To: Members of the Executive Committee

From: John Edwards, Chair

Date: 23 February 2015

Subject: **Proposal for the closed session topics 2015**

The aim of this memo is to assist the Executive Committee to select a theme for the first day of the closed session at the Amsterdam Conference. Selecting a topic could potentially take up the whole of the time allocated for our March meeting, and as such I urge members to exchange views with each other (either bilaterally, or with the Committee as a whole) so that we might arrive at a consensus before we convene in Washington DC.

The Secretariat received a number of ideas from Conference and Committee members including three proposed topics that have been worked up in more detail:

1. The challenges of genetic data and data protection by CNIL (Annex A);
2. Data protection oversight of security and intelligence organisations at domestic and global level – NZ OPC (Annex B);
3. Data protection and social media – NZ OPC (Annex C)

The Secretariat has compiled a list of other suggestions for topics and speakers that have been received (Annex D).

Recommendation

- That the Committee **either** by consensus agree to dedicate the full one day Closed Session to **one** of the topics from Appendices A – D: **OR**
- That we run the first day of the closed session as two distinct half day topics.

Chair's Observations

My preferred topic, given the recent international focus on the activities of the NSA and other intelligence gathering organisations in the light of the Snowden revelations would be those at Annex B (Data protection oversight of intelligence organisations). Taking this topic at the Closed Session would provide a valuable opportunity for CNIL to brief our colleagues on its work in this area, and that of the A29 Working Group, as well as recent developments and the ongoing workplan of the UN, and the response from private sector telecommunications companies and online platforms.

While I very much appreciate the effort that CNIL has gone to prepare a detailed proposal on the topic of genetics I would note that there have been a number of conferences and papers on the data protection, privacy and ethical implications of advances in genetic technology in recent years. The value of the Closed Session is that we are able to discuss matters that cannot be as easily debated by officials in a public forum.

Given that the genetics topic is obviously of considerable interest to France, and no doubt to other European DPAs, there could be scope to have some sessions dedicated to the topic as part of the Open Session?

Alternatively, I would support the Executive Committee committing to a Closed Session dividing the available time between the Intelligence and Security, and Genetics topics. I remain open to any other suggestions from members, however I would ask that if any new topics (beyond Appendices A-C) are to be introduced for consideration, they are accompanied with a reasonably detailed proposal and distributed to members as soon as possible.

John Edwards
Chair

Annex A

International Conference – Closed Session - CNIL proposal

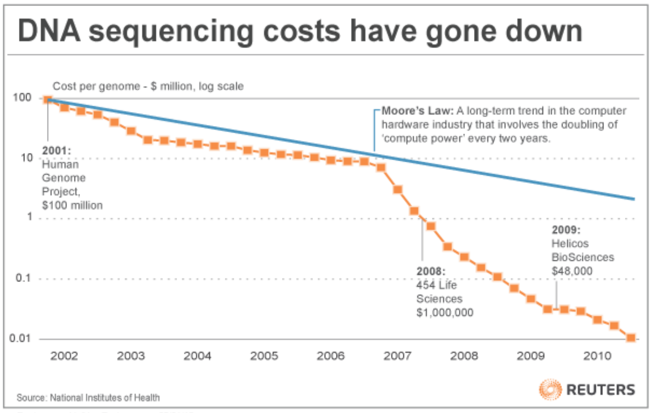
International Conference – Closed Session

Proposal for topic

THE CHALLENGES OF GENETIC DATA AND DATA PROTECTION

For several years, genetics has fascinated the public whether in the field of literature, philosophy or scientific research. The idea of a set of data, inherently part of an individual and largely defining him/her has captured the imagination of many generations.

Today the use of genetic data is no longer confined to the realm of imagination and speculation. In fact, it now becomes ever easier and faster to sequence the genetic code from an individual biological sample. This phenomenon is enhanced by the fact that the price of sequencing has fallen substantially.



Source: National Institutes of Health

Reuters graphic/Van Tsui 05/01/12

Genetic data provide or are likely to provide numerous and various, scientific, medical and personal information relevant throughout the life of an individual. Identification by genetic data is unique but can reveal information on several people. It is therefore no wonder that one of the major issues of genetic data is **predictive medicine**. Genetic tests make it possible to detect the presence of genetic markers acting as risk factors of developing certain diseases.

In recent years, many companies selling personal genomics kits have been created. The most famous is probably "23andMe" created by Susan Wojcicki. Google invested in 23andMe and Larry Page is very interested in the question (he has been himself diagnosed with a rare genetic disease).

However, the subject is in no case restricted to medicine, many fields can be impacted: **research, insurances, identification in general (police, border controls, paternity test…**

Challenges

International instruments actually **prohibit any discrimination based on genetic data**. Under Article 21 of the Charter of Fundamental Rights of the EU, "any discrimination based (...) on genetic features" shall be prohibited, and this prohibition can also be found in the Council of Europe's Convention on Human Rights and Bio-Medicine (Article 11) and UNESCO's Universal Declaration on Human Genome and Human Rights (Article 6).

It follows from all these elements that collection and use of genetic data should be carefully considered.

In fact, there are **serious concerns about potential abuses of genetic information** (racial discrimination, denial of services because of genetic predispositions, disclosure of intimate familial relationships, e.g. partenity).

More generally, a number of unanswered legal and ethical questions still need to be addressed:

- What can genetic data tell us and in what context can they be used?
- To what extend should the use of genetic data be limited?
- What legal, social, philosophical and ethical problems arise?
- Are classical data protection principles appropriate? E.g. is traditional consent sufficient? For what purposes can genetic data be considered relevant, adequate, not excessive?
- How might these problems be resolved?

Possible organization of the closed-session

1. A new era for scientific research

- Possible speakers:
  - [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
- Themes:
  - Predictive medicine, bio hacking
  - Privacy implications

2. Use and re-use for industrial and commercial activities

- Possible speakers:
  - [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
- Themes:
  - Profiling for medical (23and Me), industrial, employment, insurance purposes
  - Privacy implications

3. Society, Ethics and Policy

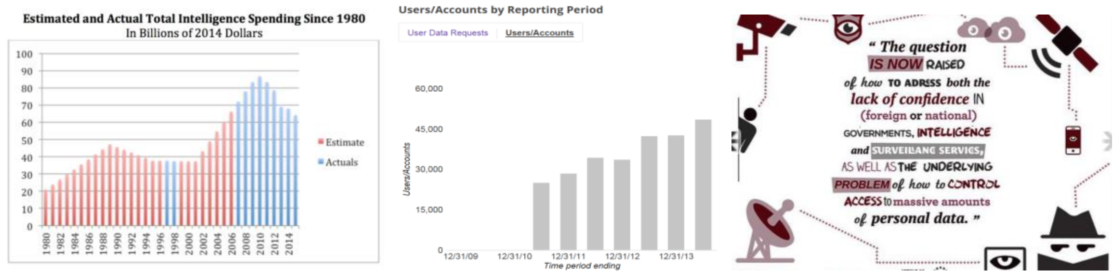
- Possible speakers:
  - [redacted]
  - [redacted]
  - [redacted]
- Themes
  - Theory of Transhumanism (“kill the death”)
  - Position of International and European institutions
  - Role of DPA and privacy regulations

ICDPPC Closed session proposed topic – NZ OPC

Data protection oversight of security and Intelligence organisations at domestic and global level

The proposed session is designed to draw together various strands of current and previous work on surveillance and mass state intelligence gathering, by the conference and other DPA forums, and focus on a particular aspect suited to productive discussion in the closed session: data protection oversight.

Picturing the issues



(For illustration only: LH graph US intelligence gathering spending – huge amounts but cost of data gathering dropping; middle graph Google's transparency reports, government request having doubled in three years ,RH graphic illustration from CNIL website of European Data Governance Forum conference.)

Why choose this topic for the closed session?

It is an important topic. The session will build on preceding work at regional and specialist forums. It will benefit from involving the world's privacy authorities talking at global level in a closed room.

It is not intended to replicate what others are doing or already have done. It achieves this by focusing directly upon the role of DPAs rather than surveillance more generally or the role of intelligence gathering bodies. It also does this by a global approach – the session should seek to transcend regional or cultural divides or national alliances. It needs to seek to get to grips with the cross-border nature of the issues.

What is happening in other data protection forums?

Most relevantly the CNIL hosted since the Mauritius conference a European Data Governance Forum on the topic which adopted a declaration said to be grounded explicitly in European values. That workshop – and its anticipated follow up work – should provide a very good starting point for the proposed session.

The International Working Group on Data Protection in Telecommunications is scheduled to consider a draft working paper (in preparation) on 'transparency reporting' at its meeting in Korea in April. 'Transparency reporting' is the practice of global internet companies, and others, periodically to report on the number and nature of demands for customer data by governments around the world.

The Conference itself has heard from David Medine, Chair of the US PCLOB at the 2013 Conference, and held a public plenary session on 'Surveillance versus Dataveillance' at the 2014 Conference.

What would be the focus of the session?

A precise outline has not been prepared but could easily be developed with Executive Committee input, especially from CNIL given its recent hosting of the European Data Governance Forum if the topic is adopted. The key directions would be to focus the session on oversight and on global approaches. To keep the session focused it is intended that discussion stay away from the general topic of the possible rules or limits for surveillance in a free society but instead be concentrated upon effective oversight of the rules or limits, whatever those rules or limits might be.

It is hoped that the session could include a practical outcome to enhance current oversight arrangements, be it guidance for domestic oversight, plans for joint endeavours, a plan for future work, or whatever. Perhaps in addition to expert presenters there could be a short paper to focus practical discussion or a rapporteur to draw discussion back towards practical outcomes relevant to data protection oversight.

Who is involved in data protection of surveillance or intelligence gathering?

It needs be borne in mind that there are many actors involved in data protection oversight and these vary substantially between jurisdictions. The session should reflect that and recognise that a DPA may sometimes not be the principal oversight body but may still have a role in encouraging, assisting or cooperating with other agencies performing that role or, sometimes, in reporting upon or holding those bodies to account. In addition to independent DPAs the kind of bodies involved might include general government accountability bodies (e.g. ombudsmen, audit bodies), specialised intelligence oversight bodies (e.g. legislative committees, inspectors-general) and internal control bodies (e.g. departmental CPOs). If one adds transparency reporting to the mix, one must then look outside government entities to the oversight arrangements within companies such as Chief Privacy Officers within Internet companies.

Who might speak at the session?

It should be possible to attract some high profile players to speak frankly at a closed session on the intelligence gathering side. We would also seek to have some experienced practitioners of surveillance oversight. Perhaps we might also ask a researcher or academic or civil society representative with experience in the area. We should also seek to obtain some geographical diversity across the presenters.

Examples of possible European presenters might include, for example, Justice Michael Burton of the UK Investigaory Powers Tribunal or be partly be drawn from the speakers to the CNIL/A29 event. Possible US presenters from the oversight community might include: [redacted] There are many additional possibilities.

Transparency reporting is intended to feature as part of the session and that might suggest some usefulness to hear from a corporate that undertakes such reporting. (That presenter could be temporarily video-linked to the session, or asked to join us only for their presentation, if it were thought their presence was inappropriate in closed session.)

Annex C

ICDPPC Closed session proposed topic

DATA PROTECTION AND SOCIAL MEDIA

For many people, social media is central to their online persona: it may be their homepage or the gatekeeper to their internet browsing activity. It may be their authenticator, online companion or perform 100 and one other tasks for individuals.

FaceBook alone, by population, is the third largest country on Earth!

The proposed session puts social media front and centre for consideration by global DPAs.

What are the objectives of the session?

To explore the fundamental aspects of social media and to introduce the cutting edge directions it is taking to help equip DPAs for the new challenges.

What might the session cover?

Precise content will depend upon which international experts are engaged. In general, the session will explore general issues such as data portability, secure deletion, behavioural research, the rise of social media as authenticator, limits on individual bargain striking, behavioural economics (e.g. emotional contagion), use of pseudonyms and responsible practices, indexing and storage of profile and transactional data. The session will also be expected to look at cutting edge or emerging industry or technological practices as well as legal issues such as the assertion of jurisdiction over platforms hosted remotely from the DPA.

Revenge porn, cyber-bullying and anti-impersonation initiatives are under development in a large number of jurisdictions. It would be timely to provide a forum for comparing approaches.

Other sessions might explore how DPAs might use social media in their work, and whether they should endorse or promote “privacy friendly” platforms.

Why explore this topic at the closed session?

The issue is central to DPAs’ work and is replete with a host of merging and cross-jurisdictional issues. We will be able to discuss issues such as the role (if any) DPAs might have in promoting or setting standards in transparency reporting, so that citizens can compare the approach of different platforms to law enforcement and government enquiry. The session would build on previous sessions on profiling, mobile apps and the IOT.

Who might speak at the session?

We would seek to obtain some world class presenters and thought leaders. We would seek to ensure some geographic spread and an appropriate mix between technologists, commerce, users, and commentators/analysts.

One sounding we have made (to positive effect is) Lars Rasmussen who is the head of international engineering at FaceBook's London Office. Lars is the co-founder of Google Maps and joined Facebook over three years ago as a VP of engineering and lead on key products, such as Graph Search and, most recently, Facebook@Work.
http://en.wikipedia.org/wiki/Lars_Rasmussen_(software_developer)

Annex D

COMPILATION OF TOPICS FOR THE CLOSED SESSION 2015

This report by the Secretariat is a compilation of topics and speakers for the closed session 2015 suggested by members of the Conference.

TOPICS
1. Data Protection as part of democratic governance
2. The web we want (www): A focus on positive attributes of the online world that we would like to encourage
3. Promote and see flourish (rather than a session only on threats to some kind of privacy status quo)
4. Privacy protection as part of corporate social responsibility
5. Nudge/behavioural economics/responsive regulation
6. Practical: Working with partners • Other regulators • Civil society • Journalists, etc.
TOPICS SUGGESTED IN THE 2014 EVALUATION SURVEY
7. Protection of critical infrastructures co-operation of DPAs worldwide
8. Balancing data protection with other fundamental rights, e.g., freedom of expression, security etc., in the age of social media
9. Competition law and privacy
10. Focus on the practical problems concerning controls and the rights of the persons concerned
11. Anonymization in big data age. Is it possible?
12. Applicability of the law on protection of personal data to the processing only for personal purposes
13. International enforcement cooperation

14. Practical aspects of how to do the job of DPA better
TOPICS SUGGESTED BY CONFERENCE MEMBERS IN THE 2013 EVALUATION SURVEY
15. Anonymisation/pseudo-anonymisation
16. Cloud computing universal identifiers (Telecom, ID, biometrics) location data (mobile phone, personal car/toll/e-Call, car at workplace, law enforcement purposes) Big data
17. IPv 6 and Ubiquitous Computing, Affiliate marketing, Education (generally speaking some kind of practical follow up of the declarations)
18. Retail tracking and location based marketing (example, Apple iBeacon) -Biometrics and 2-factor authentication (example, Samsung iris and iPhone fingerprint technologies)
19. Privacy of politicians, civil servants and all public sector employees - freedom of information and personal data protection, in particular emails, signatures, attendance of meetings
20. The sessions tend to concentrate on global issues, whereas the concern of many DPAs (particularly smaller DPAs) is more domestic. Maybe this balance could be reconsidered.
21. Some aspects that new or early DPA´s are facing in the third world would be of interest to share and learn about the challenges there are facing.
22. Oversight of surveillance activities is timely. However, we can't focus just on the US. Do Parliamentary Committees work? How can we achieve more transparency/public reporting?
23. Mass data collection and blurring line between private and public use
24. Promoting continuous improvement, capacity building and sharing best practice in 'performing the job' of a national or state DPA e.g. measuring performance, effectively influencing stakeholders, managing ethical dilemmas, improving regulatory practice, etc.
25. Raise awareness on emerging trends/threats: wearable computer / internet of things / big data (in correlation with mass surveillance capacities), etc.
26. Legal treatment of autonomous information gathering, due to technology, so without consent.

Suggested Speakers	Notes
1. Bruce Sterling	http://en.wikipedia.org/wiki/Bruce_Sterling
2. Daniel Solove	http://en.wikipedia.org/wiki/Daniel_J._Solove
3. Lawrence Lessig	http://en.wikipedia.org/wiki/Lawrence_Lessig
4. David Brin	http://www.davidbrin.com/index.html
5. Ban Ki Moon, UN Secretary General	
6. Zeid Ra'ad Al Hussein, UN High Commissioner for Human Rights	http://www.ohchr.org/EN/AboutUs/Pages/HighCommissioner.aspx
7. James Risen	Author of Pay any Price. Theme of perpetual security state.
8. David Brin	http://www.davidbrin.com/index.html
9. Dave Eggers/ Dan (Daniel) Solove	