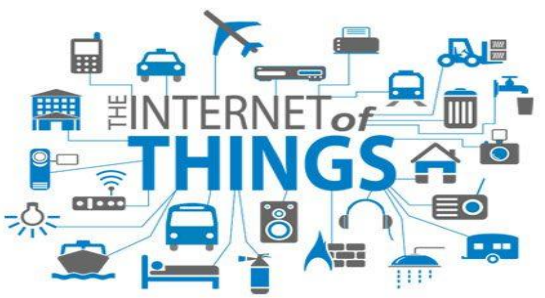
Computer Security Day 2016

Privacy and Internet of Things

Presenter: Drudeisha Madhub
Data Protection Commissioner
30.11.16

Data Protection Office

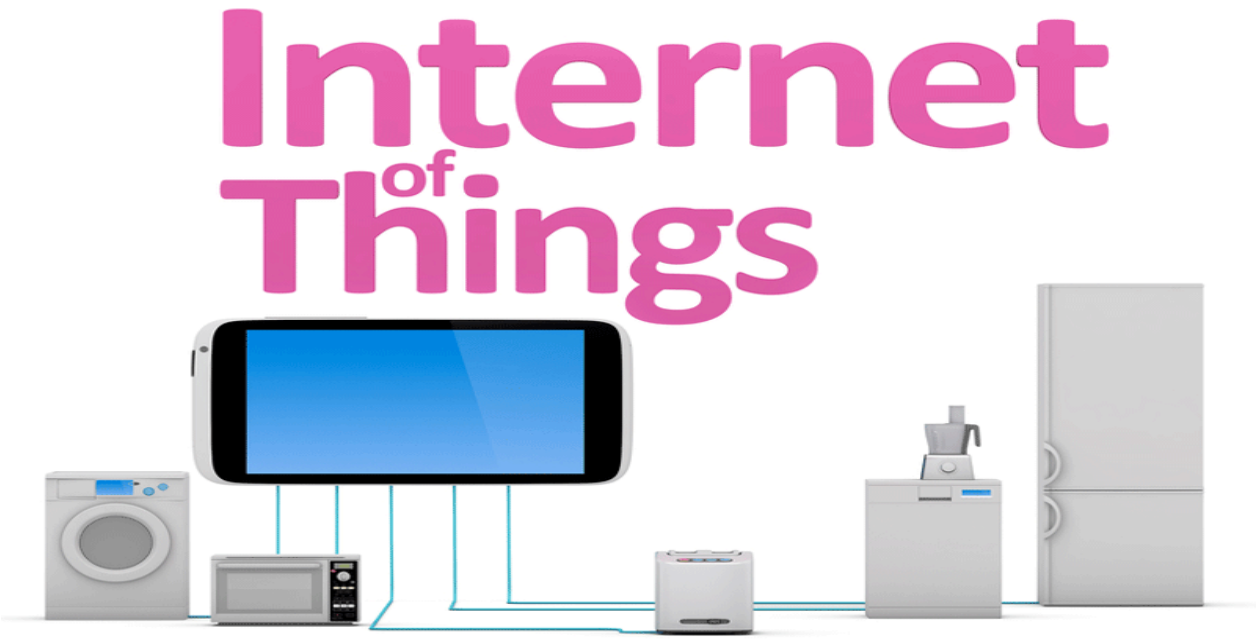
Internet of Things (IoT)



- The IoT is an infrastructure in which sensors embedded in common, everyday devices (“things”) are linked to other objects or individuals and can record, process, store and transfer data as they are associated with unique identifiers which can interact with other devices or systems using networking capabilities.
- IoT can make our lives easier by changing the way we do things.

Internet of Things (IoT)

- However, IoT can also reveal intimate details about the doings and goings of their owners through the sensors that they contain.



Data Protection Office

Do internet enabled devices produce personal data?

- Personal data is any information that identifies or is reasonably likely to identify an individual.
- For some devices, e.g smart phones, the answer can be obvious: Smart phones do process information about a user such as location data.

Data Protection Office

Do internet enabled devices produce personal data?

- For other types of devices such as domestic washing machines, the answer might become less obvious.
- It is therefore very important to consider whether an individual can be identified from the devices to consider the application of the Data Protection Act. The Data Protection Act has mandate on the processing of personal data only.

Data Protection Office

Privacy Risks

1. **Lack of control**

- Users might find themselves under third party monitoring.
- IoT pushed data towards a device manufacturer may not be adequately reviewable by a data subject which can result in excessive self exposure for the user.

Data Protection Office

Privacy Risks

- Communication between objects can be triggered automatically or by default without a data subject being informed about it.
- The inability to define virtual boundaries like active and non-active zones for specific things can result in an uncontrolled flow of data.

Data Protection Office

Privacy Risks

2. Quality of user's consent

- The issue of valid consent may arise as users may not be fully aware of the data processing activities being done by devices.
- Users might face difficulty to distinguish between a normal device and a connected device (IoT). For instance, a user might not know that he is buying a watch with monitoring devices such as embedded cameras, microphones and motion sensors.

Privacy Risks

- Inability for users to renounce or opt out from certain features of an IoT device.

Data Protection Office

Privacy Risks

3. Usage of data for totally different purposes

- With the increase in the amount of data produced by IoT and new ways in analysis and cross matching of data, there are greater risks that data can be used for secondary purposes, often unknown to the user.

Data Protection Office

Privacy Risks

4. Behaviour Patterns and Profiling

- Sufficient amount of data from different objects can reveal aspects of an individual's habits and behaviours.
- This can affect the way an individual behaves. It also invades the most private sphere of an individual's life, including his home. For instance, it might influence a person to avoid non-usual behaviour to prevent the detection of what might be considered as anomalies. This can therefore trigger considerable intrusions in the private life and intimacy of individuals.

Privacy Risks

5. Inability to remain anonymous

- An IoT environment can reduce the possibility of people to remain unnoticed.
- For example, sensors collecting location data can be used to analyse movement of pattern of crowds and individuals.

Data Protection Office

Privacy Risks

6. Security risks

- IoT devices and platforms exchange data on the service provider's infrastructure. Therefore, security risks arise not only on the devices but also on the communication links, storage infrastructure and other inputs of the ecosystem.

DPO Data Protection Office

Privacy Risks

- Also, an IoT ecosystem has different levels of processing where the technical design and implementation can be provided by different stakeholders. Inadequate coordination between stakeholders may create weak points that can be used to exploit vulnerabilities in an IoT system.

Stakeholders in the IoT ecosystem

Examples of stakeholders might be:

- Device manufacturer
- Device owner
- Device user
- Operating System Developer
- Device Software Developer
- Online service provider(e.g. web server)
- Advertising Network

Data Protection Office

Stakeholders in the IoT ecosystem

- The complex mesh of stakeholders involved asks for/implies the necessity of a precise allocation of legal responsibilities among them with regard to the processing of individual's personal data, based on the specificities of their respective interventions.

Data Protection Office

Recommendations

1. Innovation in Privacy information

Mauritius Data Protection Act

- Under section 24 of the DPA, no personal data shall be processed unless the data controller has obtained the express consent of the data subject.

Data Protection Office

Recommendations

- Consent of data subjects is not required only where the processing is necessary:

(a) for the performance of a contract to which the data subject is a party;

(b) in order to take steps required by the data subject prior to entering into a contract;

(c) in order to protect the vital interests of the data subject;

(d) for compliance with any legal obligation to which the data controller is subject;

(da) for the purpose of making use of a unique identification number to facilitate sharing information and avoid multiple registrations among public sector agencies;

(e) for the administration of justice; or

(f) in the public interest.

Data Protection Office

Recommendations

Article 5(3) of Directive 2002/58/EC (the e-Privacy directive) for European Council:

Member States shall ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC, inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller. This shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user.

Recommendations

- This provision demands that the user consents to such storage of access for these actions to be legitimate, unless they are strictly necessary to provide a service explicitly requested by the user. This is important because stakeholders other than the user can have access to privacy sensitive information stored on the devices.

Recommendations

- Therefore, data controllers acting in the IoT(first and foremost device manufacturers) must :

➢ provide clear and comprehensive information to users about the identity of the controller, type of sensors, the information it captures, the purpose of the data capture, the recipients of the data, the user's right of access to data and

➢ ensure that users consents for such processing.

Data Protection Office

Recommendations

- Example: A pedometer records the number of steps made by its user and stores this information. The user has an application on his computer to download the number of steps from this device. If the device manufacturer wants to upload data from the pedometer to its servers, he must obtain the consent of the user.

Recommendations

- In addition, manufacturers can use a combination of different methods to provide privacy information. For example, a device manufacturer can use both an interface on the device as well as its website to provide information on the devices.
- IoT devices may be shared by several data subjects or even rented. A setting should be available to distinguish between different individuals using the same device.

Data Protection Office

Recommendations

2. Legitimate Processing

- IoT stakeholders must ensure that processing is legitimate and is necessary for the performance of a contract to which the data subject is party. There must be a direct and objective link between the processing and the purposes of the contractual performance expected from the data subject.

Data Protection Office

Recommendations

3. Data Quality

- Using the minimisation principle, IoT devices should not collect and store data "just in case" or because "it might be used later".
- Also, when personal data is not necessary to provide a specific service to run on the IoT, the user should at least be offered the possibility to use the service anonymously.

Data Protection Office

Recommendations

- Every stakeholder in the IoT should ensure that once a user has put an end to his subscription, his personal data should be deleted.

Data Protection Office

Recommendations

4. Sensitive Data

- Explicit consent should be taken from users if sensitive data is being processed. For instance, if a company has developed an application that can analyse raw data from electrocardiograms to detect drug addiction patterns, then the company has to obtain the user's explicit consent, unless the data subject has made the data public himself.

Data Protection Office

Recommendations

5. Security

- Privacy protections should be inbuilt in IoT devices using ‘‘ Privacy by Design’’.
- Privacy Impact Assessment should be performed to ensure a realistic appraisal of privacy risks.
- Device manufacturers should provide simple tools to notify users when security vulnerabilities are discovered and a way of fixing them.

Data Protection Office

Recommendations

- Secure encrypted communications should be used to protect data in transit.
- It may also happen that if someone discovers a security flaw in the device's software, it might not be clear whose responsibility it will be to fix it or how the fix would be applied. If no action is taken, such a flaw could allow an attacker to compromise the device.

Data Protection Office

Recommendations

- Software support should be provided throughout the lifetime of the device. This solution however depends on at least 2 conditions which could be difficult to fulfil in practice: firstly, the continuing availability and willingness of developers to maintain the software ad secondly the ability of consumers to easily apply any software updates.

Data Protection Office

Recommendations

6. Right of access

- Users must be able to exercise their rights and thus be “in control” of the data at any time.
- A data subject may write to a data controller to obtain information about whether data kept by the data controller includes personal data related to the data subject, the purposes for processing data and the recipients to whom the data are disclosed.

Data Protection Office

Recommendations

7. Possibility to withdraw consent/oppose

- Device users must be provided with the possibility to revoke any prior consent given to data processing.

Example

A user installs a connected fire alarm with additional features such as an occupancy sensor, an ultrasonic sensor and a light sensor. The user should be provided with the possibility to disable those sensors that are not required to make use of the fire alarm.

Data Protection Office

Recommendations

- The methods for withdrawing consent should be understandable to the user and as user-friendly as possible.
- Device manufacturers should be able to communicate to all other IoT stakeholders involved as soon as a data subject withdraws his consent or opposes the data processing.

Data Protection Office

36th International Conference Mauritius Declaration

- During the International Conference of Data Protection and Privacy Commissioners in Mauritius in 2014, representatives of the private sector and academia joined together to discuss the positive changes and risks that the Internet of Things may bring to daily life.

Data Protection Office

36th International Conference Mauritius Declaration

- The Mauritius Declaration on the Internet of Things are summarised below:
- Self-determination is an inalienable right for all human beings.
- Data obtained from connected devices is “high in quantity, quality and sensitivity” and, as such, “should be regarded and treated as personal data.”

Data Protection Office

36th International Conference Mauritius Declaration

- 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.
- Those offering connected devices “should be clear about what data they collect, for what purposes and how long this data is retained.”

Data Protection Office

36th International Conference Mauritius Declaration

- Privacy by design should become a key selling point of innovative technologies.
- Data should be processed locally, on the connected device itself. Where it is not possible to process data locally, companies should ensure end-to-end encryption.

Data Protection Office

36th International Conference Mauritius Declaration

- Data protection and privacy authorities should seek appropriate enforcement action when the law has been breached.
- All actors in the Internet of Things ecosystem “should engage in a strong, active and constructive debate” on the implications of the Internet of Things and the choices to be made.

Data Protection Office

Conclusion

- IoT is here to stay.
- But the Internet of Things raises important concerns with regard to the privacy of the individuals and civil rights which should be addressed.

Data Protection Office

References:

https://ico.org.uk/media/about-the-ico/consultation-responses/2014/2512/ico-response-to-ofcom-consultation-on-internet-of-things-20141001.pdf

http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf

https://www.insideprivacy.com/international/data-protection-officials-adopt-internet-of-things-declaration-and-big-data-resolution/

Data Protection Office

Thank You

Data Protection Office

Address : 5th Floor, Happy World House,
Port Louis
Email : pmo-dpo@govmu.org
Tel: 2122219, 2122218

Data Protection Office