La protection des données du Quantified Self et de l'IoT

Dr Florent Frederix
On-line Trust and Cyber-Security
Direction Réseaux de communication, contenu et technologies
Commission européenne
Content

- Quantified Self (QS)
- (Sensitive) Personal data
- Security risks QS
- Privacy risks QS
- Art. 29 Working Party (WP29) on QS
- WP29 on eHealth
- WP29 on Internet of Things (IoT)
- QS data at risk in the IoT
- WP29 recommendation on the IoT
What is Quantified Self (QS)?

WP29 => Wearable Computing, Quantified Self and Domotics:

• **Wearable Computing**: objects and clothes with sensors.

• **Quantified Self**: objects carried by individual to record data on lifestyle.

• **Domotics**: sensors that record when a user is at home, patterns of movement .... and may transmit data.

Reference: WP29 opinion on the Internet of Things
(Sensitive) Personal Data

Ethnic origin... **health** .... qualify as “**sensitive data**”.

Art. 8 of Dir. 95/46/EC ... **explicit user consent**...

**QS devices** mostly register not health data, yet may provide information about the **individual’s health** as the data is registered in time.
Security risks of QS devices

Example: US ICS-CERT now checks everything (pacemakers, defibrillators...)

Some findings: a heart pump and some cardiac implants have security flaws that make them vulnerable to hacking.

Privacy risks of Quantified Self

Example:
Google Glass raised many privacy concerns led to being banned in certain public locations.

Working Party 29 on QS

Independent body on data protection
Art. 30 of 95/46/EC, Art. 15 of 2002/58/EC.

Addressed QS in 8/2014 "Opinion on Recent Developments on the Internet of Things" and in Data protection for eHealth applications (February 2015).
WP29 on Quantified Self

A pedometer storing step data for a few days does not process 'health data'. But an application combining several years' of records of an individual is processing health data.
WP29 on Quantified Self

If the data controller provides a remote platform to collect and process data, the domestic exception only applies to the actual usage by the user and does not exempt the data controller from the data protection law (WP163, WP223).
The combination of location data with other information read from the device would still make it necessary for the data controller to obtain the consent of the data subject.

(Art. 7(a) & Art. 5(3) of the ePrivacy Directive)
WP29 on the Internet of Things

IoT can develop **unlawful form of surveillance** and raise **security concerns** (*WP29 Opinion 8/2014*)

The interaction between objects will result in **hardly manageable data flows** challenging the protection of the data subjects’ rights.
Quantified Self and the IoT

IoT stakeholders qualifying as data controllers must comply with 95/46/EC and 2002/58/EC.

Art. 5(3) of 2002/58/EC applies if an IoT stakeholder can access information stored on an IoT “terminal equipment” and demands that the subscriber/user consents. This is important because it can give others access to privacy-sensitive information stored on such devices.
WP29 recommendations on IoT

- **PIA required** for IoT applications.
- IoT Stakeholders must **delete raw data as soon as they extracted the aggregated data** required for their data processing.
- Principles of **Privacy by Design** and **Privacy by Default** apply.
- Data subjects must be able to exercise their rights and "in control" of the data at any time.
WP29 requirements for OS and Device manufactures

• inform stakeholders if data subject withdraws consent

• provide granular access choices and a “do not collect” option

• prevent location tracking
WP29 requirements for OS and Device manufactures

• provide tools to locally read, edit and modify the data before they are transferred to any data controller.

• inform everyone impacted by a discovered device vulnerability
WP29 requirements for OS and Device manufactures

- apply **Security by Design** and **Cryptography**
- limit data leaving devices and aggregate
- protect data of **different individuals** using same device
A note on the new Data Protection Legislation

• Data Protection Regulation will replace Dir. 95/46/EC

• New Data Protection Regulation currently discussed in Council

• Italian presidency report on proposal (December 2014) is > 200 pages
References

- Dir. 95/46/EC on Privacy and Data Protection
- Dir. 2002/58/EC on e-Privacy
- Art. 29 Working Party Opinion 8/2014 on Recent Developments on the Internet of Things
- Art. 29 Working Party Opinion 5/2010 on online social networking
- Privacy and Data Protection Impact Assessment Framework adopted on 12 January 2011 for RFID Applications by the Art. 29 Working Party