38th International Conference of Data Protection and Privacy Commissioners

Robotics and artificial intelligence session (Monday 17 October 2016)

INFORMAL REFLECTIONS ON POLICY QUESTIONS

After 3 expert presentations on robotics and AI, the session moderator posed 6 policy questions for delegates to ponder:

1. What new mechanisms will be required for privacy protection in a world populated by social robots?

2. Can a robot or AI infringe privacy if there is no human intervention or oversight?

3. Will unpredictability/opacity due to machine learning require DPAs to revise accountability mechanisms? How should this be achieved?

4. What can "purpose limitation" do to ensure reliable AI systems that do not disclose beyond our reasonable expectations?

5. How can a special regime for "sensitive data" (gender, ethnicity, religion) contribute to reduce unlawful bias?

6. How can the "right not to be subject to automated decisions" and the "right to an explanation" survive in an AI-saturated environment?

Delegates were invited informally and anonymously to jot down their thoughts in relation to those questions or any privacy priorities in this area. There follows transcripts of 20 responses handed in after the session (the other delegates keeping their thoughts to themselves …).

---oo0oo---

DPA privacy priorities for emerging robotics and artificial intelligence applications

1. We will need to "review" the concept of consent (for data to be used)
2. There needs to always be clear who takes responsibility for the robots activity. Clear mechanism how this is established need to be detailed.
3. If the case of "Guard" as to the robots activity is clear and any responsibility for its activity is established the account should be on this.
4. "Limitless" robots activity should not be allowed, parameters on algorithms and processes should be a precondition in general.
5. The use of special regime should be used strictly and limits as to the openness of specific use of robots should be defined in the sense of familiarity with all the risks of each specific algorithm.
6. We need to define it taking it into account the nature of these technologies (such as the fact, scope of existence of bias, unpredicted use/purpose).

1. More use of preventative tools such as PIA/DPIAs, DPOs, PbD etc. are required for social robots.
2. If privacy in the right to self-determination, than yes, a robot can also infringe it. The question is, 'who is/will be/should be accountable for that and whether we need some new regulation.
3. The "opacity argument" should not be easily accepted. We need accountability not for data but for algorithms as well.
4. Purpose limitation principle must survive in the big data era. Algorithm designers should respect it.
5. Rules for sensitive data must be hard-coded into any design of AI, big data, social robots etc. History has taught us with very dramatic examples of how things can go very wrong when these data are misused.
6. automated decision making rules will be more and more important if not crucial ion the world of AI, big data and profiling. The dictatorship of algorithms should be prevented.

---

1. We are always at data protection principles at the end of the day.
2. No, the data processor is always accountable. A robot should remain only a tool.
3. By cooperation of lawyers and IT-scientists.
4. The purpose limitation is of utmost importance.
5. They should (review) forbidden theme, for processing. Fairness is more than relevant.
6. By cooperation of all: lawyers, IT-scientists, different profiles – including ethics.

---

1. How to address the fundamental issues of data protection and privacy within the emerging Robotics and AI.
2. Privacy by Design.
3. Who controls or owns what information to enable attribution of legal responsibilities and or obligations.
4. Control what decision or information?
5. How do we control behaviour?

---

1. How to state the difference between humansand artificial intelligence (judgment conscience)

1a. And accordingly to it to state limits to development of AI

2. To find out what platforms could be used to bring together data computer scientists and lawyers to analyse the process of working with data and to address this process with appropriate tools to guarantee privacy.
3. Is it possible to separate “general” data from sensitive data?

Further use of collected data, sensitive data processing risks.
Effectiveness of security measures.
Transparency issue
Capacity of DPAs.

Do we need to develop new privacy rules to deal with robotic related privacy concerns or the existing legal framework is good enough?

---

1. Processing by Robotics have to be treated the same as any other processing operation by automatic means. Therefore all DP requirements have to be adopted in the same manner.
2. How is the Data Controller going to be determined?
3. In the case of children, how is consent by parents going to be implemented?
4. How are retention periods going to be observed?

If artificial intelligence is used together with machine learning - to process personal data in unpredicted ways, - with unknown data; how will we then protect the right of date subjects with regard to:

- Consent
- Information
- Control of data?

---

1. Transparency also at the level of Product Specification which should clearly indicate the extent and possibilities for data processing.

2. Information to date subjects shall also be given directly.
3. The clear determination of who will be held responsible for the data processing and whether there will be one or more data controllers.
4. Timely deletion of personal data (or removal of identifiable data) when this is no longer necessary.

---

1. Who is data controller, technology or those who use “the” Technology?
2. Should we regulate technology or use of technology?
3. Why is it so difficult for those who develop new technology to pay attention at least to the basic data protection rules?

Privacy/DPA priorities (in random order):

1. Consistent and coordinated approach by the DPAs to make clear that robotics and AI are not excluded from the general DP principles;
2. Establishing/developing closer links between DPAs and research/technology community, ex. consultative forums, etc.
3. Investing (to the extent possible) into in-house knowledge and skills in DPAs with regard to new technologies, for ex. with the assistance of academic world.

---

1. Clear competences of the DPA
2. Combining IT and legal knowledge
3. Control the inputs as data controllers and evaluate the flow of the data periodically.

Before we try to create new legal mechanisms to cope with privacy and artificial learning and intelligence we should ask in how far traditional principles as

- Transparency of processing and
- Purpose limitation or
- Liability principles e.g. for the *actions* of animals etc.

can do the job

1. Requirement to know:
   - What is happening to whom and when and, for what purpose
   - What engagement is there with those who are the subject of the data.
2. Yes

Our privacy priorities would be:

- Purpose limitation when it comes to training data which is used for machine learning.
- Sensitive personal data when it comes to the possibilities of social service robots (e.g. health data) when it comes to for example the robot interacting with the autistic child (the project in Singapore).

---

1. The designer/creator of AI and robotics be held accountable for the outcome brought about by their creatures, no matter they have control over the outcome.
2. Algorithmic transparency.

<u>Pressing Policy issues arising from Robotics/AI</u>

1. Challenge of getting international consensus on AI conceptual aspects.
2. Capacity building for DPAs – concepts, vocabulary, investigative.
3. Accountability for people who programme or use robots (e.g. driverless cars) when things go wrong – who is at fault? Who will pay? How to set things rights?
4. Will intellectual property laws be an effective bar to transparency of algorithms?
5. Will individual be able to exercise choice to deal with a robot rather than human or vice versa?
6. Persistent surveillance from intelligent sensors.
7. Ethics of defaults for algorithms and transparency of algorithms.
8. Legal capacity, and skills/expertise, to check/audit the 'black box'.

---

1. Purpose of limitation

How to clarify purpose of limitation before AI analyses data set. There are various possibilities that the collected data is used for. Like emerging smart phone, there is an unpredictable possibility as well.

Right to object for such usage is needed when a data subject recognises unpredictable usage of his/her data.

---

1. Prior checking of data processing of social robots.
2. Yes – behind every robot is a human who programme it. The data resources available for other purposes or humans. All this data is vulnerable to be interpreted or stolen.
3. Yes. Standards could be set. Guidelines could be published. Ex-post checking (prompted by complaints) must be conducted.
4. Reasonable expectations is a concept which is too broad.
5. DPA enforcement, strict liability of data controllers.