee explicitly agreed, in effect, that the Consultative Committee under the Convention could receive and assess applications to accede, and it would then consider such applications and issue invitations to accede where appropriate. The importance of this is that Convention 108 is the only realistic possibility for a global binding international agreement on data protection to emerge. In comparison, the likelihood of a new UN treaty being developed from scratch are miniscule, or as Bygrave puts it, 'realistically, scant chance' (2010, p181). Nor will the resolutions of the meeting of the world's data protection and privacy commissioners amount to anything by themselves.

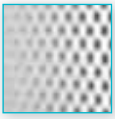
Because it has 43 existing members, there are significant advantages for non-European states in acceding to Convention 108 and the Additional Protocol. These fall into three categories. In

relation to EU countries, non-European states obtain a guarantee of free flow of personal data from the EU country (unless the EU country derogates from Convention 108 on that point), which the Directive does not give them. While Convention 108 accession will not automatically lead to a finding of 'adequacy' by the EU, it is hard to see the EU denying a finding of adequacy to a non-European state that accedes to the Additional Protocol as well as the Convention. Practically, it does not even seem necessary: none of the non-EU European countries that are Council of Europe members (and parties to the Convention) have even bothered applying for an adequacy finding (see the Table in Greenleaf 2011). In relation to other non-EU countries that are parties to the Convention, there arise mutual obligations of free flow of personal data between them, unless either derogates because of the other's lack of a data export restriction. Then there are more general advantages: it is a modest step toward a stronger international data protection regime, not a radical one; it involves voluntary acceptance as an equal party to a treaty of obligations concerning data, rather than by what can be seen as the unilateral imposition of a standard by the EU; and it avoids the necessity for individual countries to make decisions about which other countries have privacy laws which are 'adequate' or 'sufficient' to allow personal data exports to them. Depending on how long it takes the Committee of Ministers to make decisions, and whether those decisions are perceived to be fair and not unduly political, it could be a more attractive process than applying for an 'adequacy' finding to the EU Commission, and sufficient in practice even though not technically a substitute for that (discussed below).

Advantages for European states in non-European accessions

An adequacy finding from the EU does not impose any reciprocal obligations on the recipient country outside the EU to allow free flow of personal data from it to EU countries. Such a reciprocal obligation can arise if the non-EU country becomes a party to Convention 108. This will soon be a significant advantage to European states.

As the number of countries outside Europe with data privacy laws increases, and those laws include data export limitations (as they almost always do), then in theory European countries (including EU member states) will face the same problems of data export limitations as are faced by non-European countries. How can they be sure that they can import person data from non-European countries without having to comply with a myriad different data export laws in those countries? The simplest and best answer from their point of view will occur when those non-European countries are parties to Convention 108 and the Additional Protocol. Then both countries will have reciprocal obligations of free flow of personal data, and those obligations will also be consistent with the European country's obligations under the Directive (for those European countries also part of the EU).



5. CONCLUSIONS

The first part of this article discusses the geopolitical fact that 29 countries outside Europe have now enacted data privacy laws covering most of their private sectors (and most of those also cover their public sectors), and this growth outside Europe is accelerating. To a surprising extent, these laws share most of the factors that are distinctive of European data privacy laws. The conclusions of this article follow from those two factors.

Globalisation of Convention 108 is possible, but not inevitable

Since there are already 29 data privacy laws outside Europe, with many of them at least having a superficial (ie on paper) strong resemblance to European privacy laws, there would seem to be fertile ground for a significant number of non-European countries to accede to Convention 108. A few would be ruled out by their failure to cover the public sector (Vietnam, Malaysia and India). Laws on paper should not be enough for accession, but a high degree of 'family resemblance' does at least suggest a plausible order for the Council of Europe to assess possible candidates for membership (as it has now asked the Venice Commission to do). It can then encourage suitable candidates to apply where it appears that reality might match the law on paper. Convention 108 looks to be at least as promising a candidate for globalisation as the Cybercrime Convention.

Despite this theoretical possibility, there is as yet little of substance to suggest that Convention 108 will become a key instrument of global governance of privacy, despite its great potential to do so. However, it has no realistic competitors as a global privacy instrument. Uruguay is the first country to request to be invited to accede, after its accession received a favourable opinion from the Consultative Committee. The CoE is 'confident that it will only be the first country in a long list' (Polakiewicz, 2011). As yet, the Council of Europe is still doing too little that is public to explain to the rest of the world that that non-European accession to Convention 108 is possible, let alone desirable or with a reasonably transparent procedural mechanism. Its Data Protection Home Page has scattered information on all these matters, but it needs to be consolidated into one convenient location, perhaps under a 'Globalisation' heading of equal prominence as 'Modernisation'. Five key issues that need to be addressed or confirmed have already been discussed above.

Another key factor may be whether members of a regional data privacy agreement such as ECOWAS see Convention 108 accession as a collective means of establishing free flow of personal data between their region and Europe, and other countries. The CoE has a joint project with ECOWAS to help ensure that the data privacy laws of its member countries meet international standards (Polakiewicz, 2011a). Globalisation of Convention 108 could become one of the most important developments in data privacy over the next decade, but it is too early to tell. It will not happen unless the Council of Europe takes more effective steps to promote the advantages of accession to the rest of the world, and to make its own policies better development and more transparent concerning the standards that must be met for accession, and the procedures to be followed.

This article has stressed the potential advantages of non-European accession to both European and non-European states, and to businesses operating within them. From the perspective of Civil Society (the perspective of this author) the key factor determining whether it will support the globalisation of Convention 108 and the Additional Protocol is that European data privacy standards are not compromised in the process, and that new accessions meet those standards. It is worth repeating that arguments in favour of globalisation are only valid on the assumptions that (i) the current 'modernisation' process for Convention 108 does not reduce the privacy standards found in the current Convention plus Additional Protocol, particularly in the key area of data exports; (ii) the non-European accession processes also maintain those standards.

Subject to all these caveats, we should observe that global conventions often take decades to obtain a 'critical mass' of ratifications. Convention 108 is well placed to do so by the end of this decade, but there is no inevitability in this result, it will take a lot of determined work.

Europe should stick to its standards

The adoption of European data privacy standards in the legislation of a large and increasing number of countries outside Europe is a reason for Europe to adhere to those standards, additional to their intrinsic merit as a statement of human rights. There are no good reasons for Europe to retreat from the privacy standards it has slowly and relatively consistently developed over forty years. There are no alternative global standards worth considering. There are good reasons for European institutions to do a better job of enforcing their own standards, but not for abandoning them.

Increasingly, versions of the European privacy standards are becoming part of the laws of most countries in the world outside Europe (as well as all European countries), as the adoption of new data privacy laws accelerates past the current 78. The significant outliers – principally the USA and China – are few but powerful. They are increasingly living in neighbourhoods of countries that do have data privacy laws. There are some developments within each outlier country sympathetic to effective privacy protection. European and other countries with data privacy laws should continue to put pressure on the businesses and government agencies of these outlier countries, in their international interactions, to comply with what is an increasingly global standard for data privacy. Respect for their domestic prerogatives should not be confused with any need to reduce fundamental aspects of global data privacy standards.

References

A29 WP (1998) Article 29 Data Protection Working Party 'Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive' (WP 12, DG XV D/5025/98, adopted on 24 July 1998)

A29 WP (1997) Article 29 Data Protection Working Party 'First orientation on Transfers of Personal Data to Third Countries: Possible Ways Forward in Assessing Adequacy' (WP 4, DG XV D/5020/97-EN final, adopted on 26 June 1997)

APEC (Asia Pacific Economic Cooperation) (2005) *APEC Privacy Framework*, http://publications.apec.org/publication-detail.php?pub_id=390, accessed 2 September 2011

Bennett, C and Raab, C (2006), *The governance of privacy: Policy instruments in global perspective*, Boston, MA: MIT Press.

Bygrave, L (2010) 'Privacy and Data Protection in an International Perspective', *Scandinavian Studies in Law*, 56, 165–200; http://www.uio.no/studier/emner/jus/jus/JUR5630/v11/undervisningsmateriale/, accessed 2 September 2011

Bygrave, L (2008), 'International Agreements to Protect Personal Data', in James B. Rule and Graham Greenleaf (eds), *Global Privacy Protection: The First Generation*, Cheltenham, UK and Northampton, MA, US: Edward Elgar, pp. 15–49.

Connolly, C (2008) 'A new regional approach to privacy in ASEAN', Galexia website, http://www.galexia.com/public/research/articles/research_articles-art55.html, accessed 2 September 2011

CoE (2011) Council of Europe, Secretariat General, Directorate of Legal Advice and Public International Law (Jurisconsult) Legal Advice Department and Treaty Office *Note of Information: Accession to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) and to its Additional Protocol regarding supervisory authorities and transborder data flows (ETS No. 181) by States which are not member States of the Council*, September 2011 (updating previous publications from at least 1999)

CoE 108 accessions (2011) Council of Europe CETS No.: 108 webpage for accessions and ratifications, http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CM=1&DF=&CL=ENG, accessed 2 September 2011

CoE (2008) – Council of Europe, Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) (T-PD) – Abridged report of the 24th plenary meeting (Strasbourg, 13-14 March 2008) (CM(2008)81); see Draft Meeting Report, at <http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/events/t-pd_and_t-pd-bur_meetings/T-PD(2008)RAP24_en.pdf>

CoE (2008a) – Council of Europe, Committee of Ministers, CM/Del/Dec(2008)1031 4 July 2008, at <https://wcd.coe.int/wcd/ViewDoc.jsp?Ref=CM%282008%2981&Language=lanEnglish&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383>

CoE (2001) - Council of Europe *Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows*, Strasbourg, 8.XI.2001, available at http://conventions.coe.int/Treaty/en/Treaties/Html/181.htm

CoE (1981) Council of Europe *Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, European Treaty Series No. 108; adopted 28th Jan. 1981

CoE Parliamentary Assembly Resolution 1843 (2011) 'The protection of privacy and personal data on the Internet and online media', Resolution 1843 (2011), text adopted 7 October 2011

CoE Parliamentary Assembly Recommendation 1984 (2011) 'The protection of privacy and personal data on the Internet and online media', Recommendation 1984 (2011), text adopted 7 October 2011

EU Commission, 2010 'A comprehensive approach on personal data protection in the European Union' (Communication From The Commission To The European Parliament, The Council, The Economic And Social Committee And The Committee Of The Regions), Brussels, 4.11.2010, COM(2010) 609 final

EU Directive (1995) *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,* adopted 24th Oct. 1995 (Official Journal of the European Communities (O.J.), L 281, 23rd Nov. 1995, p. 31 *et seq.*)

ECOWAS (2011) Economic Community of West African States (ECOWAS) Press Release 'ECOWAS reaffirms commitment to democracy', 12 August 2011, on ECOWAS website

ECOWAS (2010) Economic Community of West African States (ECOWAS) *Supplementary Act A/SA.1/01/10 on Personal Data Protection Within ECOWAS* (February 16, 2010)

Froomkin, A M (2000) 'The death of privacy' Stanford Law Review 52(5) 1461-1543

Georges, M (2011) *Report on the modalities and mechanisms for assessing implementation of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) and its Additional Protoco*l, Bureau of the Consultative Committee of the Convention for the Protection of Individuals with Regard To Automatic Processing of Personal Data (T-PD-BUR)

Greenleaf, G (2011) 'Global data privacy laws: Forty years of acceleration' in (2011) 112 *Privacy Laws & Business International Report,* 11-17, September 2011

Greenleaf, G (2011a) 'Asia-Pacific data privacy: 2011, year of revolution?' in *Kyung Hee Law Journal* (forthcoming), available as [2011] UNSWLRS 29 at <http://law.bepress.com/unswwps/flrps11/art30/>

Greenleaf, G (2011e) 'Breach notification and diffused enforcement in Taiwan's DP Act' *Privacy Laws & Business International Report*, Issue 109, 12-13, February, 2011

Greenleaf, G (2010) 'Taiwan revises its Data Protection Act' 108 *Privacy Laws & Business International Newsletter* 8-10, December 2010

Greenleaf, G (2009c) 'Five years of the APEC Privacy Framework: Failure or promise?' *Computer Law & Security Report* 25, 28-43

Greenleaf, G (2008) 'Non-European states may join European privacy convention' *Privacy Laws & Business International Newsletter*, Issue 94, 13-14

Greenleaf, G (2008b) 'Australia', Chapter 5 in Rule J and Greenleaf G (Eds) *Global Privacy Protection: The First Generation*, Edward Elgar, Cheltenham, 2008

Greenleaf, G (2003) *Australia's APEC privacy initiative: the pros and cons of 'OECD Lite'*, *Privacy Law & Policy Reporter,* 10(10), 1–6; longer version available at <http://www2.austlii.edu.au/~graham/publications/2004/APEC_V8article.html>, accessed 2 September 2011

Greenleaf , G and Bygrave, L (2011) 'Not entirely adequate but far away: Lessons from how Europe sees New Zealand data protection' *Privacy Laws & Business International Report*, 111, 7-8, July, 2011

Hoofnagle, C (2010) 'Country Studies B.1 – United States of America' in Korff, D (Ed) *Comparative Study on Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments*' European Commission D-G Justice, Freedom and Security, http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_country_report_B1_usa.pdf, accessed 2 September 2011

Julin, T 'Sorrell v. IMS Health May Doom Federal Do Not Track Acts' *BNA Privacy and Security Law Report*, 10 PVLR 1262, 09/05/2011

Michael, J (2008) 'EU 'adequate' states to be fast-tracked by Council of Europe' *Privacy Laws & Business International Newsletter*, Issue 94, 14-15

McLeish, R and Greenleaf, G (2008) 'Hong Kong', Chapter 8 in Rule J and Greenleaf G (Eds) *Global Privacy Protection: The First Generation*, Edward Elgar, Cheltenham, 2008

Montreux Declaration (2005) - 'The protection of personal data and privacy in a globalised world: a universal right respecting diversities', Declaration of the 27th International Conference of privacy and Data Protection Commissioners, Montreux, Switzerland, September 2005

Munir, A and Yasin, S (2010) *Personal Data Protection in Malaysia* Sweet & Maxwell Asia, 2010

OECD Guidelines (1980) *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* adopted by O.E.C.D. Council on 23rd Sept. 1980 (O.E.C.D. Doc. C(80)58/FINAL)

Palazzi, P (2011) 'Data protection law in Latin America' (PPTs), presented at Privacy Laws & Business Annual Conference, Cambridge, July 2011

Polakiewicz, J (2011) 'Convention 108 as a global privacy standard?', International Data Protection Conference, Budapest, 17 June 2011 (Head of Human Rights Development Department, Directorate General of Human Rights and Legal Affairs, Council of Europe, but the paper is written in a personal capacity), available from Council of Europe website Data Protection Home Page

Polakiewicz, J (2011a) *Opening intervention*, International Data Protection Conference, 21 September 2011, Warsaw; available from Council of Europe website Data Protection Home Page

Polakiewicz, J (1999) *Treaty-making in the Council of Europe* 1999. Council of Europe

Park, W (2008) 'South Korea' Chapter 7 in Rule J and Greenleaf G (Eds) *Global Privacy Protection: The First Generation*, Edward Elgar, Cheltenham, 2008

Park, W and Greenleaf, G (2011) 'Korea reforms data protection Act' *Privacy Laws & Business International Report*, 109, 20

Raab, C (2010) 'Information Privacy: Networks of Regulation at the Subglobal Level' (2010) 1(3) *Global Policy*, 291-302

Regan, P 'The United States', Chapter 2 in Rule J and Greenleaf G (Eds) *Global Privacy Protection: The First Generation*, Edward Elgar, Cheltenham, 2008

Rule, J and Greenleaf, G (Eds) *Global Privacy Protection: The First Generation*, Edward Elgar, Cheltenham, 2008

Smith R E 'Letter to the Editor' *Privacy Laws & Business International Report*, Issue 113, October 2011

Solove, D *The Digital Person* New York University Press, 2004

Waters, N (2008) 'The APEC Asia-Pacific Privacy Initiative – a new route to effective data protection or a trojan horse for self-regulation?' [2008] UNSWLRS 59, http://law.bepress.com/unswwps/flrps08/art59/, accessed 2 September 2011

Waters, N (2011) 'The Asia Pacific Economic Cooperation (APEC) privacy framework - Implementation and enforcement: Moving forward or treading water' (PPTs), *Privacy Laws & Business Annual Conference*, St John's College, Cambridge, July 2011

Waters, N (2011a) 'APEC CBPR - ready to party but will anyone come?' *Privacy Laws & Business International Report*, Issue 113, October 2011

ENDNOTES

1 This paper was developed while the author was a Visiting Fellow at the AHRC-Script Centre, Faculty of Law, University of Edinburgh. An earlier version was presented to the *International Data Protection Conference*, Polish Data Protection Authority (GIODO), 21 September 2011, Warsaw. Parts of the paper are based on a chapter '*Global data privacy in a networked world*', to be published in the I Brown (Ed) *Research Handbook on Governance of The Internet,* Edward Elgar Publishing, Cheltenham, 2012 (in press). Very helpful comments were provided by (in alpha order) Inês Antas Barros, Colin Bennett, Lee Bygrave, Magda Cocco, Robert Gellman, Marie Georges, Chris Hoofnagle, Christopher Kuner, Pablo Palazzi, Jörg Polakiewicz, Charles Raab, Daniel Solove, Blair Stewart, and Nigel Waters, but responsibility for all content remains with the author. Assistance with the Table in this paper is acknowledged separately with the Table. Comments are welcome to <graham@austlii.edu.au>. A copy is at <http://www2.austlii.edu.au/~graham/>.

2 The completion of the Table is based on advice received in relation to Latin American countries from Pablo Palazzi (Allende & Brea, Argentina); in relation to francophone countries, from Marie Georges (Planete Informatique et Liberties, Paris); in relation to lusaphone (Portuguese-speaking) countries, from Magda Cocco and Inês Antas Barros (Vieira de Almeida & Associados, Lisbon); and in relation to Canada, from Colin Bennett (Victoria University, BC); overall responsibility remains with the author. Articles supporting many of these assessments are in the bibliography.

PROGRAMMES OF THE DATA PROTECTION CONFERENCES

INTERNATIONAL DATA PROTECTION CONFERENCE BUDAPEST, 16-17 JUNE 2011

Thursday, 16 June 2011

09.00 – 09.30 Registration

09.30 – 10.45 General context – where we are now and where we are heading – current and future dilemmas of privacy protection

The first panel is designed to present the broad and actual context in which legal instruments related to privacy protection must be interpreted and to discuss the current challenges and perspectives for the future data protection regime. The timing of the conference, June 2011, offers an opportunity to assess the achievements of the Hungarian Presidency in the field of justice, including data protection. The presentations in this part are meant to discuss the possible perspectives of the future data protection regime.

9.30 Welcome address by Róbert Répássy, Minister of State for Justice, Ministry of Public Administration and Justice

9.45 Keynote address by Françoise Le Bail, Director General of Justice, European Commission

10.00 Keynote address by Aurora Mejía, Director General for International Legal Cooperation and Religious Affairs, Ministry of Justice, Spain

10.15 Keynote address by Peter Hustinx, European Data Protection Supervisor

10.30 Keynote address by Piotr Stachańczyk, Undersecretary of State, Ministry of Interior and Administration of Poland.
Moderator: Ferenc Zombor, Deputy State Secretary, Ministry of Public Administration and Justice of Hungary

10.45 – 11.15 Coffee break

11.15 – 12.45 Working session I. - Free movement of personal data, the internal market dimension – outlook from case law

The free movement of personal data is the second objective declared in the current Directive. The internal market dimension of the data protection regime is highlighted in several Communications tabled by the Commission, all suggesting changes in specific provisions on the flow of personal data within the European Union. Consequently the question presents itself whether divergent data protection regimes in Member States distort the functioning of the common market, implying that a more harmonised legal framework would significantly help data subjects in the exercising their rights?

Chair of the panel: Giovanni Buttarelli, Assistant European Data Protection Supervisor
Presentations followed by a panel discussion.

11.15 Marie-Hélène Boulanger, DG Justice, Data Protection Unit, European Commission

11.30 Maarten Truyens, DLA Piper UK LLP, Data protection fragmentation in the internal market: some practical examples

11.45 Jonathan Weeks, Deputy Legal Director for Intel in EMEA, Better Harmonisation: Protecting Privacy & Creating Trust

12.00 Questions and answers

12.30-14.30 Lunch break

14.30-16.00 Working session II. – Protecting the individual 'in the cloud' – rights of the data subject in the IT environment

The conference will devote distinguished attention to societal changes and political implications induced by the globalised information society. These questions are also relevant related to the upcoming setting up of a new, comprehensive legal framework on data protection. In this context, the mechanisms by which the current Data Protection Directive's objectives may be put into practice in a more efficient manner – also in the cloud – could be thoroughly discussed. Concrete cases where national legislations could protect (or failed to protect) individuals will be discussed. Relevant jurisprudence and opinions in this regard present further points to discuss (e.g. use of cloud services, e-health, e-government). The protection of individuals and the fundamental rights aspect of data protection are the core element of the legal regime. Easing the exercise of the rights of data subjects and the adjustment of current instruments to globalisation and changing IT environment are major challenges to address.

Chair of the panel: Christopher Kuner, Data Protection Task Force of the International Chamber of Commerce (ICC), Paris
Presentations followed by a panel discussion.

14.30 Sławomir Górniak, Technical Competence Department, European Network and Information Security Agency (ENISA), Cloud Computing – Security and privacy issues

14.50 Janni Christoffersen, Data Protection Commissioner of Denmark, Cloud computing – a challenge to data protection?

15.10 Wojciech Rafał Wiewiórowski, Polish Commissioner for Data Protection, Privacy and ISP Liability in the Cloud

15.30 Questions and answers

16.00-16.30 Coffee break

16.30-18.00 Working session III. – Raising awareness about rights related to privacy – education of the rights to citizens – closer to citizens

Researches show that citizens are often aware of their rights related to the protection of privacy and personal data. In the meantime, the exercise of rights proves frequently very difficult. Role of parents in protecting minors' interests is an issue of special relevance in this regard.

From video clips to comics and video games, a lot of initiatives have flourished. The panel will present several initiatives and discuss what the best strategies are.
Chair of the panel: Karolina Rokicka, Academy of European Law (ERA)
Presentations followed by a panel discussion.

16.30 Sophie Kwasny, Head of the Data Protection Unit, Council of Europe, Raising awareness on data protection: The contribution of the Council of Europe

16.45 Urszula Góral, Director of Social Education and International Cooperation Department, Polish Data Protection Authority (GIODO), Educational activity of the Polish Data Protection Authority

17.00 Peter Michael, Data Protection Secretary of the Joint Supervisory Authority

17.15 Andreas Krisch, President of European Digital Rights (EDRI), Data protection: Raising awareness amongst all stakeholders

17:30 Questions and answers

Friday, 17 June 2011

09.00 – 10.30 Working session IV. – New principles in the field
In recent years, several new data protection principles have been elaborated. The privacy by design principle, the principle of accountability, the promotion of privacy enhancing technology are all different aspects to be considered from the legislative point of view. This panel is aimed at exploring the possible implications of these new principles.
Chair of the panel: Wojciech Rafał Wiewiórowski, Polish Commissioner for Data Protection
Presentations followed by a panel discussion.

9.00 Paul De Hert, Professor at the Vrije Universiteit Brussel, From the Principle of Accountability to System Responsibility - Key Concepts in Data Protection Law and Human Rights Law discussions

9.15 Hielke Hijmans, Head of Section, Secretariat of the European Data Protection Supervisor, Principles of data protection: Renovation needed?

9.30 Florence de Villenfragne, Senior Researcher, University of Namur, Modernising Convention 108: complementing 30 years old principles

9.45 Szabó Endre Győző, Chairman of DAPIX, Ministry of Public Administration and Justice of Hungary, New principles – in the light of the discussions within the Council
Council conclusions on the Commission's Communication

10.00 Questions and answers

10.30-11.00 Coffee break

11.00-13.00 Working session V. – Global compatible standards of privacy / data protection

The European Union is committed to ensure a high level of protection to all data subject, even when data processing is somehow linked to a third country, yet this is only possible if international standards are elaborated. In this regard, the Madrid Standards (or 'Madrid process') could be an outstanding example, serving as a starting point for further discussions. A reference to the Council of Europe Convention 108 which, as underlined by the Ministers of Justice in Istanbul in November 2010 (Resolution No 3 on data protection and privacy in the third millennium) is 'currently the only potentially universally binding legal instrument in the field' would fully correspond to the topic of this fourth session. The current adequacy policy of the European Union needs to be improved, which naturally brings this topic into the ambit of the present conference.

Chair of the panel: Peter Hustinx, European Data Protection Supervisor
Presentations followed by a panel discussion.

11.00 Agustín Puente, Head of the Legal Department of the Spanish Data Protection Agency, Global and implementable international standards

11.15 Rosa Barcelo, legal officer, European Data Protection Supervisor, Global Dimension of Data Protection

11.30 Ilias Chantzos, Government Affairs Director in EMEA and APJ for Symantec

11.45 Christopher Kuner, Chairman, Data Protection Task Force of the International Chamber of Commerce (ICC), Paris, Global standards for data protection and privacy: the business viewpoint

12.00 Jörg Polakiewicz, Head of Department, Council of Europe, The potential of Convention 108: the way forward

12.15 Questions and answers

12.45 Closing remarks by Attila Péterfalvi, former Parliamentary Commissioner for Data Protection and Freedom of Information of Hungary, Member of the Management Board of the Fundamental Rights Agency

INTERNATIONAL DATA PROTECTION CONFERENCE WARSAW

Wednesday, 21 September 2011

09.00–09.30 Registration

09.30–10.00 Official Opening of the Conference
Piotr Stachańczyk, Undersecretary of State, Ministry of the Interior and Administration, Poland, Dr. Wojciech Wiewiórowski, Inspector General for Personal Data Protection, Poland, Jörg

Polakiewicz, Head of the Human Rights Development Department, Council of Europe, Paul Nemitz, Director of the Fundamental Rights and Union Citizenship Directorate, European Commission

10.00–11.30 Working Session I – Effectiveness of personal data protection principles in the changing world.

Deep changes of the contemporary world related to IT technologies development and globalization have not led to negating the importance of the personal data protection principles existing so far; they have rather entailed a question on the way of ensuring their effectiveness in the new environment. New concepts and principles formulated in the recent years shall be a reply to this question. While continuing a discussion initiated at the Conference in Budapest, it is worth deepening an analysis of some of them, not only from the legislative perspective, but also from the perspective of the future practice. They include the principle of privacy by design, privacy enhancing technologies, PIA, or related accountability principle. Will these concepts be a mythical Holy Grail or will their implementation ensure effectiveness of personal data protection, or will they remain just empty slogans? Do the so far experiences with implementation of PETs allow for optimism? What are the conditions for success? On the other hand, the European Commission proposes introducing the right to be forgotten. Is it a new right, when can it be used and be workable? This panel is aimed at exploring these issues.

Moderator: Jacob Kohnstamm, Chairman of the Article 29 Data Protection Working Party
Presentations: Wacław Iszkowski, Polish Chamber of Information Technology and Telecommunications, Ilias Chantzos, Senior Director EMEA & APJ Government Affairs, Symantec Corporation David Wright, Trilateral Research & Consulting, London (Presentation), Peter Fleischer, Global Privacy Counsel Google, Caspar Bowden, Independent privacy advocate

11.30–11.45 Coffee Break

11.45–13.15 Working Session II – current and future framework of personal data protection in the police and justice.

While awaiting completion of the process of revision of Convention 108 and Recommendation R(87) 15, as well as presentation of the new framework of personal data protection in the EU, it's worth to summarize the current legislative changes, as well as ongoing discussions, and reflect on the present and the future shape of the model of data protection in the area of police and judicial cooperation in criminal matters. Application of general rules or special "tailor made" rules, the relationship between the future legal framework and special protection systems (eg. within Europol), the scope of the modification of common data protection principles in this sector, the future model of supervision, or a way to demonstrate the necessity and proportionality of new instruments for the exchange of information - are questions that the panelists will try to answer.

Moderator: Dr. Filip Jasiński, Chairman of the GENVAL Working Party of the EU Council for PNR/TFTS
Presentations: Kevin Fraser, Representative of the UK Government, Dr. Franziska Boehm, University of Luxembourg, Daniel Drewer, Data Protection Officer, Europol, Dr. Ben Hayes, Statewatch, Dr. Mireille Caruana, Council of Europe Expert

13.15–14.15 Lunch break

14.15-15.45 Working Session III – European data protection standards as a benchmark for others – practical experience, problems and future directions of action.

Undoubtedly, global challenges require global solutions. Hence the desire to pursue the creation of common standards for data protection and promotion of all initiatives to this end is understandable. Europe has been and should continue to be the driver of such activities, as evidenced by the opening of membership to Convention No. 108 to countries outside of the Council of Europe or the launch of the Madrid process aimed at developing universally recognized principles of data protection. Mindful of these far-reaching goals, sight should not be lost of the ongoing implementation process – influenced by both the Council of Europe and the European Union – of the regulations on personal data protection in additional countries. This process is not easy and still requires various forms of support and involvement of numerous institutions and organizations, including, in particular, data protection authorities, which have inter alia created various forums of cooperation with authorities of these countries. This panel is an attempt to assess past experiences, identify core problems and the most effective forms of support, as well as directions for further action.

Moderator: Peter Schaar, Federal Commissioner for Data Protection and Freedom of Information, Germany

Presentations: Jean-Philippe Walter, Chairman of the T-PD Committee, Council of Europe (Presenation in French), Dr. András Jóri, Parliamentary Commissioner for Data Protection and Freedom of Information, Hungary, Daniel Weitzner, Deputy Chief Technology Officer for Internet Policy at the White House, Christoph Luykx, Intel

15.45–16.00 Closing Remarks

16.00 End of the Conference

Responsible editor: Ferenc Zombor

Editor: Endre Győző Szabó

This volume was published by the Hungarian Official Journal Publisher,
1085 Budapest, Somogyi Béla u. 6., HUNGARY

Responsible publisher: Zsolt László Majláth

This publication has been realized with the support of the European Commission
(Project „Data protection measures at European level, international challenges
and directions of future improvements", agreement number –
JUST/2010/FRAC/AG/1297 – 30 –CE-0377148-00-05).

ISBN 978-963-9722-96-5

MINISTRY OF PUBLIC ADMINISTRATION AND JUSTICE

EUROPEAN COMMISSION

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

ERA

ADATVÉDELMI BIZTOS

GIODO
Generalny Inspektor Ochrony Danych Osobowych

MSWiA
Ministerstwo Spraw Wewnętrznych i Administracji

GOBIERNO DE ESPAÑA MINISTERIO DE JUSTICIA