ITU Kaleidoscope 2015

Trust in the Information Society

DRONES. CURRENT CHALLENGES AND STANDARDISATION SOLUTIONS IN THE FIELD OF PRVACY AND DATA PROTECTION

Presenters:

Cristina PAUNER University Jaume I, pauner@uji.es

Irene KAMARA, Vrije Universiteit Brussel, Irene.kamara@vub.ac.be

Jorge VIGURI, University Jaume I, jviguri@uji.es

Barcelona, Spain
9-11 December 2015

CRISP

Evaluation and Certification Schemes for Security Products

DRONES. CURRENT CHALLENGES AND STANDARDISATION SOLUTIONS IN THE FIELD OF PRVACY AND DATA PROTECTION

Cristina Pauner
University Jaume I (Spain)
Irene Kamara
Vrije Universiteit Brussel (Belgium)
Jorge Viguri
University Jaume I (Spain)

1. INTRODUCTION

- Nowadays, EU data protection legislation does not cover new threats posed by new products, services and systems (specially RPAS or drones).
- How can a drone be defined in legal terms? Wide range of applications with unlimited functionalities.

Current problems:

- Lack of a common and consistent framework. The EU legislation is widely fragmented, which leads to legal uncertainty.
- What personal data should be protected? Unknown.
- Lack of mutual recognition for national certificates.
- *"Self-regulation through certification may be an alternative to detailed legislation, but not to all legislation".*

2. CHALLENGES POSED BY DRONES TO THE FUNDAMENTAL RIGHTS TO PRIVACY AND DATA PROTECTION

- *2.1. The impact of drones on the right to privacy*

- No general concept of privacy (depending on social and technological factors) but fundamental right and an element of human dignity.
- The right to privacy interferes with other rights or liberties (freedom of expression or right to association).
- Potential problems: the combination of technologies embodied in drones allow a totally new type of surveillance, that is likely covert or hidden, highly intrusive and potentially permanent on persons and objects.
- **Widespread concerns about the potential damages that drones may cause to privacy.**

2. CHALLENGES POSED BY DRONES TO THE FUNDAMENTAL RIGHTS TO PRIVACY AND DATA PROTECTION

2.2. The impact of drones on the right to data protection

- Inability to determine general risks on the right to data protection.
- Risk assessment:
  - **Lack of transparency** in the collection, storage, and even further transmission and data processing.
  - **Lack of purpose specification and function creep.** Personal data need to be collected for specific purposes and they cannot be processed in an incompatible way with those purposes for which the data are intended.
  - **Ensure data security, integrity and confidentiality**. Required security measures shall be implemented and personal data which is not strictly needed must be removed or anonymised.
  - **Profiling**. The process of assembling bulk data may create disproportionately large datasets which may lead to discrimination by identifying individuals or social groups for adverse treatment based upon flawed assumptions.

3. STANDARDISATION OF DRONES: A DEVELOPING FIELD

Several activities related to drones:

- EC Roadmap on civil RPAS – new legislation expected by end 2015
- EASA – “Concept of operations”
- EUROCAE – 2 working groups (WG-73 on UAV systems and the WG-93 on Light Remotely Piloted Aircraft)
- JARUS – Certification specification
- ISO –ISO/TC20/SC 16 on UAS (8 participants, 4 observers)

Need for regulation of drones

(legislation/ self-, co-regulation, other)

4. STANDARDISATION OF DRONES: A DEVELOPING FIELD

Existing Privacy-related Standards/ mandates	Topic	Areas/Risks still to be covered
ISO/IEC 29100:2011	Privacy terminology& high level privacy principles	Terminology related to drones/RPAS/UAV and their capabilities
ISO/IEC 29101:2013	Information Technology–Security Techniques–Privacy Architecture Framework	1.vast collection of big data (flying capability for a long time over large areas) 2. function creep and 3. security of all the collected and transmitted data
European Commission Standardisation request M/530	Privacy by Design- security products/systems	Data protection risks related to recreational/commercial use of drones → not in scope
OASIS Privacy Management Reference Model (PMRM)	privacy management functionality and compliance controls	Privacy management for drones needs extra care to accountability, transparency issues, data minimisation, data subject rights (access, rectification, erasure)
OASIS Privacy by Design Documentation for Software Engineers	translates the PbD principles to conformance requirements within software engineering tasks	Generic conformance requirements might require many more requirements to "stricter" jurisdictions (i.e. EU)

CRISP
Evaluation and Certification
Schemes for Security Products

5. RECOMMENDATIONS

- Drones impact on privacy and data protection is not yet certain because it is known as a new emerging technology.
- GDPR is intended to replace Data Protection Directive to strengthen the existing legal framework. However, it is not intended to cover all current and future challenges.
- In order to achieve a consistent legal framework, other forms of governance are outlined in this paper:

    a. EU data protection legislation must remain technology neutral in order to be suitably flexible. Other mechanisms such as guidance and recommendations developed by DPAs and delegated acts by the EC should be also implemented.

    b. The use of standardisation activity in the sector of drones as a proactive measure shall be encouraged.

    c. Certification schemes will need to be developed for the systems to operate safely and with due regard for third party interests.

Thank you

Questions?

pauner@uji.es

Irene.kamara@vub.ac.be

jviguri@uji.es