2016 GPEN Sweep – Internet of Things

(with a focus on accountability)

Background

The 2016 GPEN Sweep aimed to examine the practices of organisations internationally in respect of how they communicate privacy related matters to their customers and data subjects, focusing specifically on Internet of Things (IoT) devices. With more and more devices and services becoming linked to the internet, the topic of IoT is of great importance to Privacy Enforcement Agencies (PEAs). Devices are now allowing people to control and monitor many aspects of their lives, from tracking their fitness to turning on their central heating from their mobile phone. IoT devices have the potential to collect a large amount of personal data from users, and it is important that users are fully informed about what is happening with their information.

A variety of methodologies were used in the Sweep, including but not limited to:

Note: The number of PEA's using each method is shown below:

- Examination of online privacy communications and materials available to potential users of a product (i.e. before purchase) – *21 PEAs*.
- Communication with companies directly – verbally and in writing – *14 PEAs*.
- Examination of devices – looking at what information is provided with the product and how privacy matters work in practice – *9 PEAs*.

PEAs chose to focus their Sweep on types of device that were of particular interest or relevance to them. Different types of devices examined by PEAs included (amongst others):

Note: The number of PEA's examining the different device types are shown below:

- Smart meters – *2 PEAs*
- Usage Based Insurance (UBI) devices -*1 PEAs*
- Fitness wearables – *10 PEAs*
- Household aids – *6 PEAs*
- Connected medical/health devices (e.g. blood pressure monitors, sleep monitors) – *11 PEAs*
- Connected cars – *1 PEA*
- Connected toys – *1 PEA*
- Smart TVs - *2 PEAs*

- Transponders - *1 PEA*
- CCTV – *1 PEA*

Summary Observations

Privacy communications relating to IoT devices are generally poor and fail to inform users about exactly what personal information a device may collect from them and what subsequently happens to the information. In particular, companies neglect to explain how information is stored and how a user is able to delete their personal information. On the whole, devices collect a large amount of personal data (although the amount differed between different types of devices, with some collecting very little); however privacy communications are generally not device-specific. Companies demonstrating good practice were in the minority and Sweepers generally felt that overall there is significant room for improvement of privacy communications.

Tombstone Data

Data Protection Authorities who submitted results: 25
Devices/companies: 314

Types of companies examined
Manufacturer: 179
Retailer: 20
Distributor: 7
Provider: 18
Local Government: 79
Marketer: 4
Other data controllers: 7

***Methodology Note**: Not all Data Protection Authorities ("DPAs") reported on every reporting field. As a result, the statistics for this Sweep were developed based on the actual data received for a reporting field as a percentage of those apps/websites swept by those DPAs that reported on that field.*

Collection, use and disclosure of data (Indicator 1)

Sweepers indicated that 59% of devices/companies failed to adequately explain to customers how their personal information was collected, used and disclosed.

The following information (plus other sector-specific information) was collected either on a mandatory or optional basis by the device examined:

- Name – 84% of devices
- Email – 83% of devices
- Date of birth/age – 64% of devices
- Location – 68% of devices
- Address – 53% of devices
- Phone number – 55% of devices
- Photograph/video/audio file – 41% of devices
- Unique device identifier – 61%

Certain types of device also collected more sensitive information, for example, connected medical devices and some fitness wearables collected medical details from users. Many also collected information about users' weight and height.

Trends identified in relation to indicator 1:

- Privacy policies were often not specific to devices. Many were designed to cover a number of services provided by the organisation and some focused on user interactions with the website rather than the design or operation of the devices themselves.
- In many cases, privacy policies provided examples of data that *may* be collected rather than listing everything.
- Some organisations tended to interpret "personal data" narrowly to only include the obvious (e.g. name, phone number, address, etc), and failed to recognise that other information such as the number of steps taken and calories burnt could also be personal data if it was attributed to an identified individual. For example, an appliances functioning data (energy consumption, trends/timing in use, etc), home environmental data (temperature, pressure, humidity, heat detection), shopping path.
- Often the user experience did not necessarily match the privacy communications.
- Some devices collected sensitive personal data (particularly health-related and medical devices), yet did not give special mention to this in their privacy policies.
- Some sweepers noted that the collection of personal information was sometimes unexpected because companies failed to provide the reason for collection – for example, while it was expected that healthy living devices would need to collect certain health related information (e.g. the blood pressure monitor would need to collect blood pressure readings), sweepers were less certain about why there was a need to collect other types of personal information such as location and date of birth.

- Sweepers were encouraged that some companies who provide a vast array of products supplemented their generic privacy policies with more detailed device/sector-specific policies (e.g. policies specifically for fitness wearables).
- Sweepers were impressed that some companies had used a privacy-by-design approach.
- Although lacking in details, in some cases privacy policies were clear, concise and written in plain language.
- Sweepers were impressed that some organisations included "just-in-time" privacy communications to users at the time they inputted their personal information, informing them of why the information was required.

Storage of data (Indicator 2)

Sweepers indicated that 68% of devices failed to properly explain to customers how the information collected by their device is stored. Furthermore, 68% also stated that the company failed to mention whether the personal data collected by the device was stored in an encrypted form.

In many privacy policies, sweepers noted that storage was completely omitted, or if mentioned, details were vague. Policies rarely informed users about how long their data is stored for, in which country it is stored, and in what form (e.g. is it stored on the device itself, in a cloud, etc.?).

Just 49% of devices failed to inform users about how their personal information was being safeguarded and what was being done to prevent unauthorised users from accessing the data (e.g. passwords protections or authentication questions).

Contact details (Indicator 3)

Sweepers indicated that 38% of devices failed to provide easily identifiable contact details that customers could use should they have any privacy concerns.

Given the amount of information that some devices collect, users should be confident that if they have concerns, these can be quickly relayed to the appropriate person/team within the organisation.

Deletion of data (Indicator 4)

Sweepers indicated that 72% of companies failed to explain how a user could delete their personal data from the device/app. Only 17% provided

information about tools available to users to clear their device of personal data should they decide to sell it/no longer use it. Similarly, only 13% provided information about tools to help users wipe their data remotely, in the event that the device is lost or stolen.

Sweepers reported that in many cases, deletion processes were often complicated. In some cases, users were unable to delete data/their account via the app, but could do it via the website. Similarly, in some cases, when users were informed about how to deactivate their account, the company failed to explain what this involved and whether this also meant that their data would be deleted.

Timely, adequate and clear responses from organisations (Indicator 5)

Sweepers noted that many organisations were often late in their responses to questions and many failed to respond altogether. Indeed, 43% of companies contacted failed to provide timely, adequate and clear responses. Three PEAs indicated that they had a response rate of 50% or less and one PEA advised that they had received zero responses.

Conclusion

In summary, privacy communications relating to IoT devices are generally poor, and fail to fully inform users about what happens to the personal data collected by their device. These GPEN Sweep findings are consistent with other studies. For example, in a recent study of health and wellness apps, the Future of Privacy Forum found that a significant number of apps fail to provide customers with basic notices about how their personal data is be collected, used and shared. PEAs continue to encourage organisations to improve their practices by ensuring users are able to understand how their data is treated at each stage of the process; collection, use, disclosure and storage. Users should also be informed about how they can control their information, for example how they can delete their data should they wish.

Other findings

- There is a noticeable presence on the market of devices that link multiple users (e.g. to compete in challenges or to link family members calendars or phones).
- Some devices/apps had functionality for sending test results to the doctor, or anyone for that matter, using common unencrypted e-mail.

- Some devices had a default setting at the least privacy protective level, e.g. accessibility by 'everyone', rather than user-specified groups, unique connections or the user alone (other than as needed to support device functionality).