Amsterdam Declaration

37th International Privacy Conference of Data Protection and Privacy Commissioners

Amsterdam 2015 - Closed Session

27 October 2015, Amsterdam, Netherlands

The Chair and host present the following summary of the discussions in the Closed Session of the 37th International Privacy and Data Protection Conference held in Amsterdam, Netherlands on 26 and 27 October 2015

Communiqué on Genetic and Health Data, Challenges for Tomorrow

For several years, genetics has fascinated the public. Today, it is increasingly cheaper and faster to sequence the genetic code from an individual's biological sample.

Genetic data provide or are likely to provide numerous and various scientific, medical and personal information relevant throughout the life of an individual. At the same time, if identification by genetic data is unique it can also reveal information on several other individuals.

The benefits of genetic data are also driving its increased use. Consumer-facing services may confirm a diagnosis, identify an increased risk of developing a disease, or indicate that a person is a carrier for a particular disease. Such information can be used by individuals and health providers to take steps to reduce the likelihood of negative outcomes. Direct care of patients offers improved outcomes and medical and scientific research offers the prospect of new diagnoses and cures for diseases. In addition, the added value of the analysis of one genome derives from the existence of other genomes in a relevant database, and from algorithms that compare the genomes to detect patterns and traits.

THEREFORE, the assembled data protection and privacy commissioners have discussed during the 37th International Privacy and Data Protection Conference held in Amsterdam, Netherlands on 26 and 27 October 2015, the challenges arising from society's increasing ability to collect, analyze and use genetic information.

AND HAVE MADE the following observations:

Characterization and identification

The use of genetic data may take different forms. It can be intended for the sole purpose of the **identification** of an individual or/and of his or her relatives. It can also serve to **characterize** individuals in order to identify correlations within a given population and to deduce the level of predispositions or risks, of medical nature or else.

Risks for data protection and privacy

While there are clearly many benefits that do and will continue to stem from individuals' voluntarily contributing their genetic information, the use of genetic data could lead to a variety of **risks, such as**: hacking and disclosure of intimate familial relationships, as well as ethnic discrimination, denial of services because of genetic predispositions, and other malicious uses. These risks are enhanced by perceptions of an absolute genetic determinism on the life and health of an individual. Such risks will depend to a large extent on the **context** in which these data are processed, the safeguards surrounding the processing of these data, and on the **reasonable expectations of the individuals**.

Some discussants mentioned that the need for comprehensive databases in order to compare genomes might create **concentration of powers** in the hand of a few private actors.

For these reasons and considering the possibility of re-identification, strong privacy safeguards such as the following should be implemented:

It is crucial that data subjects remain in **control** of their data, receive appropriate information and have their **choices respected**. This can be achieved through various means that ensure a dynamic **management of consent throughout the life cycle of the data,** supplemented by additional guarantees such as: institutional review boards (IRB), privacy management programs, privacy impact assessments, privacy by design and certifications.

Moreover, while genetic data can be used to irrevocably identify one individual, it also **reveals information about third parties**, contributing to their identification and characterization. This suggests the need to consider whether, and the circumstances under which, it would be appropriate to provide notice and other **rights to third parties** when contribution of one individual's genetic data reveal information about the third parties.

Necessity for Greater Communication with the Scientific Community

It would be beneficial to the data protection and scientific communities if there were more exchanges between them that are designed to build greater understanding and ensure that continuing innovation provides the significant benefits from genetic information, and at the same time protecting fundamental or consumer rights.

Communiqué on Data protection oversight of security and intelligence: The role of Data Protection Authorities in a changing society

The unprecedented level of public discussion of the activities of intelligence and security agencies worldwide, together with the changing security environment with potential for terrorist activity in all countries has raised a number of challenging issues for Data Protection Authorities and Privacy Commissioners ("DPAs").

DPAs shoulder multiple responsibilities and communities look to DPAs for privacy leadership in this context regardless of strict boundaries of jurisdiction. Where DPAs do not have a direct enforcement role in respect of intelligence and security activities, most still have roles as ombudsmen, auditors, consultants, educators, negotiators and policy advisers.

DPAs met to discuss how they can respond to the new and changing environment. They heard that the public should expect intelligence and security agencies to observe the rule of law, pursuant to appropriate regulation, and to exercise restraint in the use of intrusive powers.

DPAs recognise the importance of the public discussion and the legitimacy of their contribution to that discussion. They heard that the current environment is characterised by:

- An undermining of public confidence from selective revelations, often unanswered by some agencies with the information;
- Sometimes fragmented and under resourced specialist oversight agencies;
- Blurring of the boundaries between intelligence and law enforcement activities;
- Lack of an informed populace;
- Difficulties in providing effective domestic and cross border coordination of oversight;
- Official Reviews and public debate in many countries.

There is no-one-size-fits-all in relation to intelligence and security oversight, and each DPA has to find its own way to contribute to the discussion, and to the oversight environment in order to build and maintain public confidence. DPAs discussed some of the elements that their influence could include;

- The promotion of proportionality and lawfulness in intelligence and security activities;
- Establishing links and coordination with local and international oversight agencies;
- Providing advice and assistance to specialist oversight agencies while retaining their independence and credibility with their communities;

- Advocating for better transparency, both from the agencies, and from commercial entities that are providing data in response to requests or demands from intelligence agencies.
- Defending wider use of encryption use as a legitimate means to protect consumer data.

John Edwards
Chairman of the Executive Committee of the International Conference of Data Protection and Privacy Commissioners

Jacob Kohnstamm
Chairman of the Dutch Data Protection Authority