EXECUTIVE COMMITTEE
ICDPPC

VOLUME 2, ISSUE 6
38TH CONFERENCE SPECIAL EDITION

ICDPPC
International Conference of Data Protection & Privacy Commissioners

COMMUNIQUE

SEPTEMBER 2016

INSIDE THIS ISSUE:

SPECIAL POINTS OF INTEREST:

- **Closed session panels**
- **Profiles of closed session speakers**

MESSAGE FROM THE CHAIR

The rise of robot intelligence

Search online for Marrakesh and the results reveal an imperial city with a deep civilisation and glorious architecture. As the venue for the 38th International Conference of Data Protection and Privacy Commissioners, it is a fitting successor to last year's conference in Amsterdam, another remarkable city of culture and heritage. I want to thank our colleagues at Morocco's CNDP for their hard work in preparing for this year's conference.

Since the first conference in Bonn in 1979, data protection and privacy authorities have been meeting to discuss emerging privacy trends, risks, threats and challenges. We've built up quite a record of subjects tackled, including law enforcement and border security, cloud computing, internet governance, web tracking, app development, the Internet of Things and many others.

The two streams of this year's closed session continue that tradition with two important and current topics - artificial intelligence and encryption. We are seeing these themes increasingly reflected in our arts and culture with, for example, television programmes like Mr Robot and Humans, and films like Ex Machina, Her, I Robot and Interstellar. These technological influences are also manifesting themselves in our workplaces and public spaces. As life increasingly imitates art, we've clearly come a long way since 2001: A Space Odyssey in 1968.

It is vital that we as an international community are prepared to offer up-to-date debate and guidance on the potential impact of our 'science fiction' future. Our communities need to be intellectually prepared to debate the pros and cons of machine intelligence and to identify and mitigate the privacy implications of this area of scientific and human development.

With this in mind, we've prepared a highly relevant programme of speakers who have exceptional expertise in the areas of robotics, artificial intelligence and encryption. The speakers we have lined up are some of the best in their fields and their deep insights are sought around the world - and will become increasingly so as science fiction becomes reality.

It seems fitting that we should be preparing to discuss the future of privacy in Marrakesh, a city that has made such a significant contribution to human civilisation.

I look forward to hearing your contributions to our discussions on these vital subjects. It will be wonderful to see many of you again and to build on the connections we've made at previous conferences. These personal connections matter a great deal as we look to finding privacy solutions for our respective communities in our connected world.

John Edwards — New Zealand Privacy Commissioner and Chair of the ICDPPC Executive Committee

CLOSED SESSION: PANEL 1 — ARTIFICIAL INTELLIGENCE AND ROBOTICS

The robots have arrived. And, more are on the way. When one considers the opportunities and risks posed by robots and artificial intelligence (AI), it is clear that the decision to populate our skies, cities, workplaces and homes with them will cause profound social and economic shifts. Cryptographic solutions have been proposed to secure these and other cloud-driven machines, and their vast, diverse data trails. Of course, cryptography—like robots and AI—can be both the remedy and poison in the transmission of data. All of this is sure to create emerging challenges for privacy and data protection.

Day 1 of the closed session at October's Conference is devoted to in-depth discussion of Robotics, Artificial Intelligence, and Encryption.

Robotics and AI

A substantial portion of the day will be devoted to an exploration of the cutting edge technologies of robotics and artificial intelligence and their broad social implications. We will be assisted in our discussions by leading experts from North America and Europe. The objective of the day will be to give Commissioners a deeper understanding of these technologies, the risks for individuals and their privacy and the impacts and opportunities for data protection authorities.

The issues will be explored under three key themes:

Social robotics and (the manipulation of) trust

We will hear about and explore the field of social robotics—semi-autonomous, embodied robots that interact and communicate with humans. Through 'anthropomorphic design', these machines are imbued with human characteristics to create a social valence that adjusts our emotional attitudes and alters our interactions with them. We will consider the potential humanizing and dehumanizing effects, and the social implications for individuals interacting with those machines. Should we be concerned about the manipulation of human trust to catalyse human-robot interactions? How will this affect data collection, use and disclosure? What are the implications for privacy and for DPAs?

Deep learning, unpredictability and the duty to explain

'Deep learning' involves machines that can learn from the data collected, rather than by programming alone. The machine can then produce outcomes that are "unpredictable by design". As the world recently witnessed when an AI created by Google DeepMind (AlphaGo) defeated grand Master Lee Sedol at the ancient board game "Go", even a machine's programmers may find the AI's 'reasoning' impossible to understand. The concept of machine 'deep learning' therefore disrupts desires for algorithmic transparency and accountability mechanisms. We will seek to understand what is happening in this area and explore the implications for privacy and data protection, especially in the context of decision-making affecting individuals.

AI discrimination and how it affects privacy

Although it was clear long before Microsoft's chatbot, "Tay", demonstrated that AI tends to replicate real world inequalities, many experts hold out hope that delegating decision-making to AIs affords a real opportunity to eliminate racism, sexism and other forms of discrimination. This session will explore the issue of discrimination in the context of AI and the implications for privacy and for the work of data protection regulators. Where might solutions be found? In code? In regulation? What new challenges may be faced by a privacy regulator?

Panellists

The panel will draw out emerging issues and implications for regulators in this fast-changing area. The panellist include Ian Kerr, Mireille Hildebrandt and Nadia Magnenat Thalmann.

> ***"Cryptography—like robots and AI—can be both the remedy and poison in the transmission of data. All of this is sure to create emerging challenges for privacy and data protection."***

AI AND ROBOTICS: SPEAKER PROFILES

Ian Kerr

Ian Kerr holds the Canada Research Chair in Ethics, Law & Technology at the University of Ottawa, Faculty of Law, with cross appointments to Medicine, Philosophy and Information Studies. His current research interrogates: (i) privacy and surveillance; and (ii) robotics and artificial intelligence law and policy. Ian Kerr's ongoing privacy work focuses on the interplay between emerging public and private sector surveillance technologies, civil liberties and human rights. His recent work, including his new book, Robot Law, studies the delega-

tion of human tasks and decision making to machines with the aim of developing frameworks for the governance of robotics and artificial intelligence.

Watching the robots - Ian Kerr

Privacy isn't just about who is watching, because, now, no one is watching. Robots cloaked in human attributes smooth the transmission of personal information without human involvement. Apple's Siri handles a billion weekly requests; hundreds of millions of people trust Siri as a digital confidante, revealing things they would not tell friends or family. Artificial intelligence (AI) can then automate this information to make crucial decisions affecting our life chances and opportunities - all of this without human interaction or oversight. With the advent of social robots and strong AI, the future needs to better understand how robots and AIs infringe privacy and what to do about it.

Mireille Hildebrandt

Mireille Hildebrandt is Research Professor of Interfacing Law and Technology at the Faculty of Law and Criminology, Vrije Universiteit Brussel, and Professor of Smart Environments, Data Protection and the Rule of Law at the Science Faculty of Radboud University Nijmegen. Prof Hildebrandt published *Smart Technologies and the End(s) of Law* (2015, Edward Elgar) and numerous other works on the implications of artificial intelligence on democracy, human rights and the checks and balances of the Rule of Law. She is one of the founding members of the Digital Enlightenment Forum and co-author of *Onlife Manifesto*.

Testing robotic and AI privacy rules - Prof Mireille Hildebrandt

Data protection is often focused on hiding or controlling personal data. Cloud robotics, cyber-physical infrastructures and other types of data-driven intelligence thrive on predictive analytics that may play around with our autonomy, privacy and our rights to equal respect and due process. To operate smoothly and safely, data-driven agents will need to pre-empt our intent, which raises a number of issues that cannot be resolved at the level of control over individual data points. EU data protection law developed specific

> ***"To operate smoothly and safely, data-driven agents will need to pre-empt our intent, which raises a number of issues that cannot be resolved at the level of control over individual data points."— Prof Mireille Hildebrandt.***

AI AND ROBTOICS: SPEAKER PROFILES (CONTD.)

protection for those subject to the decisions of data-driven agents; the time has come to test the salience of this protection.

Nadia Magnenat Thalmann

Nadia Magnenat Thalmann is Professor and Director of the Institute for Media Innovation, Nanyang Technological University, Singapore. She is also the founder and director of the MIRALab, an interdisciplinary lab in Human Computer Animation, University of Geneva. Her global research area is the modelling and simulation of behaviour for virtual humans and social robots. Prof Thalmann is also working on 3D mixed realities and medical simulation. She has created a social autonomous robot, Nadine - a likeness of herself which is able to speak, recognise people and gestures, express mood and emotions, and remember actions. Prof Thalmann's recent awards include the

2012 Humboldt Research Award, and two Doctor Honoris Causa (from University of Hanover in Germany and the University of Ottawa in Canada). She is a member of the Swiss Academy of Engineering Sciences.

Making AI respect privacy - Nadia Magnenat Thalmann

Artificial intelligence (AI) is complex software that allows a machine or a robot to understand the environment and react to it in a proper way. That means that by capturing all kinds of information on each individual, and doing analytics, the machine or robot can produce the details of the personality of anyone—for example, their eating habits and decision-making processes. The solution is to put controls on a machine or robot so what a robot observes, analyses and decides cannot be transmitted to anyone who is not authorised. Access to any personal information should not be made available to anyone and should not be used publicly without the formal consent of the person. This is our main societal problem - to prevent private analytics done by AI tools becoming available to everyone or used for other purposes. Appropriate national and international laws need to be in place before such technology has the potential to impact on our private lives.

> ***"Artificial intelligence (AI) is complex software that allows a machine or a robot to understand the environment and react to it in a proper way."—Dr Prof. Nadia Magnenat Thalmann.***

CLOSED SESSION: PANEL 2 — ENCRYPTION

Encryption and rule of law: an international conversation

Encryption is usually perceived as a highly technical process of encoding data into a secret format in order to secure it. While this is certainly true, it provides much more. It ensures the integrity of data and messaging and it provides accountability. It provides a mechanism for authenticating individuals and organizations, and can do so in a manner that provides anonymity. Cryptography is a multi-faceted technology: it can be used to lock-up data, it can be used to ensure authorized access, and while it can be used to monitor and track individuals accessing data, it can do so in privacy-respecting ways.

Our closed session will conclude with an in-depth discussion on developments in the application and use of encryption technologies and their impact on the ability of organizations and governments to meet three objectives that are vital to the continuing strength and reliability of the digital economy: (i) the ongoing need to protect and secure data; (ii) the need for law enforcement and national security agencies to have access to personal information under lawful processes; and (iii) the requirement to protect the privacy of individuals. These discussions will examine the technical, geo-political and legal dimensions at play and will aim to contribute to an enhanced appreciation of how these issues interfere with or reinforce one another, as the critical dialogue continues both domestically and internationally.

The issues will be explored in accordance with the following theme:-

Authorised access to encrypted communications

Encryption is at the core of how organizations worldwide are able to meet their legal obligations and to protect data from unwanted intrusion. Yet these protections have become so strong, effective and targeted, that any compromise to accommodate security objectives risks compromising the personal data.

Law enforcement and security agencies have historically been provided with lawful means to access information in support of investigations or intelligence-gathering. Technological evolution in the area of cryptography has made it increasingly difficult for governments to access this information.

Participants will be called upon to consider key questions such as:

To be effective, must encryption necessarily result in preventing the enforcement of lawfully obtained orders for the production of personal information?
Is it possible to enable authorized access without creating technological vulnerabilities or other forms of unauthorized access?
If so, how can it be done technologically and legislatively in a way that respects fundamental rights?

Panellists

The panel will be led by Prof. Ian Kerr, who will draw out emerging issues and implications for regulators in this fast-changing area. The first panellist is Latha Reddy and the second panellist is Christopher Kuner.

The Executive Committee acknowledges the assistance of Prof. Ian Kerr in the development of both sessions.

> ***"Cryptography is a multi-faceted technology: it can be used to lock-up data, it can be used to ensure authorized access, and while it can be used to monitor and track individuals accessing data, it can do so in privacy-respecting ways."***

ENCRYPTION: SPEAKER PROFILES

Prof. Ian Kerr

Prof Kerr holds the Canada Research Chair in Ethics, Law, & Technology at the University of Ottawa, Faculty of Law, with cross appointments to Medicine, Philosophy and Information Studies. Ian's full profile is set out above.

Latha Reddy

Latha Reddy is a Distinguished Fellow in the Cyberspace Cooperation Department of the East West Institute. She is the former Deputy National Security Adviser of India. In addition to assisting

the National Security Adviser of India, Reddy was responsible for cybersecurity and other critical internal and external security issues. She is also an official of the CIGI Global Commission on Internet Governance.

Dr Christopher Kuner

Dr Christopher Kuner is Professor of Law and Director of the Brussels Privacy Hub, a research centre at the Vrije Universiteit Brussel (VUB) in Brussels. He is Affiliated Lecturer at the University of Cambridge and Visiting Professor at the London School of Economics, and has taught at the summer session of the Hague Academy of International Law. A prolific author, Dr Kuner is Editor-In-Chief of the journal, International Data Privacy Law, and Senior Privacy Counsel at Wilson Sonsini Goodrich and Rosati in Brussels.

Restricting encryption won't work - Dr Christopher Kuner

Encryption is a key technology that can help realise data protection and privacy in practice. It illustrates how technology can enable privacy, not just threaten it. Attempts by govern-

ments to restrict the use of encryption and to build weaknesses into it have not worked in the past, and will not work now. Existing concepts of proportionality and transparency can be applied to protect privacy while respecting the legitimate security concerns of society when encryption is used.

> ***"Encryption is a key technology that can help realise data protection and privacy in practice. - Dr Christopher Kuner"***

WHAT'S IN STORE FOR THE PUBLIC CONFERENCE

In 2013, the 35th International Conference of Data Protection and Privacy Commissioners in Warsaw adopted a resolution on "digital education for all". The resolution called on governments, non-governmental organisations and all other sectors to act together to educate people with the essential skills needed to effectively participate in the digital environment.

The 38th conference is continuing this theme at its Open Session with discussions on initiatives in digital education from all five continents. The two panel discussions will be moderated by CNIL President Isabelle Falque-Pierrotin and New Zealand's Privacy Commissioner John Edwards, with the participation of Victoria's Commissioner for Privacy and Data Protection, David Watts, Mexico's INAI President, Ximena Puente de la Mora, and Hong Kong's Privacy Commissioner for Personal Data, Stephen Wong, as well as representatives from GIODO, OECD and UNESCO.

Other topics to be included at the Open Session include:

- Privacy and personal data protection as a driver for sustainable development (moderator Bojana Bellamy, President of CIPL, with keynote speaker Brad Smith, Microsoft President and Chief Legal Officer)
- Adequacy, localisation, and cultural determinism (moderator Martin Abrams, Executive Director of IAF, with keynote speaker Giovanni Buttarelli, European Data Protection Supervisor)
- Technology and science trends: what impact on privacy? (moderator Trevor Hughes, President and Chief Executive of IAPP, with keynote speaker Edith Ramirez, Chairwoman of the Federal Trade Commission)

- How to reconcile security and privacy; Oversight and accountability principles for government access to data (moderator Daniel Therrien, Chairman of Canada's Office of the Privacy Commissioner).

"38th International Conference of Data Protection and Privacy Commissioners: Opening new territories for privacy"

ICDPPC

International Conference of Data Protection & Privacy Commissioners

ICDPPC SECRETARIAT

Email: ICDPPCExCO@privacy.org.nz
Follow us on twitter @ICDPPCExCo

SIDE EVENTS AT THE CONFERENCE

A number of side events will be held on the margins of the 38th Conference in Marrakesh, Morocco.

Following is a list of side events on 18 October and 20 October 2016.

- Nymity: Demonstrating Compliance to Regulators
- Giz:Data Protection in the International System of Human Rights
- IAF & FPF: Technology, challenges and effective governance
- GPEN: Connected Thinking: Better enforcement outcomes through sharing methodologies and expertise in connected privacy
- CNDP: Meeting of African DPAs
- Microsoft: Accelerating MEA Digital Transformation
- AFAPDP: Meeting with the network of data protection authorities of the Francophonie
- PHAEDRA II: Cooperation between DPAs
- Common thread Network: Annual Meeting
- IAPP: Exclusive Welcome Reception for 38th International Data Protection and Privacy Commissioners Conference
- Dutch DPA: Privacy Bridges: broader and bolder
- CIPL: The Role of Risk Assessment and Transparency in Enabling Organizational Accountability in the Digital Economy
- U.S Department of Commerce: Privacy Shield: Industry training & DPA liaison workshop
- DCAF: The protection of personal data in the security and defence sector.

Some side events may be only open to accredited members and some may be by invitation only.

Registration details will appear on the website at www.privacyconference2016.org/en as they are settled by the organiser of the side event and are available.

REGISTER FOR THE 38TH CONFERENCE

The 38th Conference is on 17—20 October 2016 in Marrakesh, Morocco.

Do not miss the data protection event of the year, hurry up and register by sending an email to the host—contact@privacyconference2016.org