Report

Closed Session

35th INTERNATIONAL CONFERENCE OF DATA PROTECTION AND PRIVACY COMMISSIONERS
PRIVACY: A COMPASS IN TURBULENT WORLD
Warsaw, 23-26 September 2013

1. Opening

The Polish commissioner Wojciech Wiewiorowski opens the conference and extends a warm welcome to all participants. More than 60 DPAs are participating this year. Jacob Kohnstamm, the Chair of the Executive Committee, thanks the Polish DPA for the work he and his team have done in organising the conference. He introduces this year's topic: the appification of society. What consequences do mobile apps have for society and data protection and how should data protection regulators respond to the challenges? The Conference will also have an exchange of views with David Medine, the Chairman of the United States Privacy and Civil Liberties Oversight Board, on the Snowden-leaks.

The agenda of the meeting and the minutes of the 2012 Closed Session are adopted without discussion.

2. Accreditations

The Chair introduces the accreditation resolution and the recommendation of the Executive Committee. The accreditations are accepted without discussion. The new members are the data protection authorities from Mauritius and Kosovo, as well as the Ombudsman's office of the City of Buenos Aires, Argentina. The new observers are South Korea's National Information Security Agency, ROSKOMNADZOR from Russia, the Canadian International Industrial Security Directorate, the Singapore Personal Data Protection Commission, the regional data protection authority from Bremen, Germany, as well as the Ecuadorian authorities DINARDAP and SUPERTEL.

3. Appification of society

Professor Hannes Federrath (Hamburg University) discusses the appification of society from a technical viewpoint. He focuses on the technical nature of apps and not on the legal analysis. Many apps do a lot of things in the background, without the end user knowing about it.
Sensors in mobile devices make new apps possible and open up new tracking possibilities. This includes the use of GPS, Wifi, Bluetooth, microphones, cameras and motion sensors. Also, adaptors that can be attached to personal mobile devices (e.g. heart rate monitors) have been introduced. Finally, houses and cars are using technology to become 'smarter', including smart meters, alarm systems, etc.

For use of this new information, several preconditions are needed:
- App needs to have access to the sensors. APIs (Application Programming Interfaces) usually have no access to special hardware features, but some platform independent APIs for camera and microphone are available.

- Local storage of data: always if offline access is needed and always if privacy aspects speak for local storage.
- Special interface design: mostly hardware dependent features.

Server-based tracking was and is always possible, based on the IP address. Client based tracking is relatively new and needs a tracking functionality on user devices, often provided by an app. This means tracking at the source, with no control by the end user over data leakages from his device, but at the same time full access by the app provider.

Most apps are based on a browser engine. The online component of the app could therefore be realised as a web service, useable in a browser. Both can provide the same look and feel, and so from a technical point of view there is no need for an app.

Which data is an app usually sending?
- Controlled by the app: date/time of start and stop of app, particular functions and possibly any data within the app.
- Controlled by the OS (after granting access): global identifiers (Wifi name/SSID, Serial number of device, etc.), location, address book entries and possibly other data stored on the device.

Depending on the model, the user is not informed about any access or transmission of data, but is informed about requested privileges before installation, has to confirm access to data and sensors at first run or has to confirm access whenever an app wants access to data or sensors.

Access control models differ between systems. In the early iOS versions, there was no access control. In the newer versions, access control is offered during installation or updating (trust) and while running (first time the app is requesting for rights, user has to confirm or reject access and can be changed afterwards in the device settings. This is limited to location, network access and address book). For Android, user control is offered during the installation or updating of an app. The user can read which sensors or data the app is requesting access to. The information is fine-grained, but the acceptance is all or nothing. While running the app, access is trust-based, depending on choices made during installation.

Professor Federrath gives several examples of apps and the data they request.

Possible solutions/optimisations could be to give the user the option to allow access to location data every time the app is being used, and to give access to specific sets of information on the phone, instead of general access to for example the full address book.

Another 'problem' with apps is the use of tracking technologies similar to third party cookies in web browsers. The cookies may be deleted once the browser is closed, however the cookies in apps cannot deleted that easy and are usually logged in app logging networks, who can build profiles based on the serial number of the device where the cookie was placed.

Suggested security model - the concept of trusted computing:
- Technical background: every app needs to have a (registered) digital certificate, to identify the app provider and is used to verify the identity of the app during use.
- Privileges are bound to a particular app and/or to a specific app provider (any app of this provider/developer).
- Concepts of trusted computing are not limited to mobile devices and can be used on any computer.

In this model, the mobile device would work with a small built-in smart card (hardware based trusted computing). This makes it easier to identify malware, because the app provider can always be identified, also afterwards and in case of misuse, the certificate of the app or user can be revoked. Trusted computing cannot fully protect mobile devices from damage, but can follow up on and defend attacks. The bad news is that end users lose control over their hardware devices, because apps may be censored or deactivated.

What is needed?
- At least: informed consent by the user.
- Activism: app testing and classification regarding privacy
- Standards: privacy profiles for classes of applications
- Law: app providers really must respect laws
- Best: external privacy certification (app privacy seal)
- Worst: the current situation.
- Regulations needed: transparency (what data is used and why), data minimisation (select before you collect), international regulations or national laws applicable to app providers.
- Self-commitments of app providers are “useless”, at least based on current practice. Self-commitments usually only work on the feature list (the app does this or that) but not on things an app does not do. This is not verifiable for the end user because all data is sent encrypted.

Before installation: detailed information to the end user about privileges requested by an app and why it is requested, as well as the identity of the developer and/or the app provider.
During installation: confirmation on all requested privileges based on usability in clear and understandable language.

Before appification, we had many multi-purpose apps and browser-based services. Now, we have many single purpose apps, where developers have lost the scope. The user has no control over tracking techniques used in apps – everything is possible. App developers need to be taught about privacy and need to limit data collection to what is necessary. A generalised approach for regulators is needed. Also, privacy classification of apps and privacy seals should to be considered.

During the discussion, delegations indicate the need to reach out to app developers, in order to ensure that they are aware of the need for privacy and to entice them to take this into account from the start of the development process. As to self commitment, many commissioners agree that codes of conduct should be considered and could

indeed work, provided they go hand-in-hand with independent enforcement mechanisms. With regard to providing effective information to users, the basic model that was developed by the Platform for Privacy Preferences (P3P) may be useful. This envisaged providers of web browsers to fill out a machine readable questionnaire, the result of which could be 'translated' into standard text elements and logo's. This way, the user could more easily assess the privacy friendliness of an app, even without reading and/or understanding the privacy policy.

Kevin Mahaffey (Lookout Mobile Security) has been trying to solve mobile privacy issues since founding Lookout in 2004. Lookout builds software on mobile phones to keep people secure by keeping malware off phones and protecting consumer privacy.

Today, mobile applications are at the centre of the mobile ecosystem. There are more than 6 million apps worldwide with over 30,000 new apps created every day. Apps are incredibly useful and powerful, but sometimes collect valuable information. The majority of apps in the ecosystem are not malicious and most of the developers of apps with privacy problems have good intentions. Application developers are trying to do the right thing for their users, but sometimes do not know how to think about privacy.

A key challenge for developers is to ensure usability, while protecting privacy at the same time. Common developer issues include: adware, lack of transparency and poor design.

Adware: adware is defined as advertising networks that collect personal data, change browser settings, drop icons or push ads without sufficient notice or consent. In August 2013, Lookout found that around 11% of all Android devices contained apps with adware installed. Lookout drove a discussion to halt adware by developing a set of Mobile App Advertising Guidelines. The technical guidelines contain both a hardline (minimum requirements on data collection, notice and choice) and a softline (recommendations to improve user experience). After releasing these guidelines, Lookout notified its users when an app contained adware. Lookout found that when users were informed that one of their apps contained adware, 95% of users chose to uninstall the app. Within a few weeks, one of the largest advertising networks that contained adware modified their privacy practices to remove adware. Change is actually happening.

Transparency: Many app developers use third party code to add functionality to their products. Developers are sometimes unaware that this third party code collects and uses data that impinges on a consumers privacy. Developers should always ensure that they understand the code that they are adding to their apps and not include libraries that they don't understand. Further, developers should address how libraries impact their users privacy in their privacy policy. Another frequent mistake that developers make is to collect unnecessary or overly-sensitive information. Developers should be selective in collecting data and not store more data than necessary. One of Lookout's tenets is surprise minimisation: do not surprise users with actions or with data collection and use.

Poor design: Privacy is a design problem, not just a legal issue. Research by Alcatel-Lucent showed that trust is more correlated with a willingness to pay than love. By designing strong privacy practices into apps, developers can build trust with their users. Lookout conducted research that showed that people do not read privacy policies, because they are too long and hard to understand. Based on the U.S. Department of Commerce's recommendations, Lookout designed a user-friendly privacy policy. The short form privacy policy quickly informs users how and why Lookout was using data and who their data was shared with without hard to understand legal terminology. By taking a design driven approach to privacy, developers can create understandable interfaces that inform their users about their data practices.

There are tens of thousands of apps created every day, from every country in the world. In the United States, the Federal Trade Commission, California Attorney Generals Office and Lookout have all created educational resources on mobile privacy. Regulators and private sector companies should work together on education initiatives and engage in developer and consumer awareness campaigns on mobile privacy.

After the second presentation, the commissioners discussed what common pieces of information users need to be provided with, how this is to be achieved and how responsibility needs to be attributed. Developers are responsible, but other actors that may have more leverage should be involved. Responsibility of all actors needs to be activated and efforts of supervisory authorities targeted. Transparency is key: no hidden features and complete and full information needs to be given in a user-friendly way. Furthermore, cooperation with technical bodies that can assess the technical side of apps needs to be explored, as a signal that data protection authorities are not afraid to tackle the technical issues in order to improve the privacy friendliness of the ecosystems. Several commissioners suggest that all DPAs commit to an awareness campaign for both users and the industry. Privacy needs to become cool. One delegation adds that awareness raising should also reflect cultural and geographical traditions, in order for a campaign to have maximum effect. Another delegation stresses the need to acknowledge postive efforts made to respect privacy by some of the big players. They should be encouraged to continue these efforts.

Colin Bennett (University of Victoria, Canada) spoke about the impact of mobile apps in political campaigns, which was already a subject of a resolution of the International Conference in Montreux (2005).

Bennett first discussed current trends in voter surveillance, mainly in the US, where many new techniques are being pioneered. 'Voter management' databases have existed in the US for a long time, as part of the electoral culture. They are primarily a US phenomenon, but they also exist in Canada, the UK and Australia. These platforms are generally run by the political parties and are used for canvassing, mailing lists and get-out-the-vote campaigns. Campaign organising becomes increasingly decentralised, and .commercially available databases are increasingly used, together with full "campaign toolkits" that provide fully integrated solutions for any campaign organizer.

Professor Bennett then discussed the use of mobile apps in contemporary campaigning. More and more political parties are making use of apps. In Europe, it looks like most parties are using apps mainly for broadcasting information and less so for capturing information about the electorate and their beliefs and attitudes on issues. Some apps, however, are for example also intended for canvassing, like Footwork in the US, which allow canvassers to enter information about likely voters directly into central databases. In the US, the Obama campaign had an app that any supporter could download providing information about Democrats in the own neighbourhood, based on voter preferences.

Social media and targeted sharing has also become much more important. Mybarackobama.com was made use of the Facebook platform, using the Facebook credentials. This way, use could be made of the social network of users of the site. In general people tend to be influenced to a large extent by their friends, especially youth. Apps are also used for campaign donations. Various apps are provided to give general information about elections and how they work, where to vote, and on the positions of the various candidates in a district. These apps also collect lots of information, and may be harvested by political parties.

Have these practices been exported to other countries? In many AngloSaxon countries (CAN, US, AUS) political parties and political activities are not covered by privacy legislation, as opposed to the EU where political opinions are considered to be sensitive data. However, it is unclear to what extent campaigning can be considered to be a legitimate purpose. This could all be considered a predominantly US problem, because of the 1st amendment protection of free speech, liberal campaign financing laws, and the extensive economy in personal data. However, a range of issues have arisen in Europe, and many DPAs have had to investigate the practices related to parties and campaigning. The ICO and CNIL have have issued reports on political campaigning.

There are many challenges ahead on this point. There are some generic issues concerning non-consensual, non-transparent and insecure capture and transmission of personal information through apps. The variety of data being captured however is the same as for other apps. But the political context also raises some more specific questions and concerns.: who is a volunteer or a canvasser? Who is a member of a party? Who is a regular contact? Who is the data controller, the app developer or the party?

The ability of political parties to collect data on the general voting population, and to "micro-target" segments of a population, is as much dependent on political tradition and culture, as on data protection. The ways election campaigns are carried out differs enormously. But voter surveillance techniques, including the use of mobile apps will surely grow in all democratic states.

4. Electronic surveillance

Following the recent revelations of various surveillance programs in- and outside the United States, the Executive Committee has invited the Chairman of the United States Privacy and Civil Liberties Oversight Board (PCLOB), David Medine, for a discussion with the members and observers of the International Conference. Mr Medine has first given a presentation on the history of PCLOB and its current activities. His organisation

also oversees the various counter terrorism programs that are currently under discussion.

After 9/11, a commission was set up to prepare possible solutions to prevent future attacks. The members of the commission in their report also said that with increased security measures, due account should be given to privacy. Losing liberties was a price not worth paying. PCLOB therefore has the task to find the balance between both. In 2004, after the 9/11 report was issued, the US Congress decided to establish a White House privacy and civil liberties oversight board. However, this board was considered insufficiently independent. PCLOB is therefore now an independent agency within the executive branch. No approval from the White House for its points of view is needed. The Board has one full-time chairman and four part-time members, who are all nominated by the US President and confirmed by the US Senate for staggered six-year terms to ensure independence. Its main task is to oversee the federal counter terrorism programs.

PCLOB seeks information from inside the government and has an unlimited right to do so. Information should not be denied. If the information is not directly provided at the lower staff level where it was requested, PCLOB can and will approach the relevant director who must order disclosure. Mr Medine also informs that US government agencies have an obligation to have guidelines on intelligence activities based on Executive Order 12333. Some of these guidelines are however almost 30 years old. PCLOB therefore requested they be updated, taking into account modern means of communication.

The focus of PCLOB lies with the government's counter terrorism efforts. With regard to the programs under sections 215 PATRIOT Act and 702 FISA which are currently under public scrutiny, PCLOB has started studies into both. Their investigation follows requests from the US President and several senators plus one representative. In July, a public (unclassified) hearing was organised to get more information. Since then more information has been gathered from other sources as well. On 4 October, a new public hearing to test possible recommendations would be organised[1]. The final report is expected by the end of the year. Discussions will take place with intelligence agencies, academics as well as with and about the FISA Court.

During the discussion, Mr Medine makes clear that PCLOB takes its task seriously and is open to considering the civil liberties of US citizens and that of other persons as well. The need to make such a distinction is not included in their legislation and therefore the Board seeks public comment on whether any distinction is appropriate or not. He also gives a glimpse of the possible recommendations PCLOB will make in its final report. In any case, a less one-sided procedure before the FISA Court is considered. In general, American judges are well suited to make decisions in an individual case, but they have more difficulties when assessing programmatic decisions. There is an interest now to make the process before the FISA Court indeed an adversarial process, to inform the judge in a better way on the pros and cons of a case. The question is how to create an adversary in this process, also taking into account the necessary independence from the government.

[1] The public hearing was held instead on 4 November due to the US Government shutdown.

As regards the discussion on collection versus use, Mr Medine states the US government wants the information in their databases because companies do not always retain them for as long as the government may need access. However, to give longer storage obligations to companies may lead to companies wanting to make other use of the data. This continues to be a difficult discussion and no clear solution that is acceptable to all interested parties has emerged. It is however clear that it is valuable to have a haystack somewhere, to target against and find the links and leads, needed for counter terrorism investigations. Without the database, even in case of a reasonable suspicion, it is difficult to find the targets.

5. Reports

The Chair reports on the work of the Executive Committee in the past year. The Berlin Commissioner reports on the work of the International Working Group on Data Protection in Telecommunications. Both reports have also been made available in writing to the members of the Conference.

6. Working group on Enforcement Coordination

The Commissioners from Canada and the United Kingdom report on the work done by the Enforcement Coordination Working Group. They have also prepared a written report for the members of the Conference. The UK Commissioner invites all members to take part in the next international enforcement conference, which will be held on 3 and 4 April 2014 in Manchester.

The Canadian and Belgian delegations have prepared new objectives and functionalities for GPEN's current website for enforcement cooperation. First, new non-protected documents on cooperation in the public sector shall be uploaded. Also, additional web forums for discussion will be created. The new additions to the website will be ready in the weeks to come and accessible for all GPEN members. Some parts of the site are publicly available as well, especially in relation to the public sector. Second, the US delegation presented a proposal to develop a secure online information-sharing platform for GPEN members for which a small amount will be charged, depending on the final functionalities and the level of participation. Initially, this platform will have an "alert function" which will allow participating GPEN members to inform each other of their respective investigations and enforcement actions to facilitate enforcement coordination and cooperation in these matters. About half of the development cost will be covered by FTC, the other half ($60.000) needs to be covered by other authorities. After that, the annual expected costs amount to several hundreds of dollars. More information on the new platform and the costs that will be incurred for participation is to follow.

The Canadian commissioner subsequently presents the results of the GPEN sweep. The most important aspect that was studied was transparency. Nineteen privacy authorities participated in the sweep in the period of 12-15 May 2013, during which 2200 websites were studied. Canada developed the methodology and led the way during the project. Every privacy authority adapted the toolbox to their own situation. They studied to what extent privacy policies were accessible, easy to find, understandable, adequate and if

there was readily available contact information for follow up questions. During the sweep, the bad and the ugly were identified. One of the companies identified as bad and ugly modified their policy within days, others remain in a black spot. Canada is proud of this project. It led to increased international cooperation as well as more awareness for online privacy policies on a global scale. Also, GPEN was tested as a communication tool.

In terms of follow up: most of the participating authorities have made public the findings of the sweep and many will also take follow up actions. Canada for example is sending around letters to around a hundred websites requiring improvements in their privacy policies. Also, a recommendation document was developed ('Ten recommendations for privacy online'). The French delegation requests that for a next sweep it should be made more clear in the communication phase if the sweep is only intended to gather information or should be regarded as a joint enforcement action.

In 2014, a similar action using the same methodology will be carried out focussing on mobile communication and wireless devices (proposal). The Chair proposes to adapt the topic to mobile apps and the appification of society as a follow up from the Closed Session. This suggestion is seconded by the US delegation, stating the focus should indeed be on apps, preferably related to the more sensitive areas.

7. Resolutions

Next to the accreditation resolution, seven other resolutions have been tabled for discussion and adoption by the Conference. The outcome of the discussion was as follows:

1. Resolution on profiling - adopted with unanimity
2. Resolution on the strategic direction of the Conference - adopted with unanimity; the delegations of Italy, France and Kosovo have indicated their explicit support for this resolution and willingness to take part in the working group
3. Resolution on enforcement coordination - adopted with unanimity
4. Resolution on anchoring data protection and the protection of privacy in international law - adopted with abstention from the US delegation; the delegation of Italy indicated their explicit support for this resolution
5. Resolution on openness of personal data practices - adopted with abstention from the US delegation as far as the public sector is concerned; the delegation of Italy indicated their explicit support for this resolution
6. Resolution on digital education - adopted with unanimity; the delegations of Morocco, Uruguay, Colombia, Mexico, Italy and Spain have indicated their explicit support for this resolution
7. Resolution on webtracking - an amended version of the resolution was tabled during the discussed and adopted with abstentions from the delegations of Slovenia and France; the delegations of Hungary and the United States have indicated their explicit support for this resolution.

8. Elections

The Dutch Data Protection Authority, the United States Federal Trade Commission and the Office of the Privacy Commissioner of New Zealand are elected as members of the

Executive Committee. The commissioner from the Netherlands is re-elected as Chair of the Executive Committee.

9. Host 36th International Conference

The Mauritius Data Protection Authority was elected as host for the 2014 International Conference.

10. Any Other Business

The EDPS and the Canadian delegation call upon all members to ensure the resolutions and Warsaw Declaration are publicised on their respective websites. Also, delegations are requested to commit to the follow up of the resolutions at a national level.

11. Warsaw Declaration

In conclusion of the 2013 Closed Session, the Chair reads out the Warsaw Declaration on the Appification of Society that was drafted on behalf of the Executive Committee and the Host.