38th International Conference of Data Protection and Privacy Commissioners, Marrakesh, Morocco

17 October 2016

Closing remarks by the Chair, John Edwards

After our last conference we canvassed our membership for topics to build a programme around for 2016. We went through quite a process and lots of discussion before we filtered the suggestions into the three topics of Artificial Intelligence, Robotics, and Encryption.

It was not immediately clear to me whether these would come together to form a coherent session, or would appear as three disjointed, albeit interesting, topics.

As it happens there were several common threads to emerge.

We've seen many fascinating presentations some amazing slides. For me one of the most striking slides was actually a pretty prosaic graph of the aging demographic.

There will soon not be enough able bodied people in the workforce, to care for the frail and elderly in the community.

We saw how robotics can help with this problem – but in order for that solution to be palatable, it requires one key element – trust.

We all know that you build trust by showing that you are a worthy and reliable steward of personal information.

We've learned that the other way to build trust is to fake it. Enter anthropomorphic design which helps to fool us into thinking we are interacting and exchanging data with a human, either remotely through an online interface like Ian's vRep, or in our homes through an all seeing, all recording, sensor-equipped humanoid machine.

Unlike a human health care worker, that machine, however cute and human it seems, has no discretion, no judgement. It is in many ways as dumb as the toaster that Ian put at one end of his spectrum. Like every other form of data processing, that device needs to be designed in ways that manage the risks of the opaque

consent under which it operates, ensures the data is only used for known purposes, and is kept secure. Here, encryption plays a role.

A robot equipped with AI, learning new tasks based on trial and success and trial and error, producing unpredictable outcomes and behaviours that its creators could not reasonably be expected to know of, and to which a user could not have consented, raises new challenges of agency, of transparency of decision making, responsibility and liability.

When that robot is able to design its on cryptographic protection and to deploy that against the user and all others, what then?

Let me leave that with you.

We have some time for regional reports tomorrow – we have been told that we will hear from the Article 29 working party, and possibly one other. However, can I invite any other representatives of regional groupings who would like to make a brief intervention to contact the secretariat so we can ensure we make provision for you.

Thank you to all the speakers today, and to Ian Kerr for an intense and illuminating day of curation, moderation and presentation.

Thanks again to our hosts at the CNDP, to the technical assistants and caterers.