36th International Conference of Data Protection and Privacy Commissioners

Closed Session

Meeting Report

1. Opening

Drudeisha Madhub and Jacob Kohnstamm open the Closed Session. They stress the importance of this first meeting of the Conference in Africa. Mrs Madhub furthermore stresses the importance of online data protection, especially in the relation between the government and individuals. It should be avoided that our data become a virtual ATM of personal data that government agencies may freely draw from.

2. Minutes 35th International Conference Closed Session

The minutes of the 35th meeting in Warsaw were adopted without change.

3. Accreditations

The accreditation resolution proposed by the Executive Committee was adopted without change.

The following authorities were accredited as member:

- Bremen, Germany: Die Landesbeauftragte für Datenschutz und Informationsfreiheit (The State Commissioner for Data Protection and Freedom of Information, LDI)
- Ghana: Data Protection Commission (GDPC)
- Senegal: La Commission de Protection de Données Personnelles (Commission of Personal Data Protection, CDP)

The following authorities were accredited as observer:

- Bermuda: Ministry of Education and Economic Development Department of eCommerce
- Japan: Specific Personal Information Protection Commission (SPIPC)
- State of Mexico, Mexico: Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (Transparency, Public Information Access and Personal Data Protection Institute, INFOEM)
- Singapore: Infocomm Development Authority (IDA)
- United States: Commodity Futures Trading Commission (CFTC)

4. Internet of Things

The Executive Committee has chosen the topic “Internet of Things” as the main topic for this year’s Closed Session. Four speakers have been asked to provide an introduction to the topic as basis for the discussion.

The first speaker is ***Professor Scott Peppet*** (University of Colorado Law School), who makes his presentation based on the article "Regulating the Internet of Things" that was circulated ahead of the Conference. Prof Peppet first talks about sensors. Over the past years, the Internet of Things has exploded into the consumer market. Two devices are important examples of that explostion: the Fitbit exercise monitor and the Nest thermostat. Prof Peppet speaks primarily on the Internet of Things devices for the consumer market. He sorts consumer devices into categories (Health and Fitness (Countertop, Wearable, Intimate Contact, Ingestible and implantable); Automobile (Event data recorders, consumer automobile devices, auto insurance telematics devices); Home and Electricity (smart home and smart grid); Employee Sensors; Smart Phones (probably the most ubiquitous and powerful of all).

Professor Peppet discusses four basic regulatory problems about the Internet of Things:
1. Everything may reveal everything -> *constrain cross-context uses of data (do not use fitness data to decide upon loans or employment)*

Combined with Big Data analytic techniques, sensor data can reveal a lot about a person, often in unexpected ways. A sensor may track steps walked or the way a person drives their car, but we may be able to draw very powerful inferences from those data about other things—such as how risk-preferring or irresponsible that person is. Sensor data can therefore reveal a lot about you, even if you are not aware. And it can reveal more than what the sensors are intended for, even though companies may not be transparent about that. This leads to the possibility that all data that comes from a sensor may be sensitive information.

2. Internet of Things data may prove very hard to de-identify -> *redefine 'personal information'*

In addition to leading to powerful and unexpected inferences, sensor data are very hard to de-identify or anonymize. Sensor data are so rich and so unique that each person's Fitbit data, smartphone data, location data, or other sensor data may be "re-identifiable." Prof Peppet refers to a recent MIT Study titled "Unique in the Crowd: the privacy bounds of human mobility." That study analyzed anonymized smartphone location data from over one million people over a year-long period and tried to determine how much information from outside the data set one would need to know to re-identify a given person. In other words, how much would I have to know about Person X (such as where Person X was on a specific date or time) to pick out Person X from the million people in the anonymous data? The answer turned out to be that 95% of persons could be picked out of the crowd with just four pieces of "extraneous" information. This is an example of the reality that sensor data can be very difficult to anonymize.

3. Internet of Things devices are (currently) insecure -> *require best security practices, require disclosure of breached sensor data*

Security has gotten a lot of publicity over the past year. Devices are small, with small batteries and small processors. Therefore, the capacity for security measures is also limited. Current generation Internet of Things devices are often quite insecure. In one study, a FitBit was hacked from 15ft away. The same applies to medical devices, which have proven to sometimes have security flaws (for example automatic insulin pumps).

Prof Peppet doesn’t think this is likely to be the biggest problem for Internet of Things devices over time, because companies will try to make their devices more secure as these devices develop. Nevertheless, these security flaws are a serious problem at the moment.

4. What counts as true consent on the Internet of Things? -> *clarify where and when notice should occur and require answers to the privacy policy questions discussed (require the information is physically given on or in the box)*

Consent is a really hard part of the Internet of Things. Prof Peppet shows as an example a breathometer, that can be connected to your smart phone to check blood alcohol content. When you buy the device, there is nothing in or on the box, nor in the user manual, about privacy. No reference is made to the existence of a privacy policy. And also once the connected app is used, no reference on privacy is made. Only at the very bottom of the website is there a link to a privacy policy, which is almost completely focused on the use of the website. The policy does not clarify which sensors are in the device, where the data is stored, how it may be used or if it can be deleted. Only when you find the information on the website can you discover that data cannot be deleted and may be used in a variety of ways.

Prof Peppet has studied twenty Internet of Things consumer devices and has been looking at their privacy policies. In general, they are very confusing. Where is the policy and to what does it apply? Are sensor data ‘personal information’ or ‘personally identifiable’ under the policy? How can sensor data be used, sold, etc? Who owns the sensor data? What data does the device actually collect? Can a consumer modify, delete or access the sensor data? And where are the data stored? Prof Peppet’s conclusion is that these first-generation consumer Internet of Things devices currently have poor privacy policies.

During the ensuing discussion, Prof Peppet stresses that in a context where consent is so weak, it is not a good fall back option to limit surprises. Only if people can truly understand what is going on, they may be able to give a valid consent. Furthermore, he has the impression that companies are becoming nervous about not complying with US and EU privacy laws. They know regulators are paying attention and may be looking at enforcement action. Also the fact that the big companies are moving towards Internet of Things devices may help to improve privacy on these devices. Many devices are developed by start ups, small companies, who do not always realise what they are doing. The more regulators however talk about these issues, the more the companies will start to realise they need to take data protection seriously. At the same time, companies will lobby to be allowed to do more with the data they are collecting. As yet, it is unclear how Internet of Things devices will make money and what the business model will be. The money is in the data and they will want us to wait for as long as possible in making decisions about our views in order for them to develop their business models. Regulators will need to act quickly, to ensure compliant business models can be developed. Data collection and aggregation on the Internet exists and we need to decide if we will allow the Internet of Things data to be integrated into that ecosystem.

The second speaker is ***Professor Rolf H. Weber*** (University of Zürich Institute of Law), who discusses the privacy issues of the Internet of Things. Prof Weber sees four challenges: globality, verticality, ubiquity, technicity.

First of all, he addresses the security and privacy requirements of Internet of Things devices. They are quite important. Devices should be resilient to attacks and ensure that data is authenticated and validated. Users should also have access to data that is collected and have control over the purposes for which the data is used. In short, also Internet of Things data should be compliant with the fundamental principles of data protection. Prof Weber subsequently discusses several possibilities for securing the data, for example by making use of virtual private networks, transfer layer security, DNS security extensions (DNSSEC) and encryption. And even though it would be difficult, it should be tried to process data anonymously, for example by the implementation of undetectability and unobservability mecanisms by using K-Anonymity.

There are new risks emerging from these new types of processing. Most importantly, the control of automatically generated data is a challenge, as is the control of data scattered across large distributed systems and control of de-anonymisation attacks. Data processing ever more often takes place out of context, which may reduce the quality of the data. This all leads to differential privacy (access and processing rules). Prof Weber questions whether or not location-based services available now in smart phones have as a consequence that anonymization is no longer possible in a mobile network. He does however stress that it is important to ensure data minimization, by offering privacy settings by default and by design. This includes the need to use encryption techniques, perturbation and obfuscation.

Prof Weber distinguishes several types of privacy infringements: access by third parties to collected data, use and distribution of data by a controller and the risk of data being combined with other data. This all results in non-compliance with the data minimization principle (and the principle of purpose limitation). Also transparency tools should contribute to more user choice and control, for example by forcing companies to give more information about the data collection, storage and other forms of data processing. Furthermore, access to the collected data should be provided.

In the afternoon, **Kate Carruthers** (Business and IT strategist) is the first speaker to take the floor discussing the continuation of the digital revolution: the internet of everything.

Objects are becoming embedded with sensors and gaining the ability to operate and communicate independent of human intervention. The big shift is that devices are becoming autonomous. The resulting information networks promise to create new business models and disrupt existing models. The characteristics are clear: first, the nature of devices is distributed, making use of peer-to-peer communications. They are API based and network neutral. This means applications increasingly do not need to go through commercial communications networks (mobile phone, WiFi). Connected devices are transformed from a single purchase product into a service that generates recurring income. Therefore, the value of the Internet of Things is not in the devices, but in the new services related to the devices.

New business models are being developed: open models, based on collaboration and loose confederations. The companies developing the products and services are agile and change ready. They work on the assumption of ubiquitous connectivity: WiFi, 4G, bluetooth, and other types of connectivy are available almost everywhere for almost all of the time. For new generations, there is an expectation to be able to communicate wherever you are.

CISCO reckons the value of the Internet of Everything is US$14 trillion. This may be on the low side, but that a lot of money is to be made is a fact.The market signals provide a similar indication: Google buying Nest, Samsung buying SmartThings, etc. Companies are being bought for many billions of dollars.

17.1% of 1400 software developers surveyed are working on Internet of Things apps and 23% expects to begin work on this in the next 6 months. There is a huge proliferation of this development, driven by convergence of techniques. The connection between devices becomes less difficult, because it is now possible to circumvent traditional network connections. Also the set up of such networks is much easier now - they become software defined and do not require a lot of skill of the end user.

In terms of context, apps are key. Between 2008 and 2017, Google Play and Apple's AppStore will be responsible for a mind-blowing number of mobile app downloads: 350 billion! This is quite a challenge for the data protection community. The big IT companies show us a very bright picture of the future: everything connects without effort to each other. The reality is not that way yet, although it improves every year.

There is a landscape of standards emerging for these devices, but there are still many parties involved.

The industrial internet of things is moving much faster, because there are less concerns about privacy and data protection.

Security is a big issue with Internet of Things devices. Many people do not realize these devices do need security. So far, security was 'less important' because the things we did on our computers were generally not that important. Now devices collect data about the most intimate parts of our lives: health data, financial data, etc. Also companies do not always secure their data sufficiently - look at all the major data leaks. The traditional approach of just installing a firewall is by large insufficient. By now, bot-herders can launch DDoS attacks from connected dryers, refrigerators, etc. How would you know as a consumer how to put these machines behind a firewall? Security needs to be implemented by design and default. On many of the devices we have used in the past, security patches and updates are already difficult to implement, let alone on these new devices where the source code often is not available. We need to start thinking about the whole chain of the internet - from the routers and switchers to the devices themselves: they all need much better security.

Computing is all around us and a lot of it is personalized. The machines know our preferences. They offer customization in order to meet our own expectations. But many users do not understand what these devices do, what data they process, etc. And even if they would understand, they do not read the privacy policy. (Example: Londoners exchanging their first unborn child in exchange for free WiFi). People may consent to a policy to be able to use a program, but you can hardly identify it as informed consent.

Miss Carruthers concludes with Amara's law: we tend to overestimate the effect of a technology in the short run and underestimate the effect in the long run.

During the ensuing discussion, Miss Carruthers states she considers it important to get the message about data protection across to young people as well. We should be honest with them and show them both the up- and the downside of what may happen. Explain how to use the privacy settings and how take their own responsibility. Furthermore, DPAs should discuss how to reach out to product and app developers, and make sure they also implement privacy friendly solutions when developing their products. It should be clear when users make a decision on data processing. Privacy policies are not helpful in that respect. They are not drafted to help the consumer, they are there to protect the companies from litigation. Companies need a mind shift on this issue.

One of the delegations makes a comparison between the emerging Internet of Things and the time when cars were first introduced. Back then, legislation was adapted to deal with "horseless carriages", and not to deal with a complete new type of transport. There is a parallel with the internet. One of the possibilities could be to reverse the onus of proof to the company, that they indeed have ensured the consumer is fully aware of what he signed up to.

The last speaker of the day is **Paula Bruening** (Intel Corporation). She does not want to dismiss the legitimate concerns raised by the previous speakers, but stresses the importance of getting privacy and data protection right. Internet of Things represents a dramatic change of technology. It is predicted to fuel the GDP of many countries. Companies should work to enable end-to-end analytics and connect devices to each other, but at the same time enable local filtering and processing of data.

The automotive and transportation sector holds the best promise for adoption of the Internet of Things: safety, efficiency and infrastructure challenges can be better addressed through the collection of vast amounts of data. Transportation experts can use this data to solve problems (self driving cars, smart fleet management, etc), resulting in improved car safety and economic savings. Self driving vehicles can reduce the number of accidents, saving lives and US$5.6 trillion across the global economy. Commuters now spend 40 minutes per day one way in traveling to or from their work. To use this time more productively will save a lot of money.

As to healthcare, Miss Bruening expects that in the next years, half of the healthcare will be delivered virtually, by making use of sensors. Integration of data generated by devices will be essential in providing better healthcare. Mobile healthcare devices will track individual fitness, but can also track the revalidation after surgery: Person2person, person2computer and person-as-computer. The latter can help persons with limited ability, by using the electric signals from their muscles to move body parts if they can't do that themselves. The aging population can be helped by smart devices, especially since more people will be suffering from chronic diseases (cardiovascular, diabetes, cancer and respiratory problems). Smart devices can monitor the status of these illnesses and ensure people can lead as normal a life as possible. With the lack of properly trained healthcare personnel, the devices can take over part of the healthcare tasks.

Miss Bruening also addresses energy and the environment. Home and building energy management systems (providing savings) and smart grids are the future in that domain. It is not the individual devices that enable the efficiency here, but the fact that they are connected to a larger network.

Finally, Miss Bruening underlines the Internet of Things causes new challenges to existing privacy principles. We should embrace the progress while not compromising on the need to comply with existing policies. Companies and regulators should work together in order to Create an environment of trust, that data is being collected and processed in a responsible way and that the rules and principles are honored. This responsibility is a shared one.

5. Updates from delegations

The EDPS informs delegates about his IPEN (Internet Privacy Engineering Network) initiative. The purpose of IPEN is to bring together developers and data protection experts with a technical background from different areas in order to launch and support projects that build privacy into everyday tools and develop new tools which can effectively protect and enhance our privacy. All members of the International Conference are invited to participate and jointly address the widening gap. Privacy regulators invest considerably in the law, but know insufficiently about technology. Further information can be obtained from the EDPS and is available on his website[1].

The federal Mexican delegation informs the delegates about the next legislation that is introduced in Mexico. The government is in the process of creating a national system of transparency and a national system for personal data. IFAI is trying to ensure that the new system also comprises a general data protection law for Mexico, as well as improvements to the freedom of information.

The federal German delegation finally announced that the German Parliament in December 2013 has elected Mrs Andrea Vosshoff to be the new Federal Commissioner for Data Protection and Freedom of Information. She was elected for a five year term. Additional information is available on the website of the DPA[2]. The German representative furthermore thanked the members on behalf of the Bremen data protection commissioners, Mrs. Dr. Imke Sommer, for the accreditation.

6. Reports

- The report of the Executive Committee was presented by the Chair and adopted. It will be changed in order to reflect that the Executive Committee recommended to accredit the Ghanaian authority as a member of the Conference.
- The report of the Berlin Group was presented by the Chair and adopted.

[1] https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/IPEN
[2] http://www.bfdi.bund.de/EN/Home/homepage_node.html

- The UK and CAN delegations gave an update on the work of the International Enforcement Cooperation Working Group. After three years of discussion, a draft arrangement is on the table that should provide a stimulus to further cross-border cooperation between data protection and privacy enforcement authorities around the world. The members of the Conference subsequently discussed the draft agreement, notably on the point of whether or not to allow non-Members of the Conference to take part in the process. It was agreed by a majority this should be possible if the authority wishing to take part is a Member of another platform of international cooperation as states in article 12 sub ii of the agreement. The agreement was then adopted by a majority of the Members present. BE and CH have made a study reservation and will decide at a later stage if they are able and willing to sign up to the agreement. IT expressly abstained from voting.
- The report of the Working Group on Digital Education was presented by FR and adopted, together with the Working Group action plan 2014-2015.
- The report of the Conference Strategic Plan Working Group was presented by NZ and adopted. NZ promised to ensure the actions proposed for 2015 in the resolution adopted in Warsaw will indeed be finalized by the next Conference.

7. Amendments Rules and Procedures

The two amendments to the Rules and Procedures of the Conference proposed by the Executive Committee (regarding awarding the organization of the Conference and chairing of the meeting) where adopted.

8. Resolutions

The Chair mentions that a message of support was received from the AUS delegation for all three resolutions.

- The Resolution on Big Data was adopted with some amendments following proposals by the US FTC.
- The resolution on Enforcement Cooperation was adopted with slight amendments. CH and BE make a reservation.
- The Resolution on Privacy in the Digital Age was adopted without change. The US FTC abstained from voting on this resolution, which relates to matters outside its jurisdiction.

9. Elections

Isabelle Falque-Pierrotin (FR) was elected as new member of the Executive Committee. John Edwards (NZ) was elected as the new chair of the Executive Committee.

10. Any other business

- BG informs the delegates they wish to organise the 2018 International Conference. Kosovo is considering to host the 2016 International Conference.

- PL thanks the members for the trust in serving as member of the Executive Committee. It also informs the members of the next workshops of the PHAEDRA project, to be held in Mauritius (after the Closed Session) and in Cracow, Poland (12 December)

11. Election next host

The 37th International Conference will take place in Amsterdam, the Netherlands from 26-29 October 2015. More information will be available on www.privacyconference2015.org.

12. Closing remarks & Mauritius Declaration

Drudeisha Madhub thanks all delegates for their participation in the Closed Session. Jacob Kohnstamm reads out the Mauritius Declaration on the Internet of Things and closed the session.