38TH
INTERNATIONAL
PRIVACY
CONFERENCE
Marrakech 2016

**19 October 2016**

## Communique on the 38th International Conference of Data Protection and Privacy Commissioners

Privacy Commissioners and Data Protection Authorities from around the world convened in Marrakech this week for their 38th International Conference.

As has been the practice for the last six years, the first part of the Conference was a Closed Session for Accredited Members and Observers.

The Closed Session began with the admission of new members. The Executive Committee was pleased to recommend to the Conference that, having met the accreditation criteria, the data protection authorities of Armenia, Cape Verde, Mali and the Philippines, as well as the Telecommunications/ICT Regulatory body of Cote d'Ivoire, should be welcomed to the ICDPPC.

Twelve entities were granted observer status, several of which had applied for, but did not yet meet the criteria for full membership.

The Conference heard from two panels, both moderated by Professor Ian Kerr of Canada, on the topics of Robotics, Artificial Intelligence, and Encryption.

Each of these rapidly developing technologies pose a number of new challenges for data protection. Both Robotics and Artificial Intelligence are intended to simulate human characteristics as they perform functions to assist users. The field of social robotics, which involves the anthropomorphic design of machines to engender, or manipulate the trust of the user is likely to lead to the widespread use of the devices to assist with the care of the elderly and others.

These devices are equipped with numerous sensors, are likely to be connected online, and are in effect all seeing, all remembering in-house guests. As such, they pose challenges for a consent model of data collection and present challenges for security

Artificial Intelligence, or machine learning, poses challenges that we are only just beginning to understand. Conference members were told that that a mark of machine learning is the unpredictability of the outcome of a data processing function. This feature was described as "unpredictability by design" and presents a particular challenge when it comes to responsibility or accountability for automated decision making, when the algorithm used to arrive at a conclusion is not known and is in fact unknowable by the designer or user of the application. Initial bias reflected in coding or sample selection used in a machine learning process can taint the algorithmic outcome, but with no transparency as to the mechanism by which the programme has produced its results or conclusions.

Encryption is an important mechanism for business and consumers to protect their information at rest, on servers, from those who would attempt to steal or corrupt it, and in transmission for those who wish to intercept or manipulate the content. Encryption poses a significant challenge for law enforcement agencies and others with lawful authority to intercept communications, but without the technical means to act on that lawful authority, because the chosen channel of the target individual is protected by strong encryption.

No satisfactory response to this challenge has yet been identified. Conference members heard that most industry and technical experts do not favour the introduction of selective vulnerability to cryptographic programmes, to enable properly authorized law enforcement access, because such solutions introduce complexity, and complexity reduces security for everyone. Nor are regulated solutions of commercially available products likely to prevent bad actors from "going dark", given that many of those most motivated to protect their communications from law enforcement and intelligence agencies have the capability to access or develop their own strong crypto.

During day two of the Closed Session, the conference received a progress report from the UN Special Rapporteur on the Right to Privacy and received reports from working groups on digital education, Privacy and Humanitarian action, Data Protection in Telecommunications, and on an Enforcement cooperation meeting.

The Conference passed a number of resolutions

- Resolution for the adoption of an international competency framework on privacy education (FTC abstaining)
- Resolution on developing new metrics of data protection regulation
- Resolution on human rights defenders (FTC abstaining)
- Resolution on international enforcement cooperation

The Conference thanked retiring Executive Committee member The Netherlands for its six-year contribution, and welcomed 2017 Conference host Hong Kong as a member. France was reelected for a further term.

**John Edwards**
**Privacy Commissioner of New Zealand**
**Chair Executive Committee of the International Conference of Data Protection and Privacy Commissioners**
**https://icdppc.org/**
**https://www.privacyconference2016.org/**