Wearable Devices are Going Mainstream: Are Consumers Poised for a Privacy Nightmare?

(a very) Brief Legal Perspective

Applicable Law | Risks | Possible solutions

By *Carolina Moura*

16th Annual Privacy and Security Conference | Canada 13 Feb 2015

Introduction

- A consumer may engage in processing of personal data with **no commercial purpose** through the usage of Social networks, Google Glass, video surveillance, quadcopters, etc..
- According to the EU Data Protection Law is a consumer liable ?
- What are the risks consumers may face?
- What can stakeholders do to minimize those risks?

1. Applicable law (material scope)

- Both the Directive 95/46/CE as well as the Future General Regulation are not applicable to the processing of personal data by a consumer in the course **of its own exclusively personal or household activity.**
- **Consumers are subject to EU LAW,** namely, if they
  - disclose personal data on the internet to unlimited number of people (Lindqvist case C-101/01 EUCJ)
  - record images in public places for security purposes (Rynes case C-212/13 EUCJ)
- Conclusion: Consumers can be **data controllers** too.

1. Applicable law (territorial scope)

- Directive 95/46/CE (art. 4) is applicable if:
  - the *processing is carried out* ***in the context of the activities of an establishment of the controller on the territory of the Member State***;
    - Google v. M Costeja Gonzalez (Case 131/12 EUCJ) - wide definition of establishment
  - ***the controller is not established in Community territory*** *and, for purposes of processing personal data* ***makes use of equipment****, (…) situated on EU territory* (…).
    - Smart watches, tablets, mobile phones, glasses, etc.
- Conclusion: EU Law is likely to be applicable in the majority of cases

2. Obligations under EU Law

- Legal basis to process personal data
- Data Protection Principles
  - Processing shall be **fair** and **lawful**
  - Data shall be collected and further processed for a **specific**, **explicit** and **legitimate purpose**
  - Data collected shall be **proportional** and only the **necessary**
  - Data shall be **accurate**
  - Data shall be **retained only** for the **necessary period** to comply with the purpose for which the data was collected
  - Personal data shall be protected with **security measures**

3. Risks

- Lack of Legal base for the processing of personal data
  - **Consumer's consent**
    - Informed | Specific or unambiguous | *Freely Given*
  - **Necessity for the performance of a contract** to which the data subject is party
  - **Necessity** to comply with legitimate interests
    - **Consumers' Right to Privacy is likely to override companies legitimate interests** (Google Case 131/12 EUCJ)
  - Situation of sensitive data made public – lack of consumer's awareness
- **Conclusion: in this context processing of personal data may be illegal**

3.1 Risks

- Lack of information and control over
  - What personal data is collected?
    - The **strictly necessary?** | Data minimization - Art. 6.º/1/c)
  - For what purpose?
    - For a **specific**, **explicit** and **legitimate** purpose? - Art. 6/1/b)
      - If from the data collected is possible to infer **secondary information** that is used for an incompatible purpose – the user may not feel confortable with sharing this secondary information
  - Is the data shared? | With whom?
  - What rights do I have?
    - Right of access | Possibility to withdraw consent and to oppose
  - Who is the responsible?
- Breach of the obligations of information | Data transparency – Art. 10.º

3.2 Risks

- Security risks
  - Controllers have the **responsibility** to implement *appropriate* technical and organizational measures to protect personal data (art. 17 of the Directive)
    - The data collected can reveal specific and private aspects of individual's **habits**, **behaviours** and **preferences** (such as when one is likely to be at home) with personal security implications
    - Security flaws
    - Unlawful surveillance

4. Some solutions - Consumers

- Consumers
  - Education - should be taught from an early age
    - Importance of the right to data protection and the right to a private life in the interconnected world
    - How to protect those rights
  - Accountability
    - Users should inform non-user data subjects whose data may be collected of the presence of a wearable device
      - What data is collected? For what purpose? To be shared? With whom?
    - Users should respect non-user data subjects' preference not to have their data collected

4.1. Some solutions - Stakeholders

- Audits and Privacy Impact Assessments
- Data minimization
- Privacy by design | by default
  - Design to inform both users and non-user data subjects of the processing of data
  - "Do not collect" option
  - Information published "*by wearable devices*" on social platforms should, by default, not be public nor be indexed by search engines
- User empowerment
  - E.g. Tool to locally read, edit and modify data before transfer to data controller
  - To allow data portability
- User Friendly Methods to obtain consent and inform of security vulnerabilities
- Settings that distinguish between different individuals using the same device

4. Thank you

Carolina Moura

cmoura@proj-d.com

+353 83 157 0 157 | carolinafilipemoura/en

More information:
Please see: European Union WP29 Opinion 8/2014 on the recent developments on the Internet of Things – 16 Sep 2014 – available at www.ec.europa.eu