36th International Conference of Data Protection and Privacy Commissioners

Mauritius Declaration

on the Internet of Things

Balaclava, 14 October 2014

The internet of things is here to stay. Ever more devices are connected to the internet and are able to communicate with each other, sometimes without the user being aware such communications take place. These devices can make our lives much easier. For example in healthcare, transportation and energy the connected devices can change the way we do things. The internet of things however, can also reveal intimate details about the doings and goings of their owners through the sensors they contain.

Self determination is an inalienable right for all human beings. Personal development should not be defined by what business and government know about you. The proliferation of the internet of things increases the risk that this will happen.

The assembled data protection and privacy commissioners have therefore discussed the possibilities of the internet of things and its consequences during the 36th International Privacy Conference held in Balaclava, Mauritius on 13 and 14 October 2014. Four speakers representing both the private sector and academia presented the Commissioners with the positive changes the internet of things may bring to our daily lives as well as the risks. The speakers also took stock of what needs to be done in order to ensure the continued protection of our personal data as well as our private lives.

The subsequent discussion led to the following observations and conclusions:

- Internet of things' sensor data is high in quantity, quality and sensitivity. This means the inferences that can be drawn are much bigger and more sensitive, and identifiability becomes more likely than not. Considering that the identifiability and protection of big data already is a major challenge, it is clear that big data derived from internet of things devices makes this challenge many times larger. Therefore, such data should be regarded and treated as personal data.
- Even though for many companies the business model is as yet unknown, it is clear that the value of the internet of things is not only in the devices themselves. The money is in the new services related to the internet of things and in the data.
- Everyone who lives today will realize that connectivity is ubiquitous. This may apply even more strongly to the young and to future generations, who cannot imagine a world without being connected. It should not though solely be their concern as to whether or not their data is protected. It is a joint responsibility of all actors in society so that the

trust in connected systems can be maintained. To this end, transparency is key: those who offer internet of things devices should be clear about what data they collect, for what purposes and how long this data is retained. They should eliminate the out-of-context surprises for customers. When purchasing an internet of things device or application, proper, sufficient and understandable information should be provided. Current privacy policies do not always provide information in a clear, understandable manner. Consent on the basis of such policies can hardly be considered to be informed consent. Companies need a mind shift to ensure privacy policies are no longer primarily about protecting them from litigation.

- Data processing starts from the moment the data are collected. All protective measures should be in place from the outset. We encourage the development of technologies that facilitate new ways to incorporate data protection and consumer privacy from the outset. Privacy by design and default should no longer be regarded as something peculiar. They should become a key selling point of innovative technologies.
- The internet of things also poses significant security challenges that need to be addressed. A simple firewall is no longer sufficient. One way to minimize the risk to individuals is to ensure that data can be processed on the device itself (local processing). Where this is not an option, companies should ensure end-to-end encryption is in place to protect the data from unwarranted interference and/or tampering.
- The data protection and privacy authorities will continue to monitor the developments in the internet of things. They undertake to ensure compliance with the data protection and privacy laws in their respective countries, as well as with the internationally agreed privacy principles. Where breaches of the law are discovered, they will seek appropriate enforcement action, either unilaterally or through means of international cooperation.
- Taking into account the huge challenges faced by internet of things developers, data protection authorities and individuals, all actors should engage in a strong, active and constructive debate on the implications of the internet of things and its derived big data to raise awareness of the choices to be made.

Jacob Kohnstamm
Chairman of the Executive Committee
of the International Privacy Conference

Drudeisha Madhub
Chairwoman of the Mauritius
Data Protection Office