Closed Session 2012

Meeting Report

Privacidad y tecnología en equilibrio

34° Conferencia Internacional de Autoridades de
PROTECCIÓN DE DATOS Y PRIVACIDAD

Thursday 25 October

Welcome

The Chairs of the Closed Session, Felipe Rotondo (URCDP, Uruguay) and Jacob Kohnstamm (Dutch DPA, Netherlands / Chairman Executive Committee) welcomed the members of the International Conference to the Closed Session. Mr. Kohnstamm explained the order of business for the two day meeting, as well as the new format of the Closed Session: one day devoted to discussions on a single issue and a half day for the so-called "internal affairs".

1. Minutes Closed Session 33rd International Conference

The minutes of the Closed Session during the 33rd International Conference in Mexico City were adopted without change.

2. Accreditations

Since the last conference, twelve authorities have applied for membership or observer status. Following the recommendation of the Executive Committee, the Conference agreed to accept the following new members and observers.

Members

- Colombia Superintendence of Industry and Commerce of Colombia
- Korea Personal Information Protection Commission (PIPC)
- Peru National Authority for Data Protection
- Saxony (Germany) - Saxon Commissioner for Data Protection (SCDP)
- Serbia – Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti (Commissioner for Information of Public Importance and Personal Data Protection)
- Tunisia - Instance Nationale de Protection des Données à Caractère
- Costa Rica - Agencia de Protección de Dados de los Habitantes
- Norway - Datatilsynet (Data Protection Authority)

Observers

- Association Francophone Des Autorités De Protection Des Données Personnelles (French-Speaking Association of Personal Data Protection Authorities)
- Organization of American States
- Korea National Information Society Agency (NIA)
- Ecuador Dirección Nacional de Registro de Datos Públicos (DINADARP)

Japan furthermore announces an upcoming change in their legislation. This might mean they need to reconsider their current observer status to the Conference in the year to come.

3. Profiling

Upon invitation of the Executive Committee, four external speakers take part in the discussions on the first day of the Closed Session to start off the discussion by informing the members on the use and application of profiling from their specific background and expertise. The four external guests are:

- Lisette van der Hel, Strategic Advisor Compliance Risk Management at the Dutch Tax Authority and Professor of Public Governance at Nijenrode Business University
- Jim Dempsey, Vice President for Public Policy, Center for Democracy & Technology
- Philip Evans, Senior Partner & Managing Director and BCG Fellow at the Boston Consulting Group
- Fred Cate, C. Ben Dutton Professor of Law, and Director, Center for Applied Cybersecurity Research – Maurer School of Law, Indiana University

Lisette van der Hel

Mrs. Van der Hel discusses the use of profiling by the Netherlands Tax and Customs Administration (NTCA). Until recently, a more traditional approach was taken when selecting and checking tax returns for possible errors or fraud. The NTCA relied merely upon the professional judgement of staff to identify those returns that required further scrutiny, for large businesses, SMEs and individuals. In today's society, that is no longer feasible, also because of the growing complexity, digitisation and globalisation. Therefore, the NTCA has introduced a Compliance Risk Management (CRM) Strategy (knowing > choosing > acting). CRM is a holistic approach in which the NTCA makes substantiated choices, what interventions could be used effectively to stimulate compliance and prevent non-compliance (so to influence taxpayer behaviour), based on the knowledge of compliance risks and behaviour of all taxpayers and related to the available capacity. Profiling plays a role – in the "knowing" stage - within this strategy for both SMEs and individuals. It helps to create knowledge about large volumes of taxpayers and to differentiate in their treatment.

The basic information used for profiling by the NTCA is the tax return submitted by the taxpayer. The content thereof is verified with third party information available for the NTCA. Much of this information is exchanged in an automated way, for example records from the social services. The NTCA also cooperates internationally with several organisations in order to obtain relevant information. The policy of the NTCA is not to gather as much data as possible, but to make smart use of the data within the CRM strategy: CRM is a knowledge-based approach and not a data driven approach. With the introduction of profiling, the NTCA intends to select subjects or objects from a complex reality based upon a limited set of attributes. This is a more objective selection process (especially if profiles are made by the computer), than just a selection by a natural person on the basis of his/her personal experience. The profile contains a set of correlated data that identify and represent a data subject or a specific group or cluster. To make an effective use of these profiles, it is necessary that professionals – not involved in creating profiles - apply the results of the profiling process.

Mrs. Van der Hel stresses the need for reliable profiles (because data are taken out of their original context and put in another context) . To achieve that, it is necessary to validate both the underlying methodology and the results of the profiles before further use can be considered.

Jim Dempsey

Mr. Dempsey makes a distinction between different forms of profiling: criminal profiling or racial/ethnic profiling are not at the core of the discussion now. The focus should be profiling in relation to big data and the techniques of data mining. However, the same basic themes apply to all forms of profiling: fairness, reliability and due process. According to Mr. Dempsey, profiling is to create, discover or construct knowledge from large sets of data and to find patters of correlation. It is a use of information technology to harness statistics, algorithms and other tools of mathematics to improve decision making.

The applications of profiling and data mining are manifold. Two examples were discussed: the health care sector and border control. In the health care sector, profiling is used to ensure better better care with lower risks, while at the same time limiting costs. Traditionally, the medical profession took little measurement of the outcomes of what works and what not. This changes now that more information is being collected, used and analysed, in order to develop guidance and to overcome bad practices and patterns. It is much easier to identify correlations in data and to gain new insights in the workings of medical treatment or medications.

As to border control, there is also a clear need to make use of profiling techniques, albeit to limit the amount of staff (and space) needed to accommodate millions of passengers on a daily basis. Profiling for both people and cargo helps to quickly identify the risks. The patterns for screening are based on trend analysis, officer experience and raw intelligence. Profiling alone is thus never the reason someone is denied access to a country because human intervention is always part of the process. However, by using profiling, also people who are not on a watchlist or have not been previously suspected of any wrongdoing, may be identified as requiring more detailed scrutiny.

Mr. Dempsey subsequently discusses the practice of profiling and the underlying algorithms in relation to data protection. He recalls the fair information practice principles, that should be applied to all profiling operations as well. However, the principle of data quality values an update. Modern techniques and especially well written algorithms now are able to work even with databases containing 'dirty data'. Data quality should thus not only see to the input of data into a database, but at least also include the quality of the output.

The final remark of Mr. Dempsey is directed at data protection authorities. They should much more be aware of technology, know how things like profiling really work. Also, they should be aware of what is happening in the 'real' world and let the lawyers and policy makers work together with academia.

Philip Evans

As the quality of data improves, the possibility to discriminate increases, states Mr. Evans. Businesses try to create segments of customers, where their activities could be focussed on. This is what companies have always been doing. In the past, the segments reflected groups of customers with similar characteristics, but due to the evergrowing amount of available data, the charactistics become more specific. The segments therefore quickly become segments of one. Companies are quite reluctant to talk about what they are doing regarding profiling. There is a lot of concern about the boundaries in which they are free to carry out these activities and the backlash from both consumers and regulators. Therefore, they play it safe, in order to avoid reputational risk. They also claim this inhibits innovation and that thus consumers do not get all the benefits they could have.

The main purpose for businesses is to 'own the customer'. This means having the customers' profile or at least having a better profile than the competitors. It also means a shift of competitive advantage to the companies who are closest to the customer (from the producers

originally).
Consumers make trade-offs: they seem willing to give information about themselves up when they can gain something in return. There is a lot of variation in how people make this trade-off, depending on who they are, what information is to be shared and with who, and how this information is being used. In the business world, the basic understanding is that profiling is a transaction: goods are supplied (personal data) and goods are given in return (coupons, discounts, promotions, etc.). The nature and value of the transaction is variable of course, but trends are visible. Enquiries show that there are different kinds of information: social network information, health records, financial and credit card data are considered to be of high value, while age and gender are much less valuable to consumers. People have little concern about sharing information with certain types of companies like retailers and cable network operators, where people are more reluctant when it regards search engines, online shops and social network sites. These results have been scientifically validated, proving as well that trust is an essential factor to enable to the economic trade-off. Trust also depends on regulatory action. However, still there is lots of variation about the way people are open for such trade-offs. Another important point is that the trade-off should be made free from coercion, well-informed and with the explicit choice of the consumers.

Fred Cate
Mr. Cate is first of all concerned about the term profiling. It is a 1960s/1970s term, suggesting the aggregation of data that are stored or organized by individual. While this does occur frequently, the term may misapprehend the nature of modern data analytics and ignore the future trajectory of data mining. Many – perhaps most – inquiries of datasets for what might be considered profiling purposes are not evaluating specific individuals, but rather look for data elements that respond to specific enquiries.
The question is raised why private sector entities profile? This is for a number of reasons.

- data hygiene and matching – there is a big amount of difficulty in managing databases, with many different ways used to record data, including transcription errors and inconsistencies. Proof: in 2011 5% of US mail was undeliverable, because the address information was incorrect. Data matching is a surprisingly difficult and error-prone process. Up to 70% of data can accurately and rapidly be integrated in databases, the rest needs human intervention. More data and consistent profiling make matching easier and faster. However, with erroneous data the risks of erroneous results increases.
- risk management – identify and verify applicants for new services or goods, including matching of individuals against certain watch lists (i.e. anti-fraud). This works also the other way around: if someone is not qualified, don't bother them with your offer. In that example, profiling is used to remove persons from a bigger list.
- regulatory compliance / preference management – irrespective of lawfulness, if the private sector has certain data, the government may have it as well. Many data collection and reporting requirements to prevent several illegal activities (including money laundering and terrorism) increasingly requiring profiles. Relates to know-your-customer rules and the reporting of suspicious transactions. Customers nowadays are generally known through the company's databases, preferably by combining the databases of several affiliates to provide a single user experience.
- Marketing – economics are in favor of profiling, because personalized or individualized offers do work. Targeted marketing reduces costs and increases yield, while it also facilitates market entry and innovation. Profiling allows companies to make it easier to match offers and demands.

- Research – there are massive volumes of data available, which provide tons of information for researchers. This could lead to new products, new services and other things, both external and intra-company. To analyse all this granular data allows for researchers to discover trends and correlations. Also profiles become much more specific then the previous generalities (white male, 45-50 years old, living in the west, thus likely to buy X). Even if data is de-identified (no name attached) it is technically quite easy to re-attach the name given all the other specific data related to that person that are available. For example, de-identified genotypic information does not exist. Genome information is just too specific for the individual. How to deal with the data protection elements of that, also in relation to marketing? Is offering a life saving drug to the said person marketing? Should it be hindered by privacy and data protection rules? There are many questions unanswered in relation to the use of personal data.

Mr. Cate confirms that private sector profiling is not limited to companies, but is also used by governments, NGOs, political parties and others. The same source data serve many uses. Data sharing, aggregation and retention are critical. Data do not always need to be identified, but usually need be be identifiable. Regulators have a clear role here: just because it is possible to identify someone doesn’t mean we should also allow that to be done.
The use of the data is key: as soon as individuals are affected regulatory oversight could come in. The use is also distinctive in answering the question what kind of regulation is needed. Some uses would require an explicit opt-in, where others may not even value an opt-out.

Highlights from the debate

- Transparency is important about both the use of profiling as such and the reason why profiling is used. The full details of the profile and/or the underlying algorithm need not (always) be public, also in order to ensure that profiles cannot be circumvented deliberately.
- Profiling in itself contains a risk of discrimination. Individuals should therefore have the possibility to challenge the assumptions under which they are being judged, following the outcome of profiling.
- Establish legitimacy (both the need for a legal ground as a fit within a democratic society) and effectiveness before making a start with profiling, followed by a continuous evaluation.
- Big data are here to stay. That brings about other issues, including data quality, but also data security. Anonymisation becomes a little less important, also because it is more and more difficult to truly de-identify personal data. Pseudonymisation is something that needs to be considered more.
- Governments are starting to rely more on profiling and algorithms in their decision making as well. The results of data analysis are being presented as objective decisions, but do have effects on the citizen. Therefore, the democratic control on these systems should be much stronger and also involve the individual more than is the case now, next to the existing supervision by data protection authorities.
- Ensure a separation of powers, for example by making a distinction between those entities who have the data and carry out the profiling, and those who subsequently use the results of the profiling. Independent supervision should be available for all stages: the data collection, forming the profile and the application of the profile.

- It is the tasks of the regulators and supervisors to analyse what is going on in their country. They need to acknowledge the added value profiling may have, but at the same time the users of profiling need to accept that regulators and supervisors may put limits on the ways profiling can be applied. The data holders need to be kept aware of the basic principles like proportionality and transparency to individuals.
- Privacy can increase trust in profiling. Commitment to privacy from the data holders – both public and private – as well as regulating what can be done with the profile can enhance individuals' understanding, trust in, and acceptance of profiling.
- In general companies tend to stick to their own databases as long as they are market leader. Their large database will then give them a competitive advantage. However, competitors are more likely to pool their data and so create a better database, in order to take over the competitive advantage.
- Distinction should be made between the use of data that have little use for society but a huge impact on the individual (for example data regarding sex life) and data that are of little importance to the individual, but may have large advantages for society (for example genome information, that could be helpful in saving lifes).
- Profiling is an issue that should be of major concern to regulators and supervisors around the world. We are profiled in such ways that have real (adverse) effects for us, without knowing where it comes from and what we can do about it. Privacy often loses out, certainly when the government becomes involved. The focus and attention of the data protection authorities should be awarded much more towards these issues.

Friday 26 October

4. Reports

Executive Committee

The report of the Executive Committee contains an overview of the work done in the past year. The Chairman of the Executive Committee informs the members about the meetings of the Committee that took place and thanks especially the FTC (United States) for the work done in relation to the accreditations of new members and the OIAC (Australia) for the coordination of the representation of the Conference with other international organisations. He requests that the members who represent the Conference with other international organisations will also ensure a brief written report is sent to the Executive Committee after the meeting of the organisation in question.[1]

Mr. Kohnstamm also informs the members that the Committee has decided that a permanent website will not be reconsidered. It appears the previously discussed option via the OECD is not possible and also practicalities like the needed time and money are not easily solved. New Zealand proposes to involve the full membership and to investigate if one of the members would be willing to host a permanent conference website. The Executive Committee will ask the membership if anyone is interested.

Finally, Mr. Kohnstamm thanks the Mexican delegation for the work done as member of the Executive Committee. They will be replaced by the representatives of the 2013 Host Authority. The report is adopted.

[1] international@cbpweb.nl

International Working Group on Data Protection and Telecommunications (Berlin Group)
The German delegation presents on behalf of the Berlin authority the report of the International Working Group on Data Protection and Telecommunications. The report was adopted without discussion.

5. Working group on international co-operation and co-ordination

Framework for International Enforcement Cooperation
The delegations of Canada and the UK present the outcomes of the Montréal meeting on enforcement coordination and cooperation, prepared by the workgroup of the Conference installed in 2011. They hope to present a full framework for enforcement cooperation by the end of the year. The reports that are on the table, and especially the draft framework, are to be a living document, to be updated as and when necessary. It is suggested to include a recommendation for authorities to coordinate with one another and to nominate a a lead authority in the event of a joint investigation Also, it needs to be clear beforehand to the best possible extent what information can and cannot be disclosed (both to each other and the general public) in the course of a joint enforcement action.

A discussion took place on the ways to determine who can be considered as enforcement authorities in the sense of the International Conference and what requirements should be applicable. There is a difference between the application requirements for the International Conference and GPEN, also due to the nature of the latter. GPEN was always intended as an open, inclusive network, primarily intended to make it easier to identify those authorities who have enforcement powers. Further cooperation in concrete cases is either bilateral or multilateral and would in any case take place – on a voluntary basis – outside the network.

Several delegations request that the Executive Committee discuss the issue of how to bring the enforcement cooperation and coordination forward, also in relation to the existence of GPEN and the requirements for membership of both the Conference and GPEN. The Executive Committee will report back to the 2013 Conference.

The Conference furthermore decides that a second meeting on enforcement coordination and cooperation should be held in the first half of 2013. The FTC offers to host such a meeting *en marge* of the IAPP Washington Conference in March 2013.

Discussion paper on public sector cooperation
Canada introduces its paper on the need for more coordination in the public sector. This builds on the experiences already gained by the cooperation on private sector issues. However, many of the authorities that are member of the Conference, also have powers in the public sphere. Also here, we can learn from each other, by sharing best practices and positions. Our governments and security services already work close together, so it is about time the supervisory authorities take this step as well.

The Conference supports the Canadian position and agrees to reflect on a suitable way forward. Of course, there will be some hurdles to overcome, but a solution could and should be found. Canada is asked to present a more detailed proposal to the Conference in 2013 for a further debate and possible decision making.

Canadian-Dutch Enforcement Cooperation

The Canadian delegation presents the lessons learned from a joint enforcement action from the Dutch and Canadian authorities into an American-based IT Company. Five lessons were presented:

1. Getting comfortable – getting to know each other and work methods
2. Playing positions – have each play to their relative strengths
3. Showing solidarity – speak with one voice and commit at the highest level
4. Being strategic – pick the right investigations and the right partner(s)
5. Developing transborder tools to reduce the need for specific MoUs for each investigation or cooperation.

Global Privacy Enforcement Network (GPEN)

New Zealand gives an update on the items discussed in the GPEN face-to-face meeting that was held on 23 October 2012. The main points on the agenda were the proposal to organise a joint Internet Sweep Day in 2013 and to develop a web-based tool for better enforcement coordination, were authorities could indicate if they wish to cooperate on investigations with possible cross-border elements. The members of the Conference were also invited to join GPEN if they have not yet done so.

6. Resolutions

Two draft resolutions were presented to the members: one on cloud computing, introduced by the German delegation, and one on the so-called future of privacy, proposed by the Dutch delegation. Both resolutions were adopted after a short discussion, with minor amendments to the texts.

7. Any Other Business

The Portugese delegation announces that the Spring Conference of European Data Protection and Privacy Commissioners will take place on 15-17 May 2013 in Lisbon.

8. Host 35th Conference

Poland presents its candidacy to host the 35th Conference in 2013 in Warsaw. After a short film showing the highlights of Warsaw, the Conference unanimously agrees to award the 2013 Conference to Poland. The meetings will take place in the week of 23-27 September 2013. More details will follow in the course of the year.

Mr. Kohnstamm congratulates the Polish delegation and confirms they will join the Executive Committee for the next two years.

9. Closing remarks & Uruguay Declaration

At the end of the meeting, Mr. Kohnstamm reads out the text of the Uruguay Declaration, reflecting the discussion on profiling on the first day. The Declaration is signed by the Chair of the Uruguayan authority and the Chairman of the Executive Committee. The Declaration will not be put to a vote, but is simply a statement on behalf of the two chairs. The Executive

Committee will prepare a follow up resolution on profiling to be discussed and voted during the 2013 Closed Session.

Finally, Mr. Rotondo and Mr. Monteverde (the outgoing and incoming Chairmen of the Uruguayan authority) thank all members for their participation in the Conference. They also thank the members of the Executive Committee and their respective staffs for the hard work done in preparing this first Closed Session under the new format.

***

List of participants

Name	Surname	Country	Organization
Ken	Anderson	Canada	IPC - Ontario
Luis	Andrade	Portugal	CNPD - National Data Protection Commission
Carmen	Baggaley	Canada	DPA
Flavia	Baladan	Uruguay	AGESIC
Angels	Barbara	Catalonia	Catalan authority of data protection
Marcelo	Bauzá	Uruguay	AGESIC
José	Bermúdez	Colombia	SIC (Colombia DPA)
Chantal	Bernier	Canada	CPVP / OPC
Paul	Breitbarth	Netherlands	College Bescherming Persoonsgegevens
Julie	Brill	United States	FTC
Silvia	Bunier	Canada	CPVP / OPC
Giuseppe	Busia	Italy	Garante Protezione Dati
Giovanni	Buttarelli	EU	EDPS
Silvana	Caccioti	Uruguay	AGESIC
Filipa	Calvao	Portugal	CNPD
Henry	Chang	Hong Kong	The Office of the Privacy Commissioner of Personal Data - Hong Kong
Allan	Chiang	Hong Kong	The Office of the Privacy Commissioner of Personal Data - Hong Kong
José	Clastornik	Uruguay	AGESIC
Estella	Cohen	Canada	Office of the Information and Privacy Commissioner - Onterio
Carol	Cowan	Canada	CPVP / OPC
Isabel	Cruz	Portugal	CNPD
Christopher	Docksey	EU	EDPS
Isabelle	Falque - Pierrotin	France	CNIL
Santiago	Farre	Catalonia	Catalan authority of data protection
Rafael	García	Spain	AEPD - Agencia Española de Protección de Datos
Bruno	Gencarelli	EU	European Commission
Urszula	Goral	Poland	DPA
Christopher	Graham	United Kingdom	ICO
Clara	Guerra	Portugal	CNPD
José A.	Guevara Bonilla	Ecuador	Dirección Nacional de Registro de Datos Públicos
Endre	Gyozo Szabo	Hungary	DPA
Yoram	Hacohen	Israel	ILITA - The Israel Lan Information and Technology Authorithy
Dominique	Hagenauw	Netherlands	College Bescherming Persoonsgegevens
Thuer	Hanspeter	Switzerland	DPA
Billy	Hawkes	Ireland	DPC
Jimena	Hernández	Uruguay	AGESIC
Markus	Heyder	United States	FTC
Peter	Hustinx	EU	EDPS
Rosario	Ierardo	Uruguay	AGESIC
Yoichiro	Itakura	Japan	Consumer Affairs Ageney

Name	**Surname**	**Country**	**Organization**
Janis	Kestenbaum	United States	FTC
Jacob	Kohnstamm	Netherlands	College Bescherming Persoonsgegevens
Sadanobu	Kusaoke	Japan	Consumer Affairs Ageney
Sophie	Kwasny	France	Council of Europe
Hagen Thomas	Ljegadt	Norway	Norwegian DPA
Carlos	Lobo	JSB Eurojust	CNPD
Drudeisha	Mahdub	Maritius	Interpol
Mariya	Mateva	Bulgary	DPA
Magaly	McLean	Costa Rica	OAS
Peter	Michael	EU	JSB Europol
Hiroshi	Miyashita	Japan	Consumer Affairs Ageney
Cecilia	Montaña	Uruguay	AGESIC
Federico	Monteverde	Uruguay	URCDP
Bárbara	Muracciole	Uruguay	AGESIC
Sean	Murray	Canada	Office of the Information and Privacy Commissioner for Newfourdland & Labrador
Laura	Nahabetián	Uruguay	AGESIC
Igor	Nemec	Czech Republic	DPA
Chris	Olsen	United States	FTC
Alfonso	Oñate	Mexico IFAI	Secretario de Protección de Datos IFAI
Vanna	Palumbo	Italy	Garante Protezione Dati
Virginia	Pardo	Uruguay	AGESIC
Iñaki	Pariente	Basque Country	Agencia Vasca Protección de Datos
María Verónica	Pérez Asinari	EDPS	European Data Protection Supervisor
Attila	Péterealvi	Hungary	DPA
Jörg	Polakiewicz	Germany	Council of Europe
José Álvaro	Quiroga	Peru	APDP - Autoridad Nacional en Protección de Datos Personales
Florence	Raynal	France	CNIL
Aleksandar	Resanovic	Serbia	DPA - Commissioner
Shona	Ritchie	EU	JSB Europol
José Luis	Rodríguez	Spain	AEPD - Agencia Española de Protección de Datos
Beatriz	Rodríguez	Uruguay	AGESIC
Graciela	Romero	Uruguay	AGESIC
Felipe	Rotondo	Uruguay	URCDP
Jesús	Rubí	Spain	AEPD - Agencia Española de Protección de Datos
Nevena	Ruzic	Serbia	DPA
Ruth	Santana	Ecuador	Dirección Nacional de Registro de Datos Públicos
Peter	Schaar	Germany	BFDI
Fumio	Shimpo	Japan	Consumer Affairs Ageney
Sohyun	Shin	Korea	Personal Information Protection Commission
Blair	Stewart	New Zeland	Office of the Privacy Commissioner, New Zeland
Wilbert	Tomesen	Netherlands	College Bescherming Persoonsgegevens

Name	Surname	Country	Organization
Alejandro	Torres	Mexico INFODF	Comisionado Ciudadano del Instituto de Acceso a la Información Pública y Protección de Datos Personales del DF
Stefan	Verschuere	Belgium	CPVP
Helge	Veum	Norway	Norwegian DPA
Mª José	Viega	Uruguay	AGESIC
Yael	Weinman	United States	FTC
Wojciech	Wiewiorowski	Poland	DPA
Steve	Wood	United Kingdom	ICO
Petra	Wuttke-Götz	Germany	BFDI
Mokhtar	Yahyaoui	Tunisia	INPDP