[redacted]

September 30, 2014 3:55 PM

[espc-announce] For Your Legal Departments: EU WP29 on the Internet of Things

---

All –

Please pass this along to your legal departments.

The Article 29 Working Party (WP29) issued an Opinion on the Recent Developments on the Internet of Things (IoT) at its September 16, 2014 plenary meeting. The opinion is available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf. The WP29 defines IoT as an infrastructure in which billions of sensors embedded in common, everyday devices are designed to record, process, store and transfer data and, as they are associated with unique identifiers, interact with other devices or systems.

The WP29:

(1) Recognizes the potential benefits of "smart things" available to EU citizens that monitor and communicate with their homes, cars, work environment and physical activities;
(2) Underlines the many privacy and security challenges which can be associated with the IoT; and
(3) Provides a set of practical recommendations addressed to the different IoT stakeholders.

The WP29 calls for the incorporation of the "highest possible" privacy and data protection guarantees for individual IoT users, which should include measures to help the users remain in complete control of their personal data throughout the product lifecycle. In addition, when organizations rely on consent as a basis for processing, the consent should be fully informed, freely given and specific. All stakeholders should perform Privacy Impact Assessments (PIAs), based on the WP29's 2011 Privacy and Data Protection Impact Assessment Framework before any new applications are launched in the IoT.

Scope of the Opinion

The WP29 focuses in this opinion on:

- Wearable Computing (clothes, glasses, watches, etc. with embedded cameras, microphones and sensors);
- Quantified Self (performance and physical state devices used by individuals who want to records information about their own habits and lifestyles, such as sleep or fitness trackers); and
- Domotics (devices placed in offices or homes, such as connected light bulbs, thermostats, smoke alarms, weather stations, washing machines, ovens, baths and other appliances).

Even though the opinion does not specifically deal with B2B applications and more global issues like "smart cities," "smart transportations," and M2M (machine to machine) developments, the principles and recommendations in this opinion may apply outside its strict scope and cover these other IoT developments.

The WP29 specifically addresses and differentiates between the following stakeholders:

- Device manufacturers: The WP29 notes that most manufacturers collect and process personal data generated by IoT devices for purposes and means wholly determined by manufacturers and as such they qualify as companies responsible for data processing (data controllers).
- Social platforms: The WP29 notes that when users publish their data on social platforms, social networks may use the data for their own purposes and as such also qualify as data controllers (e.g., a social network may use information collected by a pedometer to infer that a particular user is a regular runner and shows him/her ads about running shoes).
- Third part application developers: The WP29 notes that some applications may reward users. For example, a home insurance company could develop a specific application to make sure that their clients' connected fire alarms are correctly configured. Unless the data are properly anonymized, such access constitutes processing of personal data, so the app developer should be considered a data controller.
- Third parties other than device manufacturers and third party application developers: The WP29 noted that such other third parties may also use IoT devices. For example, health-insurances may wish to give pedometers to customers to monitor how often they exercise and adapt their insurance premiums accordingly.
    - Although such third parties may have no control over the type of data collected, they qualify as data controllers for so far as they collect and store the data generated by the devices for their own specific purposes.
- IoT data platforms: The WP29 notes that manufacturers have progressively developed platforms in order to host the data collected, and centralize and simplify data management.
    - Such platforms may also qualify as data controllers, when the development of such services actually implies that they collect the users' personal data for their own purposes.

Recommendations

The WP29 notes that the recommendations to the different stakeholders below provide guidance that is additional to earlier documents adopted by the WP29, and in particular the earlier recommendations on apps on smart devices (Opinion 02/2013).

- **Recommendations for *all* Stakeholders:**
    - A PIA, based on the 2011 Privacy and Data Protection Impact Assessment Framework, should be performed before any new applications are launched in the IoT;
        - Where appropriate/feasible, stakeholders should consider making the relevant PIA available to the public at large, and specific PIA frameworks could be developed for particular IoT ecosystems (such as smart cities);
    - Considering that many IoT stakeholders only need aggregated data, they should delete raw data as soon as they have extracted the data required for their data processing;

    - As a principle, deletion should take place at the nearest point of data collection of raw data, for instance on the same device after processing;
- The principles of Privacy by Design and Privacy by Default should be applied;
- Individuals/users should be empowered to exercise their rights and thus be "in control" of the data at any time according to the principle of self-determination of data;
- Providing notice, offering a right to refuse or requesting consent should be done in as user-friendly manner as possible;
    - In addition, notice and consent should focus on information which is understandable by the user and should not be confined to a general website privacy policy; and
- Devices and applications should be designed so as to inform users and non-users, for example, via the device physical interface or by broadcasting a signal on a wireless channel.

· **OS and Device Manufacturers should:**

- Inform users about the type of data that are collected by sensors and further processed, the types of data that they receive and how it will be processed and combined;
- Be able to communicate to all other stakeholders involved as soon as an individual/user withdraws his consent or opposes the data processing;
- Provide granular choices when granting access to applications, which should not only concern categories of collected data but also the time and frequency at which data are captured;
    - IOT devices should offer a "do not collect" option to schedule or quickly disable sensors;
- Limit device fingerprinting by disabling wireless interfaces when they are not used, or use random identifiers (such as random MAC addresses to scan Wi-Fi networks) to prevent a persistent identifier from being used for location tracking;
- Provide tools to locally read, edit and modify the data before they are transferred to any data controller, and store personal data processed by a device in a format allowing data portability;
- Provide a user-friendly interface or tools for users who want to obtain both aggregated and/or raw data stored, in order to guarantee individual's right of access to his/her personal data;
- Provide simple tools to notify users and other stakeholders and to update devices when security vulnerabilities are discovered. Users should be made aware when a device becomes deprecated and is no longer updated;
- Follow a Security by Design process and dedicate some components to the key cryptography primitives;
- Limit as much as possible the amount of data leaving devices by transforming raw data into aggregated data directly on the device;
- Make a setting available to distinguish between different individuals using the same device so that they cannot learn about each other's' activities;
- Work with standardization bodies and data platforms to support a common protocol to express preferences with regard to data collection and processing; and
- Enable local controlling and processing entities (the so-called personal privacy proxies) allowing users to have a clear picture of data collected by their devices and facilitating local storage and processing without having to transmit the data to the device manufacturer.

· **Application Developers should:**

- Design notices and warnings to frequently remind users that sensors are collecting data;
    - When the application developer does not have a direct access to the device, the app should periodically send a notification to the user to let him know that it is still recording data;
- Facilitate the exercise of user's rights of access, modification and deletion of personal information collected by IoT devices;
- Provide tools so that users can export both raw and/or aggregated data in a standard and usable format;
- Pay special attention to the types of data being processed and to the possibility of inferring sensitive personal data from the data collected; and
- Apply a data minimization principle: when the purpose can be achieved using aggregated data, developers should not access the raw data and follow a Privacy by Design approach.

· **Social Platforms should:**

- Set up default settings of social applications based on IoT devices that would ask users to review, edit and decide on information generated by their device before data publication on social platforms; and
- Not have information published by IoT devices on social platforms public by default, or have it indexed by search engines.

· **IoT Device Owners and Additional Recipients should:**

- Obtain informed and freely given user consent and not economically penalize or degrade user access to the capabilities of his/her device if a user decide not to use a specific service;
- Put users whose data is being processed in the context of a contractual relationship (i.e., a hotel, a health-insurance or a car renter) in a position to administrate the device;
    - Irrespective of the existence of any contractual relationship, any non-user must also be put in a position to be able to exercise his/her rights of access and opposition; and
- Make sure that users of IoT devices inform non-users whose data are collected of the type of data collected through an IoT device. They should also respect individual's preference not to have his/her data collected by the device.

· **Standardization bodies and Data Platforms should:**

- Promote portable and interoperable as well as clear and self-explanatory data formats in order to facilitate both: (i) transfers of data between different parties; and (ii) helping data subjects understand what data is actually being collected on them by IoT devices;
- Not only focus on the format for raw data but also on the emergence of formats for aggregated data;
- Promote data formats that contain as few strong identifiers as possible in order to facilitate proper anonymization of IoT data;
- Work on certified standards that would set the baseline for security and privacy safeguards for data subjects; and
- Develop lightweight encryption and communication protocols adapted to the specificities of IoT, guaranteeing confidentiality, integrity, authentication and access control.

+ + +

Best regards,

Reed

==========