

# DELIVERABLE D5.1 – Workshop 1 Report



## HIDE PROJECT

Project funded by the European Commission-FP7

Contract: 217762

Co-ordination and Support Action (CSA)

Start date of the project: 1 Feb 2008

Duration 36 months

1° Reporting Period

Deliverable:	D5.1
Title:	Workshop Report
Due date:	31.07.2009
Actual submission date	02.08.2009
Lead contractor for this deliverable:	NUS, CBmE
Contact: Alastair V. Campbell	<a href="mailto:Medave@nus.edu.sg">Medave@nus.edu.sg</a>
Dissemination Level:	PU

## **Workshop Report**

### **International Data Sharing and Biometric Identification – The Ethical Issues in an Asian and International Context Singapore 2-3 July 2009**

The workshop on International Data Sharing and Biometric Identification – The Ethical Issues in an Asian and International Context, was the first out of two problem solving workshops to be held in the HIDE project. The workshop is part of the activities carried out within the HIDE project Work Package 5. This one and a half day workshop took place at Balmoral Hall, in the hotel Royal Plaza on Scotts, Singapore on 2-3 July. A total of 42 people including 13 speakers participated in the workshop. The workshop was organized by the Centre for Biomedical Ethics (CBmE), Yong Loo Lin School of Medicine, National University of Singapore (NUS), Singapore, in cooperation with Centre for Science, Society and Citizenship (CSSC), Italy. This report summarises the workshop session by session.

Annexes to this report:

Annex I: Overview of sessions and working questions

Annex II: Abstracts for presentations

Annex III: Slides for presentations

- a. Ruth Chadwick,
- b. Bénédicte Havelange,
- c. Malcolm Crompton,
- d. Abu Bakar Bin Munir,
- e. Tom Sorell,
- f. Terence Sim,
- g. David Zhang,
- h. Vinayak Godse,
- i. EricYap

Annex IV: Participants List

Annex V: Short biographies of speakers and chairs

## **Background**

### ***Workshop Philosophy***

One of the main purposes of the workshop was to identify and discuss some of the ethical and legal challenges that the APEC Privacy Framework may pose to the EU Data Protection Directive. The two main objectives of the workshop were:

- To discuss international data sharing and biometric identification used for surveillance/security purposes and in particular the ethical issues in an Asian as well as an international context.
- To identify and discuss potential value conflicts relating to key concepts such as privacy, security and identity.

The workshop philosophy (as outlined in the HIDE project DOW Work Package 5) is to bring together experts from various disciplines and nations and create a forum for a dialogue where everyone speaks as an individual and not on behalf of groups, institutions or governments. The main aim is to identify and alter stereotyped, negative images and to discuss possible small but meaningful steps towards resolutions of complex problems. This can best be done by taking an analytical approach, where speakers and participants are asked to explain their own perspectives and to engage in a dialogue rather than a debate.

As the HIDE policy forums had the purpose of addressing ethical issues related to biometric identification and protection of personal data, mainly within a European and American context, the problem solving workshop in Singapore was an opportunity to address some of the same issues in a broader international context. With this in mind the Singapore workshop was also designed to put focus on the APEC Privacy Framework, as well as to focus on perceptions of key concepts such as privacy, security and identity within an Asian context. One of the core strategic aims was to create a forum for a dialogue by bringing together speakers with expertise in different academic disciplines as well as representatives from industry and government institutions.

### ***Identifying the speakers to be invited and the issues to be addressed***

The workshop programme consisted of an opening session/lecture followed by four major sessions addressing different aspects of international data sharing and biometric identification under four themes:

- Session I: International Data Sharing;
- Session II: Privacy vis-à-vis Security;

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

Session IV: Personal Data and the Human Body: Rights and Ethics

The theme for each session was decided by the workshop organizers (Alastair V. Campbell, CBmE and Emilio Mordini, CSSC). In order to ensure the level of consistency between the presentations, a short description of the scope of each workshop session as well as a number of working questions were prepared and sent to speakers and chairpersons upon invitation.<sup>1</sup>

The speakers were selected according to their individual expertise in relation to the themes of the four sessions. An important aim in the planning of session I was to ensure that the presentations were carefully combined so that they addressed the challenges in international data as seen from an EU context, a US context and from a broader range of perspectives within an Asian-APEC context. It was therefore important to ensure such a balance in the choice of speakers. As one of the main objectives of the workshop was to focus on ethical issues related to international data sharing and biometric identification in an Asian context, the focus in the planning of session II was to ensure a large number of presentations addressing different perspectives of privacy and security from various approaches within Asia.

A similar balance as that achieved in session I was planned for sessions III and IV, but due to last minute cancellations from speakers, this aspect of the workshop strategy was not reflected in the final version of the programme for these sessions.

A working title for each speaker's presentation was suggested. Based on this the speakers was asked to prepare an abstract and submit this 6 weeks prior to the workshop.<sup>2</sup> This made it possible for the organizers to contact each speaker about focus on content in some cases so that overlap, in particular in presentations outlining technical details about the legal frameworks, was avoided.

***Speakers:***

*Opening session:*

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

*Session I:*

---

<sup>1</sup> The scope of the sessions is outlined under the description of the four sessions. See also Annex 1.

<sup>2</sup> The abstracts and slides for each presentation can be found in workshop report Annex II and Annex III)

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

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

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

**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

*Session II:*

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

**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.

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

**Mr. Vinayak Godse**, Senior manager, Security Practices, Data Security Council of India (DSCI), Nasscom, India.

*Session III*

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

**A/Prof. Eric Yap**, Assist. Director (Human Systems), Head (Human Systems), Defence Science & Technology Agency, DSO National Laboratories and Ministry of Defence, Singapore

*Session IV*

**Mr. Colin Minihan**, Senior Advisor, Privacy and Freedom of Information Policy Branch, Dept. of the Prime Minister and Cabinet; Chair of the Data Privacy Sub-group, The Electronic Commerce Steering Group (ECSG) APEC, Australia.

**Mr. Michael Hardin**, Senior Policy Analyst, US-VISIT Programme, U.S. Department of Homeland Security, USA.

**Chair:**

**Prof. Alastair V. Campbell**, Chen Su Lan Centennial Professor of Medical Ethics, Director of Centre for Biomedical Ethics (CBmE), National University of Singapore, Singapore (opening session & general discussion)

**A/Prof. Joseph Liow**, Associate Dean, S. Rajaratnam School of International Studies, Nanyang Technological University, Singapore (session III)

**Prof. Emilio Mordini**, HIDE Project coordinator, Centre for Science, Society and Citizenship (CSSC), Italy (session II and IV)

**Prof. Leonardo De Castro**, Director of the Programme for Capacity Development in Biomedical Ethics, Centre for Biomedical Ethics (CBmE), Research Office, National University of Singapore, Singapore (session III)

## **Thursday 2 July**

### **Opening session (9:00-9:50am)**

The workshop was opened by Prof. Alastair V. Campbell, Centre for Biomedical Ethics, National University of Singapore. After welcoming speakers and participants he gave a brief introduction to the workshop philosophy. The Singapore workshop was highlighted as an opportunity to discuss the ethical issues of data sharing and biometric identification in a wider international context. Professor Campbell encouraged all speakers and participants to make full use of the time for questions and discussion. These opening remarks were followed by the lecture by Prof. Ruth Chadwick.

*Prof. Ruth Chadwick:*

#### **International Data-Sharing: Standardisation, Harmonisation and Ethics**

The thematic focus of Prof. Chadwick's opening lecture was the process of harmonisation that lies behind the discussion of standards, and in particular the role of ethics in this context. Prof. Chadwick raised the question: whether it is possible to have harmonization in ethics and what this would mean in practice? Prof. Chadwick argued that setting a standard is not enough; it is also necessary to look at who has the power to set the standards. The presentation concluded that a harmonisation in relation to ethics can best take place if it is not interpreted as a matter of reaching a 'unison' of voices. Instead, it was argued, harmonisation with respect to ethical issues around privacy protection should be seen as an ongoing process where existing values can also be challenged. Such a process should give room for cultural dialogue as well as taking into consideration how concepts such as privacy are dealt with in different spheres (the biomedical research context, the medical context and the context of basic data sharing). Rather than considering standards mainly in terms of trade-offs between different values, Prof. Chadwick used a 'playing-card metaphor' and

argued that it is necessary to consider options of trumps as well. This however, requires negotiation over the nature of the problem and identification of areas of possible conflict.

Prof. Campbell asked about Prof. Chadwick's view on the human rights model's potential as a model for harmonisation of ethics. Chadwick argued against the idea of using the human rights model, because such a model does not take into consideration the traditions and the differences in various contextual spheres that she believes are necessary to answer the question of whether ethics can be 'harmonised.'

## **Session I**

### **International Data Sharing**

**(9:50am-12:45pm)**

The aim of session I was to discuss the challenges in existing international regulations with regard to sharing of personal data.

The session was designed to give a diverse picture of the challenges occurring in international regulations on data sharing, in order to ensure a solid basis for discussion. Therefore, each speaker was presenting on the basis of his/her special expertise and experience with regard to implementation of guidelines and regulations of data sharing, both regionally and internationally. Benedicte Havelange presented from an EU perspective, and Jim Harper gave a US perspective, whereas Malcolm Crompton and Abu Bakar Bin Munir highlighted issues related specifically to the APEC Privacy Framework, looking at it from their own perspective. The main themes raised during each presentation, as well as in the discussion, are outlined below.

*Mrs. Bénédicte Havelange:*

#### **International Data Sharing: The EU perspectives**

Bénédicte Havelange gave an overview of the EU legal framework for data protection and privacy protection, seen in the context of other international legal frameworks in these areas. In this context Havelange outlined the aspect of the fundamental right to privacy and data protection embedded in the EU legal framework. Havelange emphasized that the harmonisation approach which is characteristic for the EU directive is first and foremost an attempt to set up common criteria for action and control measures to ensure that data collection and use of collected data are in line with the fundamental right to protection of

privacy that the directive is built upon. In this context it was made very clear that protection of privacy goes beyond data protection as well. The role of the independent supervision and the cooperation between national authorities and EU authorities was explained, as well as the main principles in the European Data Protection Directive. Several countries have claimed the overriding importance of sharing data in order to combat crime in an international context. However, it is becoming increasingly clear that collecting and sharing more and more data in order to combat crime has not proved effective. Havelange described it as a misconception and a false comfort that must be addressed not only in the EU context, but also at international level, and she saw this as an important challenge to overcome in the context of international data protection. Havelange referred to her outline in her power point slides of the existing legal frameworks in an international context and pointed out the diversity of applicable regulations and initiatives. She argued for more harmonisation of data protection regulations at an international level and mentioned that it would be a good idea to turn to more challenging frameworks for inspiration, but also emphasized that harmonisation on a trans-Atlantic level must not be done at the cost of a high level of data protection, as is seen within the EU directive.

*Mr. Malcolm Crompton:*

**Trust, Transparency and Data Governance: Challenges in the APEC privacy framework and the EU directive**

In the first part of his presentation Malcolm Crompton outlined the context in which the APEC Privacy Framework has been developed. He mentioned the different cultural perceptions of privacy and the very different ways of dealing with privacy issues in relation to data sharing and data protection within the 21 APEC member economies as one of the greatest challenges that the framework has to deal with. Crompton then moved on to talk about the challenges in terms of data sharing in an international context where different frameworks apply. He outlined the nine data protection principles in the APEC Privacy Framework and highlighted where he sees similarities and differences between the APEC Privacy Framework and the EU Data Protection Directive. It was stated that data sharing and data protection is not just a matter of protection of privacy, but just as much about control and about identifying the risks that are present, so that one can comply with the first principle that focuses on preventing harm. In this context Crompton focused on principle 9 on 'accountability'. This principle states that it is a responsibility of the 'controller' of the person's information to ensure that the recipient of the personal information also complies with the principles in the framework. It is particular in this principle that Crompton sees the strength in the APEC Privacy Framework, as compared to the EC directive.

*Prof. Abu Bakar Bin Munir*

### **Protection of Privacy: Implementation of the APEC Privacy Framework in National Regulation**

In the first part of his presentation Prof. Abu Bakar Bin Munir outlined the current status and ongoing initiatives with regard to implementation of the APEC Privacy Framework with special focus on the Asian region. In the second part of the presentation Prof. Abu Bakar Bin Munir outlined some of the issues regarding the implementation of the APEC Privacy Framework that have been the subject of discussion, both among supporters and critics of the framework. The APEC Privacy Framework does not require any particular means of implementation. It can accommodate various ways of implementation. Not all member economies may choose to implement the framework in comprehensive legislation. This aspect of the APEC Privacy Framework has been highlighted by supporters, who emphasise the flexibility of the framework as a strength. In practice it means that implementation can accommodate various methods, either through central authorities, multi-agency enforcement bodies, designated industry bodies, or it can combine such methods depending on what the member economy may prefer. This is one of the reasons why some supporters see the framework as a possible foundation for a global standard. Abu Bakar Bin Munir pointed out that this aspect of the framework has also been criticised because some people consider that the lack of an overall enforcement mechanism places the framework in a weak position.

*Mr. Jim Harper:*

### **Dimensions of Data Sharing: A U.S. Perspective**

In his presentation Jim Harper addressed the differences in perceptions of privacy and how this influences international data sharing. Harper claimed that too little attention is being paid to the human interests and values that are reflected when 'privacy' is used as a frame of reference in a data protection/data sharing context. Different human interests are at stake in different aspects of data protection/ data sharing. He outlined the context-dependent aspect of the notion of privacy as one of the greatest challenges in the discussion on data sharing. He identified five aspects of the notion of privacy that he considers important to take into account when discussing the potential risk of doing harm in relation to data sharing.

1) Protection of privacy can refer to control of personal information and the interest in privacy protection from government interference. 2) It can also refer to fairness i.e. the general interest that the data collected is accurate and does not pose a risk of discrimination to the individual from whom the data is collected. 3) Protection of privacy in data protection can also refer to personal security. In this

context privacy refers to the interest in preventing someone getting access to another person's data, for the purpose of harming others. 4) The fourth notion of privacy is to be seen in the context of the right to be left alone i.e. it refers to the interest in ensuring limitation on whom the information can be shared with and what it can be used for. 5) The fifth notion of privacy and interest in privacy protection is connected to the personal interest in liberty i.e. personal freedom to 'move' around. (Harper referred to the US-VISIT programme in this context, where fingerprints are collected from all people arriving at American borders). Harper argued that the differences in human interests at stake and the values we relate to protection of privacy in a specific context complicate the process of policy development in an international context. He argued that the greatest challenge with regard to data sharing and privacy protection lies in identifying the human interests at stake and in weighing the risk of doing harm against the benefits of collecting and storing huge masses of data (as is the case with the US-VISIT programme).

### **Discussion session I**

On the issue of harmonization, which was addressed in both Ruth Chadwick's opening lecture and in Bénédicte Havelange's presentation, it was clear that the participants agreed that more harmonisation is needed and that ethics and the further development of legal frameworks should go hand in hand in this context. International standards for data protection are required, but in order to develop such standards we need an international dialogue on the issues at stake. The differences in how rights are interpreted in the legal framework were discussed. Emilio Mordini addressed the difference between interpreting the right to privacy as a 'freedom right' (i.e. right to protection of family/private sphere) as opposed to a 'dignity right'. He argued that a legal framework, that interprets privacy protection more in the direction of a right to privacy considered in light of human dignity, will present a higher level of protection in a data context. Bénédicte Havelange agreed that the way forward may be to abandon the emphasis on the notion of privacy and turn more in the direction of interpreting data protection in the light of the right to dignity. Malcolm Crompton argued in favor of downgrading the use of the word privacy and instead using terms such as dignity, control and trust. He highlighted that the notion of 'privacy' protection tends to have a negative connotation and is associated with problems for many business enterprises. He argued that issues that are normally associated with privacy protection need to be addressed in a more positive light, where it is about improving security and improving privacy. Josef Cannataci emphasized that one of the things that may be important to consider in the future discussion on data protection is whether the notion of

privacy creates more room for diversity than it does for harmonisation. The question is whether it would be better to focus more on the notion of dignity and the protection of human dignity in the legal context, rather than on the notion of privacy and personality. The participants seemed to have very different opinions with regard to this matter. On the question about what is being done in the APEC countries in this respect, it was made clear by Abu Bakar Bin Munir and Malcolm Crompton that although there is a requirement in the APEC privacy Framework for the member economies to take action on these matters, one has to bear in mind that in many of the APEC economies, privacy is not a priority or even an issue. So despite the obligation to do something, the practice in terms of taking action towards ensuring privacy protection is a different matter when one is speaking from an APEC context.

In light of Jim Harper's presentation, criticism was raised regarding the US-VISIT programme. Jim Harper and Malcolm Crompton claimed that the use of computerized identification of fingerprints to identify illegal immigrants was too unsafe in terms of the risk of possible mismatches which can affect innocent people arriving at the American border. Michael Hardin rejected this critique by emphasizing that this is a risk that is dealt with by the system used and that several security measures are in place to avoid mistakes.

In this context Karen Maschke emphasized the importance of transparency and involvement of the public in political decisions regarding security measures that involve collection and sharing of personal data as well as transparency with regard to what the information is being used for. Jim Harper argued that although democracy and liberty go hand in hand, democracy can be detrimental to liberty, and it is a question of how much the government should interfere in the private sphere, very much depending on which of these two concepts one interprets as having the highest value.

The discussion moved to the focus on fingerprints and the particular use of this biometric technology in the US-VISIT programme. Jim Harper argued that collection of fingerprints can be seen as an indignity because of its prior use in identification of criminals. In response to this, Tom Sorell argued that fingerprinting of people arriving at borders may be undignified in some aspects, but it is not in itself an indignity if there is a security threat, provided that the process is the same for everyone, and that the programme has been developed by a recognizable democratic process. Sorell argued that, if there are democratic safeguards, many of the things we dislike could be seen as legitimate. In this context Roger Brownsword raised the issue of how we are to find an effective way of defining boundaries i.e. finding an ethical concept that will enable us to

draw the line in relation to biometrics. He highlighted that given the way the digital world is going it is no longer possible to keep anything private, and that the concept of privacy therefore may be problematic in this context. He argued that privacy may not be the most efficient concept and raised the question whether the notion of dignity may be a better term to introduce in the data protection context. It was discussed whether most people would find it easier to relate to the notion of dignity, and thereby more easily express their concerns in relation to data protection, based on their perception of what violation of dignity means. In this context Paul McCarthy mentioned the body scanner as an example of a debate where the notion of dignity was used to identify the problem. However, it was widely agreed among the workshop participants that the concept of dignity potentially poses the same problems as the concept of privacy, in terms of complexity of meanings. The participants also agreed that indignity is a very subjective notion that we will probably never agree on. Malcolm Crompton suggested taking a more pragmatic approach and focusing more on the necessity of identifying the risk of mistakes being made and the allocation of risk after the data has been collected, as an important issue to pay attention to in the attempt to identify when data collection is unacceptable.

## **Session II**

### **Privacy vis-à-vis security**

#### **(2:00-4:45pm)**

The scope of this session was to discuss the challenges in terms of cultural differences in perceptions of privacy, security and surveillance, specifically in relation to privacy enhancing technologies and personal detection technologies. In the planning of this session it was particularly important to ensure that the various approaches to issues on privacy and security were addressed in an Asian context, where the notion of privacy seems to be very different from the Western approach to privacy as a right. The four presentations in session II addressed issues related to policies regarding data collection and development of biometric detection technologies for security purposes. The speakers came from very different backgrounds, and thus issues regarding privacy and security were approached from a philosophical angle (Prof. Tom Sorell); within a policy context (Vinayak Godse); and from a more science based angle (Dr. Terence Sim and Prof. David Zhang).

As chair of the session Prof. Emilio Mordini opened the session by stating that he does not consider privacy and security as in opposition. Rather he sees the

bureaucracy with which some countries handle the collection of personal data for security purposes as the real problem, because this seems to lack transparency.

*Prof. Tom Sorell:*

### **Privacy, Intrusion and the Detection of Terrorism**

In his presentation Prof. Tom Sorell outlined a number of different approaches to privacy in liberal theory. He explained the definition of criminality and crime in the context of liberal theory and how terrorism can be seen as a life-threatening crime that can justify both reactive and preventive policing by use of general surveillance or more specific profiling. Direct surveillance and profiling can be seen as privacy-intrusive, but at the same time be considered as necessary in order to combat terrorism. However, one of the main points in Prof. Sorell's presentation was that although it may be justifiable to use profiling in preventive policing, this can be highly intrusive if not used in proportion. Profiling was said to be less intrusive as a form of identification of suspects and it has fewer costs in privacy. However, Sorell argued, the problem is that the profiling used has a tendency to create a stereotyped picture of potential terrorists, that is highly discriminating. Sorell raised the question whether profiling is more objectionable than direct surveillance, because it seems to have a tendency to create a whole population of suspects. He emphasized that intrusion into the private sphere can be both wanted and unwanted. It can be wanted because it is a way of securing the citizens against the intrusion into privacy through life-threatening crime, but it can be unwanted if it creates discrimination in terms of classification or stereotyping of certain population groups. Prof. Sorell also emphasized that it is difficult to argue for privacy and non-governmental intrusion, as we are currently living in a society where people breach their own privacy through the internet, in reality TV etc. Therefore, he argued, it is not so much whether intrusion into the private sphere can be justified in general, but rather whether the intrusion can be justified in terms of proportionality.

*Dr. Terence Sim:*

### **Privacy and Biometric technologies**

In his presentation Dr. Terence Sim focused on biometric identification in relation to privacy. He outlined a 'nightmare' scenario in order to illustrate four different notions of privacy, and how at least three of these four notions are challenged by biometric technologies. Dr. Sim emphasized that it is a mistake to automatically see biometric technologies as privacy-intrusive. He stressed the need for more focus on the privacy-enhancing or at least privacy-neutral aspects when developing and introducing new biometric systems. He went on to argue that paying more attention to such aspects is the best way forward in order to gain

more acceptance of use of biometrics for various security purposes. The use of biometrics for personal detection and identification purposes has to be convenient for the user. Among the other aspects he highlighted as important to consider in the development process is whether the introduction of biometric technology is appropriate in the specific context, or whether the choice of biometric technology will be considered more intrusive than other types for a given purpose.

Another important issue to be taken into consideration, before introducing a biometric system in a specific context, is the risk of function creep (use of DNA and retina biometrics can, for example, reveal medical conditions, and finger vein patterns can reveal blood oxygen level which all indicate something about the detected/identified person's health). Finally Dr. Sim addressed the issue of privacy intrusion in relation to accepting the introduction of biometric technologies. He emphasized that privacy is no longer the issue, as the tendency goes in the direction of sharing personal information with others on the internet etc.

*Prof. David Zhang:*

#### **Palm print Identification**

Prof. David Zhang gave an introduction to his current research in palm print identification. He described this approach as a biometric technology with very promising potential as a type of automatic personal identification system that can be used in a wide security context. Use of palm print in biometrics is promising because this print represents a rich variety of features, and all these features together create a unique identifier. Furthermore, it is possible to notice changes in the palm print and still be able to identify the same person, which can be a problem with other biometric technologies such as fingerprint.

On the issue of the development of biometric technologies in China, Prof. Zhang mentioned that there is a growing tendency among people in China to see privacy as the ability to live a life without intrusion, and with the ability to control who has access to their personal data. Prof. Zhang emphasized that he sees a lot of biometric technologies as the way forward in fighting the increasing incidence of identity fraud crime, because conventional technologies like knowledge- or token-based techniques fail to deliver the security required.

*Mr. Vinayak Godse:*

#### **Privacy and Data Protection Policies in India**

Vinayak Godse outlined the current landscape of privacy perceptions in India. He described the general perception of privacy in India as mainly relating to the physical home/ living space. He emphasized that Indian culture and society are

collectivist, and since people are living very close to each other, sharing information does not appear so much of an issue, as is the case in most Western countries. He described privacy as scoring very low on the so called the Individualism Index. He explained that the majority of people are not aware of risks such as identity theft or government surveillance.

However, as IT development creates more and more jobs in India, there is currently a change in India's privacy landscape. Godse explained that changes can be seen not only in terms of a growing awareness because of increased use of technical solutions for financial, IT and tele-services etc., but also a result of a general change in the family structure in India, which seems to be going more in the direction of individualism. Furthermore, India's IT industry provides more and more services to other countries with more firm regulations with regard to data protection. In order to protect Indian businesses' interest in going global, it has become clear that there is a need for national policies and regulation of privacy. It is in the context of these changes in India's privacy landscape that we can understand recent initiatives such as the development of biomedical guidelines and data security initiatives.

### **Discussion session II**

Bénédicte Havelange opened the discussion with a comment on Sorell's presentation. Havelange argued that the EU barometer survey which Sorell quoted in his presentation could be seen as rather simplistic, because of the leading way the questions in the survey were posed. She emphasized that there is quite a lot of evidence that profiling does not work in the fight against terrorism. Sorell partly agreed with Havelange that there are elements in the Euro barometer that are questionable in terms of whether it really gives an accurate picture of the public's attitudes to personal data sharing. However, he stressed that when carrying out such surveys, one must be prepared for answers that are orientated against privacy rights, despite the fact that one would expect a different answer. Karen Maschke, Paul McCarthy and Josef Cannataci emphasised that it is not to be expected that the public has definite perceptions of privacy. It was argued that, although the public does not seem to be worried about privacy, it does not mean that it should no longer be protected and the role of the media regarding perceptions of privacy should also be taken into account in this context. In response to this Sorell pointed out that it is true that the public perception (in the UK context) is changing and that one has to distinguish between people's attitudes to surveillance, depending on what it is used for. In this context, Sorell also pointed out that there seem to be a growing tension in the UK between the experts' and the public's opinion on what should be tolerated

with regard to preventive policing. He highlighted this as something that needs to be debated.

With reference to Sorell's comparison between profiling and surveillance, Jim Harper highlighted that in order to conduct profiling of the type Sorell was describing, one will have to do a lot of surveillance as well – and probably even more than by using direct surveillance. Therefore he found it difficult to see how there could be a clear distinction between profiling and surveillance. Sorell responded that what he was trying to outline in the presentation was the tension between profiling and surveillance. He explained that because profiling is likely to produce stereotypes, this creates a pressure for evidence-based policing, which could take form of surveillance. He therefore saw profiling and surveillance as complementary.

Alastair Campbell pointed out that terrorists perceive themselves to be involved in justified wars of resistance. Hence they will not accept the description of themselves as 'criminals'. In light of this both he and Emilio Mordini raised the question whether it is possible to adopt the notion of crime as a way of justifying surveillance etc.. The problem of the definition of law in an international context also arises here. Sorell responded to these questions during the general discussion (see the following).

Paul McCarthy commented on a survey presented in Terence Sim's presentation. McCarthy questioned him as to whether he had any thoughts about why the young people interviewed in a local survey (referred to in Sim's slides), seemed to be happy to use fingerprint for personal identification in various contexts, despite the fact that such a high percentage of them seemed to consider this biometrics technology as very intrusive. Sim responded that there is a 'know' factor related to it. As the respondents in the survey are undergraduate students from Singapore, they are already very familiar with fingerprint, as it is widely used and more and more commonly accepted in Singapore. He emphasized that a survey including a wider variety of age groups would perhaps show a different pattern.

## **General Discussion**

Session II was followed by a plenary discussion where participants and speakers had the chance to discuss issues that were not necessary directly related to a specific presentation.

Roger Brownsword commented on privacy vis-à-vis security and the distinction between preventive policing and reactive policing. He outlined the stereotypical strategies behind what he described as the Orwellian state and the Kafkaesque state. The Orwellian picture illustrates a state heavily relying on surveillance, where nothing is private. The Kafkaesque picture illustrates a state relying heavily on technology and the accuracy of the technology, and where the issue at stake is whether we trust the technology to a point where we have no further appeal. Brownsword referred to the 'nightmare' story that was outlined by Sim in his presentation, as an example of a Kafkaesque picture. He emphasized the need for clarification about which one of the two 'pictures' we are worried about when discussing privacy issues in relation to security.

Roger Brownsword also related this to Sorell's point about the current change in the UK regarding data collection and surveillance used in the battle against crime and terrorism, and highlighted that a change from a strategy that emphasises reactive policing to one that emphasises preventive policing, also has an influence on the legal process. In light of this he argued that an important aspect to take into account, when reflecting upon privacy issues in such a context, is to take a close look at what will happen to the rule of law in such a shift.

Joseph Cannataci followed up on Brownsword's comment and argued for the importance of more discussion on how we can get the legal process right, so that it fits with where the rule of law is.

Jim Harper argued that it may not be necessary to change the laws much.

Instead he argued that is important to reflect upon the specific issues such as terrorism that challenge the existing framework.

Sorell responded to the question previously raised by Emilio Mordini and Alastair Campbell regarding the definitions of criminality in a context where there is no common legal framework within which to define it. Sorell responded that most domestic legislation will capture terrorist action, and that some will also capture terrorist conspiracy, and that he cannot see any theoretical problems in locating a crime and a terrorist in the community where they are breaking the rule.

He did not see the problem lying in the lack of international jurisdiction, but rather in the fact that it is difficult to get the jurisdiction right, as people do not agree (the public, the governments etc.) on the problem of jurisdiction.

In the context of agreed principles in this area Karen Maschke and Paul McCarthy emphasized that agreement on 'the right' thing to do, is far from feasible, as one has to take into account that there are many interests (political, financial, public etc.) involved in all policy making process.

At the end of the session Simon Dobrišek raised the question of how governments can benefit from workshops like this, and which objectives should be focused on in these types of discussions. One possibility is trying to ensure an ongoing discussion on privacy and data protection, but another consideration is how this can contribute to the bigger picture. In his closing remarks to the general discussion Alastair Campbell responded to Dobrišek's question. He argued that the objective is not to set some kind of universal ethical standard, but rather to remain critical and reflective. Campbell referred to the Nuffield Council on Bioethics report on forensic DNA banks as an example of how bioethics can contribute to the debate on data collection and protection of personal data in the European context. He emphasized the importance of a critical and reflective approach in terms of discussing and reporting on the ethical issues. He argued that this is the best way forward for bioethics to contribute to the policy debate rather, than trying to set a single ethical standard.

## **Friday 3 July**

### **Session III: Is there a right to have an identity? (9:20-11:10am)**

The scope of session III was to discuss various aspects of biometrics and personal detection technology in relation to different perceptions of what it means to have an identity.

The session was chaired by Professor Leonardo de Castro (Centre for Biomedical Ethics, National University of Singapore), who introduced the session by illustrating some examples where the identity question has been shown to be highly relevant in relation to the use of biometrics. The first example referred to a presentation by scientist doing research on how particular features in human behavior are expressed in scans of the brain. In his presentation the scientist expressed the hope that in the future it would be possible to install brain scanners in airports, so that it would be possible to identify terrorists from the images provided by the scanner.

The second example referred to a person who asked his secretary to sign his paycheck in his absence. After a few times, when the secretary had signed the paycheck in the person's name, the original signature of the person was no longer associated with the person's identity and he was unable to identify himself by the signature. The chair's introduction was followed by the two presentations in session III, which reflected on the issue of the right to identity from a philosophical rights based approach (Roger Brownsword) and from a scientific

approach focusing on personal identification and identification of ethnicity by the use of DNA profiling (Eric Yap).

*Prof. Roger Brownsword:*

### **Is there a Universal Right to Identity?**

In his presentation, Prof. Roger Brownsword addressed two questions: Are there universal rights? And, is there a right to identity?

Taking an ethical rationalist approach (that of Alan Gewirth) Prof. Brownsword walked the participants through the argument, that from purposive agency one can construct an idea of generic rights. An intermediate step, that of creating the community of rights, Prof. Brownsword argued, was the key in understanding our obligations and duties to one another, and our correlative rights, as a matter of reason. All agents are entitled to the benefits of this community without discrimination, and therefore this is the basis of fundamental and universal rights. Applying this to the second question Brownsword asked whether we should carry ID cards. He argued there is no foundation for claiming a right to identity as such, because rights themselves presupposed that we are all equal within the 'agency commons' (community of rights). But that is not to say that we do not have different needs within this community. He then went through a series of other questions in which the use of technology may be problematic with regard to the having of rights.

A question regarding the theoretical foundation for the agency commons (community of rights) was raised by Jacqueline Chin, who asked how the people in power in the society would react to the idea that one is to respect the rights of other people. In reply, Prof. Brownsword emphasized the rationality lying behind the recognition of the 'agency commons', and that the logic of their agency compels them to think this way.

*Dr. Eric Yap:*

### **Ethnicity and Identification by DNA profiling**

The presentation focused on the question: What does it mean to have a genetic identity?

Dr. Eric Yap presented from his 'two identities' a) from his identity as a geneticist, from which he would outline what genetic identity means in relation to his research on genetic profiling; and b) from his identity as a citizen and consumer, from which he would outline what it means to have genetic privacy as consumer and citizen. In the first part of the presentation Dr. Yap outlined the most common uses of DNA profiling such as profiling of gender, forensic identification, testing of relationship (pedigrees and family relations), missing person investigation and genealogy and ancestral studies. The aspect of personal identity was addressed

in the specific research context of studies on whether DNA profiling can be used to tell us something about the relationship between different population groups. Yap outlined his studies on the Y-profile of specific population groups to find out whether DNA profiling can be used for identification of ethnic groups. It was emphasized that although there are some patterns to be found the research results also showed that within the same ethnic group the Y-profile can vary a lot. He highlighted that when analyzing genetic information this way there is potentially the risk of finding out information about population groups, family members or ones own genetic profile (issues around health etc) that may not be desirable. Furthermore there is the potential issue of consequences for health insurance etc. This led to the second part of the presentation that dealt with genetic information used in ID cards.

Here, Dr. Yap focused on genetic identity with emphasis on 'my identity as a citizen'. The genetic information contained in the recently introduced identity card in Singapore was outlined. Dr. Yap showed a copy of an identity card to illustrate the biometric features applied and what kind of information about the individual it is possible to extract from this type of ID card (seen from a geneticist's perspective). This included information about health and health risk. The specific biometric feature in this ID card is a fingerprint, but the card also includes a number of other features about the health conditions such as information related to the genetic identity of the individual. Yap described genetic information as a qualitative type of biomedical information for which existing ethical and philosophical frameworks may be usefully applied and adapted.

To a question from Emilio Mordini on whether he believed that it is valuable to have an identity card like the one in Singapore, he responded that looking at it from a scientific point of view he thinks it is relevant to have the card, and although he was not in a position to dissect the ethical issues that may be raised in this context, he emphasized that the ID card was generally widely socially accepted.

### **Discussion Session III**

The following discussion focused on how 'identity' is to be understood in the context of human rights theory. Alastair Campbell asked whether measures that seem to reduce human beings to numbers or a specific stereotype could be seen as going against the key notion of the community of rights (referred to as agency commons). He argued from the idea of a right to a non-reduced identity or a right to a complexity of identities. It was discussed whether identity was referred to in different ways and whether one could refer to an 'identity right' as a right to uniqueness, rather than looking at identity in the context of individuality.

Brownsword responded that what we make of ourselves as agents is less

relevant in this context (i.e. the community of rights). The community of rights (agency commons) claims that we are all identical as agents, but it is just the beginning of what we are as individuals.

Eric Yap highlighted the importance of keeping in mind that technology may enrich individuality and furthermore that genetic features already make the individual unique.

Malcolm Crompton suggested taking a more pragmatic approach by looking at the issue of privacy protection in relation to ownership rights. Josef Cannataci suggested looking at identity and personality as interlinked, and how these issues are dealt with in national implementation of the European directive of data protection.

## **Session IV**

### **Personal Data and the Human Body: Rights and Ethics**

**(11:40am-1:00pm)**

Session IV was arranged as a panel discussion, with two invited panel speakers, Colin Minihan (Chair of the APEC sub-group on privacy, Australia) and Michael Hardin (Senior advisor, U.S. Department of Homeland Security, US-VISIT programme, USA). The two panelists presented their viewpoints and commented on some of the main issues addressed throughout the workshop. The panel presentations were followed by a plenary discussion addressing: a) issues around different types of privacy and differences in values of privacy can be reflected in an international privacy framework on data sharing; and b) different viewpoints with regard to whether personal data related to the body differ from other types of personal data with regard to data protection and international data sharing.

#### *Colin Minihan, Panelist commentary (1)*

Colin Minihan gave a brief overview of the current initiatives in a domestic context, where he highlighted a number of existing laws in Australia regulating privacy. In this context he mentioned that discussions with regard to expanding the existing regulatory framework to the area of biometrics are taking place in Australia. Minihan then moved on to talk about privacy protection in the APEC context. With reference to Ruth Chadwick's presentation Minihan described the development of the APEC privacy framework as a pragmatic approach, focusing more on the 'cultural dialogue' model and less on the 'human rights' model. Human rights are embedded in the framework, because of the close link to the

OECD guidelines, but the framework is not rights based in the same way as the European Directive on Data protection. He emphasized the objectives of the APEC privacy guidelines as a matter of finding a common ground and a practical approach to data sharing and protection of personal data that embrace or comply with the cultural differences among the 21 APEC member economies. The framework was described as a minimum-apply-framework, where focus is being put on similarities. He emphasized that he does not see a realistic possibility of a dialogue on basic privacy perceptions taking place within an APEC context at this point. Minihan described the APEC Privacy Framework as an approach that seeks to take some basic principles that underpin what is happening in the APEC region and apply these in the best practical way in order to ensure the cross border flow of data. With reference to the discussion in session I and II regarding the need for an international standard/ harmonised framework, he emphasized the necessity for more dialogue and emphasized the APEC framework as an example of a pragmatic 'solution' to meet the challenges related to trans-Atlantic and international data sharing.

*Michael Hardin: Panelist commentary (2)*

In his presentation Michael Hardin focused on the issue of personal data and privacy as it is dealt with in the US-VISIT programme. US-VISITs task is to provide identity service for various agencies within the US, including border control. The practical task is to provide identity information fast but without compromising on privacy issues. He outlined how the central privacy policy is put into action in the US-VISIT programme and the measures taken to ensure transparency for all visitors and American citizens. Furthermore, he outlined the procedures in place for dealing with cases where people have been held back for wrong reasons. He explained how dialogue with the citizens on privacy issues is an important instrument in ensuring the program's further development. He then spoke about how data link to the body. He outlined the basic ideas behind a test programme done in cooperation with Canada, on exchange of biometric information – in this case fingerprint. Michael Hardin explained how practical measures are in place to ensure protection of privacy of the person whom the fingerprints belong to. This includes attaching fingerprint information to a number, rather than directly to the identity of the person. Hardin highlighted this as an example of how biometric data can be handled in a secure way, and claimed that such use of biometric data provides more protection for the individual than usual ways of exchanging data would do.

To conclude, Hardin mentioned that he does not see many differences between the American approach and that of other countries (for instance countries in

Europe), either with regard to the purposes for which the information is collected or with the way information is handled.

**Discussion:**

The two panelist presentations were followed by a general discussion. The first theme addressed concerned biometrics. Several participants and speakers emphasized the need for a framework specifically addressing biometrics and personal data related to collecting and sharing of biometric data. Bénédicte Havelange suggested that biometric data deserves special attention because it differs from other types of data, in that it relates directly to the body. Colin Minihan was more in favor of working towards general guidelines that can then be discussed within more specific areas depending on what type of information one is dealing with and depending on interlinks with other frameworks.

The discussion moved to the question on how to reach some level of common understanding, as a point of departure for a discussion regarding development of international standards on privacy protection in relation to biometrics. The differences in the human rights based approach taken in the EU directive and the pragmatic approach taken in the APEC privacy framework were further addressed. Colin Minihan, Bénédicte Havelange and Joseph Cannataci all highlighted a multiple track approach as the way forward, rather than arguing for either one or the other framework. Emilio Mordini closed the general discussion with a suggestion that we could use 'liberty' as the common ground for discussion. He argued that consensus regarding whether to argue from the notion of 'dignity' or on 'personality' when approaching the issue of privacy protection would not easily be reached. Despite these disagreements, he argued, there seemed to be a common ground in the idea of 'liberty'. In light of this he suggested we use liberty as the key notion to evaluate the questions about security and privacy.

Alastair Campbell closed the workshop by briefly summing up some of the main outcomes. With reference to the many disciplines represented at the workshop he emphasized the importance of dialogue in an area that is not only ethically and politically sensitive, but also entails discussing data and data sharing in different ways depending on which discipline one is approaching the issues from. The biggest challenge in this context is perhaps to understand the different 'languages' in terms of style, approach, assumptions and methodology represented by the various disciplines/professional groups present. In light of this, the workshop had shown that the way towards understanding goes through listening to the different approaches and thereby enabling the participants to

'compare notes' – and in this case in a context that is not merely a European one.

## Summary and Conclusions

The Singapore workshop was the first out of two problem solving workshops taking place in the HIDE project. As highlighted in the introduction, the main aim of this type of workshop is to identify problems and possible small steps towards solutions. In the case of the Singapore workshop the aim was to identify and discuss some of the ethical and legal challenges that the APEC privacy framework may pose to the EU data Protection Directive and in this context also to identify and discuss potential value conflicts related to key concepts such as privacy, security and identity. In the following we have listed the main themes addressed during the workshop and highlighted some of the suggestions for 'small step solutions' that were discussed.

- **Dialogue as a model for progress towards harmonisation**

Harmonisation and standards for data sharing on a wider international level are needed but must not compromise the protection of personal data.

The workshop confirmed that dialogue is important in terms of identifying and understanding cultural and regional differences in the way basic concepts such as privacy are dealt with. It was clear from the presentations focusing on privacy in an Asian context, that some of the values associated with privacy in a Western context are not considered as important in some of the Asian countries.

It was generally agreed that some of the biggest ethical and legal challenges in relation to international data sharing lie in the differences of interpretation of privacy. The challenge therefore lies in finding a way for a fruitful dialogue on the issues that are at stake in data protection with regard to protection of the private sphere. Whether this is by encouraging more dialogue about what privacy means, or whether it means turning to other spheres/contexts in which privacy is also discussed, or perhaps turning to different concepts when interpreting existing legal rights, was left as an open question.

- **Identifying ethical issues in relation to biometrics from a 'privacy' or a 'dignity' perspective.**

The theme was addressed specifically in relation to the discussion on how privacy is to be interpreted as a right within the context of the EU Directive on Data Protection. However, during the discussion it became clear that that the

notion of privacy is problematic in the context of both the EU Directive on Data Protection and the APEC Privacy Framework. The question of whether 'dignity' would be a more effective key concept when evaluating the ethical issues related to biometric technologies applied for security purposes was quite fully discussed. There was general agreement among the workshop participants that 'privacy' is too complex a notion to use as an ethical foundation for an evaluation of the values at stake. The idea of 'dignity' as foundation for evaluation was not presented as a *solution* to the problem, but was mentioned as a concept that might be more useful.

- **Identity interpreted as individuality or uniqueness**

This theme was raised in session III. Although the participants disagreed on whether identity should be interpreted in terms of rights, it was clear from the discussion that more attention needs to be paid to the issue of identity and how this relates to protection of privacy in the context of biometrics.

- **Transparency, public perceptions of privacy and democratic decision making**

This theme arose in session II in relation to the discussion on preventive and reactive policing. There was a general agreement among the participants that there is a need for more debate on the various interests at stake in the policy making process, as well as for more focus on public perceptions of privacy.

- **Finding a common ground for identification of the human interests at stake in relation to data sharing and biometric identification used for security purposes.**

This theme was addressed both session II and session IV, and it was generally agreed that in terms of working towards more harmonization in international frameworks, it is necessary to take a multiple track approach that can take into account the underlying differences in interpretations of concepts such as privacy, dignity and identity. Liberty was suggested as a key notion that perhaps could be used as common starting point for evaluation of questions regarding security and privacy.

By  
Lisbeth Witthøfft Nielsen (CBmE)  
and  
Professor Alastair V. Campbell  
Centre for Biomedical Ethics,  
Yong Loo Lin School of Medicine  
National University of Singapore