

# Abstracts



**Opening Lecture**

**INTERNATIONAL DATA-SHARING:  
STANDARDISATION, HARMONISATION AND ETHICS**

By  
Prof. Ruth Chadwick, Director of the ESRC, Centre for Economic and Social Aspect  
of Genomic (CESAGEN), Cardiff University, United Kingdom

**Abstract**

There have been calls for harmonisation in the light of the international context in which data-sharing is now taking place, in relation to developing links between different database initiatives, for example, which may have been developed in quite different socio-cultural contexts. But this raises the questions of what is meant by harmonisation, how it relates to standardisation, and the extent to which it is desirable from an ethical point of view. It is argued in this paper that seeking harmonisation should not be interpreted in terms of the 'unison' of different voices: on the contrary the analogy of musical harmony should alert us to the possibility, in ethics also, of the interplay of different voices in relation to a 'text' or 'standard'. The extent to which variations are permissible, and the ways in which new instruments have the potential to disrupt pre-existing harmony, thereby challenging fundamental values, also have to be considered, along with the practical implications for data-sharing.

## **Session I: International Data Sharing**

# **International Data Sharing, Privacy and Data Protection: The EU Perspective**

By Mrs. Bénédicte Havelange, Policy and Information Unit, Office of the European Data protection Supervisor (EDPS), Belgium

### **Abstract**

Recent years have been marked by a growing demand for international data sharing both for public security purposes and for commercial/private interests. Access to and protection of these data are climbing the transatlantic and wider international agenda. They have raised tensions between the EU and its partners across the world, but they have also made the reflection on data and privacy protection progress significantly.

This presentation will first address how privacy and data protection developed in the EU. In particular, these aspects which are very specific to the EU approach will be discussed:

-the 1995 EU Data Protection Directive has a dual purpose: permit the free flow of information while ensuring a high level of protection for the individuals. It is interesting to see how this apparent tension has been dealt with.

-In the recent years, data protection has gained a recognition as a fundamental right, which gives the EU data protection system very distinctive features.

-The role of independent data protection authorities will also be explained since it is one of the most prominent characteristics of EU data protection.

Secondly, the presentation will explained the EU approach of international information sharing, both from a legal perspective and from a policy point of view.

Finally, some relevant case studies will illustrate how the principles are applied. These examples will focus mainly on the exchange of (especially biometric) data for public security and immigration purposes.

## **Session I: International Data Sharing**

### **TRUST TRANSPARANCY AND DATA GOVERNANCE: CHALLENGES IN THE APEC PRIVACY FRAMEWORK AND THE EU DIRECTIVE**

By

Mr. Malcolm Crompton, Managing Director of Information Integrity Solutions P/L,  
Privacy commissioner for Australia 1999-2004, Australia

#### **Abstract**

Every day, an increasing proportion of the personal information about each of us moves across borders and so into different legal jurisdictions. Business is initiating this to improve service quality and reduce costs to customers; governments are doing it for similar reasons and to improve border controls, policing and some of their other functions; citizens and customers are initiating transfers when they make a purchase online or wish to travel overseas.

The European Union has addressed the safe transfer of personal information across borders within the Union as part of EC Directive 95-46. The Directive also establishes a framework intended to apply to the movement of personal information outside the Union based on whether there is 'adequate' privacy protection for the information, including through Binding Corporate Rules. Only a very limited number of jurisdictions outside the EU have been found to have 'adequate' privacy law and very few companies have been able to obtain approval for Binding Corporate Rules.

APEC is the world's largest regional grouping and the most recent to adopt a privacy framework. It is now putting in place a mechanism to allow the safe movement of personal information between participating APEC jurisdictions. Its initial focus has been on ensuring the accountability of companies for complying with Cross Border Privacy Rules that meet the requirements of the APEC privacy framework, combined with workable redress mechanisms when a problem arises.

The EU BCR and APEC CBPR concepts are very similar in theory but differ considerably in practice. Both are promising but yet to deliver at any scale. In theory at least, they could be the starting point for finding ground for a truly global framework for allowing the safe movement of personal information between jurisdictions.

There are many examples of effective federations of states and provinces into nations that allow safe movement within the federation. Stronger mechanisms are constantly being developed for safer movement of individuals and finance between jurisdictions. These examples suggest that there is no reason to believe it is any more difficult to do the same for personal information.

The recent enforcement action by the Australian Communications and Media Authority against Dodo Australia Pty Ltd offers promise for how to enforce the requirements of a privacy framework.

The benchmark test is simple: individuals should not be exposed to any additional country risk simply because another party has moved personal information about them into another jurisdiction unless they are in a position to make a fully informed decision to allow it.

Achieving the benchmark will require rebalancing so that equal attention is paid to enforcement as is paid to the framework and rules.

**Session I: International Data Sharing**

**PROTECTION OF PRIVACY:  
IMPLEMENTATION OF THE APEC PRIVACY FRAMEWORK IN NATIONAL  
REGULATION**

By

Prof. Abu Bakar Munir, Dean of the Faculty of Law, University of Malaya, Malaysia

**Abstract**

The very diverse 21 member economies of Asia-Pacific Economic Community (APEC), which include, Australia, Canada, China, Japan, Vietnam, Malaysia, Singapore, Russia and the U.S, adopted the APEC Privacy Framework 2004. Some argue that the Framework can be a good foundation for global standard. Google describes the Framework as the most promising foundation, and states that, "Surely, if privacy principles can be agreed upon within 21 APEC member economies, a similar set of principles could be applied on a global scale". Some have been very critical of the Framework. A privacy law expert argues that the principles in APEC's Privacy Framework are at best an approximation of what was regarded as acceptable information privacy principles twenty years ago when the OECD Guidelines were developed. In relation to the implementation, the expert argues that the Framework is considerably weaker than any other international privacy instrument. This paper discusses briefly the Framework's data protection principles. The paper then examines, specifically, the implementation aspects as provided for in Part IV of the Framework. In conclusion, the paper makes an assessment on what have been or being done in some member economies, after five years of the APEC Privacy Framework, to protect privacy.

**Session I: International Data Sharing**

**DIMENSIONS OF DATA PROTECTION: A U.S. PERSPECTIVE**

By

Mr. Jim Harper, Director of Information Policy Studies, the Cato Institute, Member of Dept. of Homeland Security's Data Privacy and Integrity Advisory Committee, USA

**Abstract**

The Human interests at stake in international data sharing and biometric identification are poorly understood. This hampers the development of appropriate and balanced government policies. "Privacy" and "data protection" refer to at least five different interests: control of personal information, fairness, seclusion, personal security, and liberty. Different countries and cultures prioritize these values differently, compounding the difficulty of policy development in the international context. When governments establish information-sharing policies for security purposes, they should weigh the costs to their citizens in terms of privacy and related values against the security benefits they anticipate from such sharing. The benefits of information sharing should be thoroughly articulated in terms of risk management so that governments do not needlessly undermine their citizens' privacy and related interests.

**Session II: Privacy vis-à-vis Security**

**PRIVACY, INTRUSION AND THE DETECTION OF TERRORISM**

By

Prof. Tom Sorell, John Ferguson professor of Global Ethics and Director of Centre for the Study of Global Ethics, University of Birmingham, United Kingdom

**Abstract**

Life-threatening and life-taking criminality-this includes terrorism-can justify not only reactive punishment after it has been carried out, but also preventive intrusion when it is being planned. Profiling may be a very unintrusive method of preventive policing, but is highly discriminatory (and frequently ineffective), whereas surveillance based on evidence is less discriminatory but more intrusive. Surveillance must be proportional, but what counts as proportional varies according to privacy's value, and the risk to life if privacy is left undisturbed. The value of privacy is not fixed for all time, but may shift with features of the social context, such as, for example, mas acceptance of kinds of exhibitionism and voyeurism associated with reality television and social networking websites. Nevertheless, some acts of preventive intrusion are unjustifiable even in those contexts.

## **Session II: Privacy vis-à-vis Security**

### **PRIVACY AND BIOMETRIC TECHNOLOGIES**

By

Assist. Prof. Terence Sim, School of Computing, National University of Singapore, Chairman of the Cross-Jurisdictional and Societal Aspects Working Group (WG6) of the Biometrics Technical Committee, Singapore.

#### **Abstract**

Privacy and biometrics appear to be contradictory terms. One deals with safeguarding personal secrets, while the other deals with identifying a person, and thus revealing many details of that person. Indeed, among the different notions of privacy -- informational, bodily, territorial, and communications privacy - biometrics not only impacts informational privacy, but also affects bodily and territorial privacy as well. However, contrary to the claims of civil libertarians and to Hollywood hype, biometrics need not be antithetical to privacy. Indeed, by understanding the relevant issues, it is possible to design into a biometrics system measures that will safeguard, and even enhance, privacy. Doing so will increase user acceptance of biometric systems, or at least, render such deployments more tolerable. This talk will highlight keys issues, and suggests ways to allow privacy and biometrics to work together.

## **Session II: Privacy vis-à-vis Security**

### **PALMPRINT IDENTIFICATION**

By

Prof. David Zhang, Chair Professor and Director of Biometric Research Centre,  
Hong Kong Polytechnic University, China

#### **Abstract**

In recent times, an increasing, worldwide effort has been devoted to the development of automatic personal identification systems that can be effective in a wide variety of security contexts. As one of the most powerful and reliable means of personal authentication, biometrics has been an area of particular interest. This interest has led to the extensive study of biometric technologies such as fingerprint and face recognition and the development of numerous algorithms, applications, and systems. Palmprints, in particular, have attracted a lot of interest. Recent interest in palmprints is justified. Palmprints have a number of unique advantages: they are rich in features such as principal lines, wrinkles, and textures and these provide stable and distinctive information sufficient for separating an individual from a large population. Having worked on palmprints since 1996, our team certainly regards the palmprint as a very effective biometric. In this presentation, we would like to provide a brief introduction to palmprint technologies. We will compare some important algorithms, as well as at the different stages of implementation of a palmprint system. We also have made available part of our palmprint database for the public to download. Further details can be found on <http://www.comp.polyu.edu.hk/~biometrics/>

## **Session II: Privacy vis-à-vis Security**

### **PRIVACY AND DATA PROTECTION POLICIES IN INDIA**

By

Mr. Vinyak Godse, senior manager, Security Practices, Data Security Council of India (DSCI), Nasscom, India

#### **Abstract**

The notion of privacy varies across the geographies, which is reflected in respective national policies and regulations. Culture plays a significant role in shaping attitudes about privacy. Although it is perceived that Indians are less concerned and aware about privacy, thrust for privacy policies and initiatives have been observed in recent years. This is because of rising issues, and respective suffering from misuse of personal information in digital and communication world. Secondly, as a leading and matured outsourcing service provider, Indian IT and BPO companies are serving the client across the globe, with different privacy cultures and their corresponding legislations. Data privacy is emerging as an important concern of Transborder data flow. The quantum and criticality of data is increasing as the outsourcing industry grows in scale and quality. The IT and BPO companies, with their clients, are also sharing the responsibility of compliance to the data protection regulations, in different capacity like data processor, co-manager and data controller. This has been key driving force behind the privacy initiatives of Indian organizations.

To protect individual's right to his personal information and protect the interest Indian business going global, there is a need of national policies or regulation for privacy. The privacy legislations should protect the interest of the organizations doing business globally, and also should be in line with the culture of the society. Indian legislations guarantees privacy as a fundamental right in spirit, and have some special and supporting legislation, which can be attributed to privacy. Recently, Indian policy makers have responded with amendment of IT Act, which incorporate specific provision for protection of sensitive personal information. Indian IT and BPO industry also felt a need of establishing a self regulatory organization for data protection. DSCI, set up by NASSCOM, an apex body of software and services Company in India, is a non-profit company focusing on data protection. Being SRO, DSCI will establish a mechanism to facilitate assurance over the data protection.

The session 'Privacy and Data Protection Policies in India', will discuss the privacy landscape in India including that of privacy culture, regulatory directions and business initiatives. It will also discuss how the awareness towards privacy is gaining momentum, and relevance of the issue of privacy in the biometric identification.

### **Session III: Is There a Right to Have an Identity?**

#### **IS THERE A UNIVERSAL RIGHT TO IDENTITY?**

By

Prof. Roger Brownsword, Director of Centre for Technology, Ethics and Law in Society (TELOS), School of Law, King's College, London, United Kingdom

#### **Abstract**

Is there a universal right to identity? Before we can hope to answer this question, we need to consider whether there are any universal rights at all. If there are no universal rights (as many sceptics contend), then there is clearly no universal right to anything, including no universal right to identity. If, however, there are some universal rights, the question remains whether a right to identity is one such right.

Adopting a Gewirthian approach, I tackle this question in two stages. In the first part of the paper, I outline and elaborate upon three key background claims.

First, I claim that, by thinking through the logic of our agency, we can make out a compelling justification for universal rights. However, it is only if we self-identify in a minimal way—viewing ourselves merely as agents (as beings with the capacity for free and purposive action) that this justification works. Once we try to personalise our agency, we can make rights claims but they will no longer universalise.

Secondly, the universal rights so justified, I claim, concern the protection and promotion of the essential conditions of, and context for, agency. Such rights relate to the freedom and well-being of agents (rather than their particular purposes and projects) and to a setting that is conducive to flourishing agency.

Thirdly, I claim that, as members of a community of rights, agents have a right to adopt and pursue whatever particular purposes or projects they wish so long as such purposes and projects are compatible with the essential conditions and context of agency for which all agents have a responsibility. In this way, the community of rights offers a setting in which each agent may develop and self-identify in a personal and distinctive way.

On this analysis, we need to operate with a thin characterisation of identity if we are to reason our way to the idea of universal (agency-based) rights; but we can thicken up (and personalise) our sense of identity once we have established the basis for a community of rights-bearing agents.

In the second part of the paper, assuming the setting of a community of rights, I consider whether (and, if so, how) it might make sense to claim a right to identity. In such a community, the critical question is whether a denial of identity either interferes with the essential conditions of agency or serves to corrode or compromise the context for agency.

My conclusion is that, for the most part, the kinds of acts (such as, identity theft, identity suppression, biometric marking and monitoring, and so on) that prompt the articulation of a right to identity are an appropriate cause for concern in such a community; but that we can usually express the nature of the concern without having to construct a distinctive right to identity.