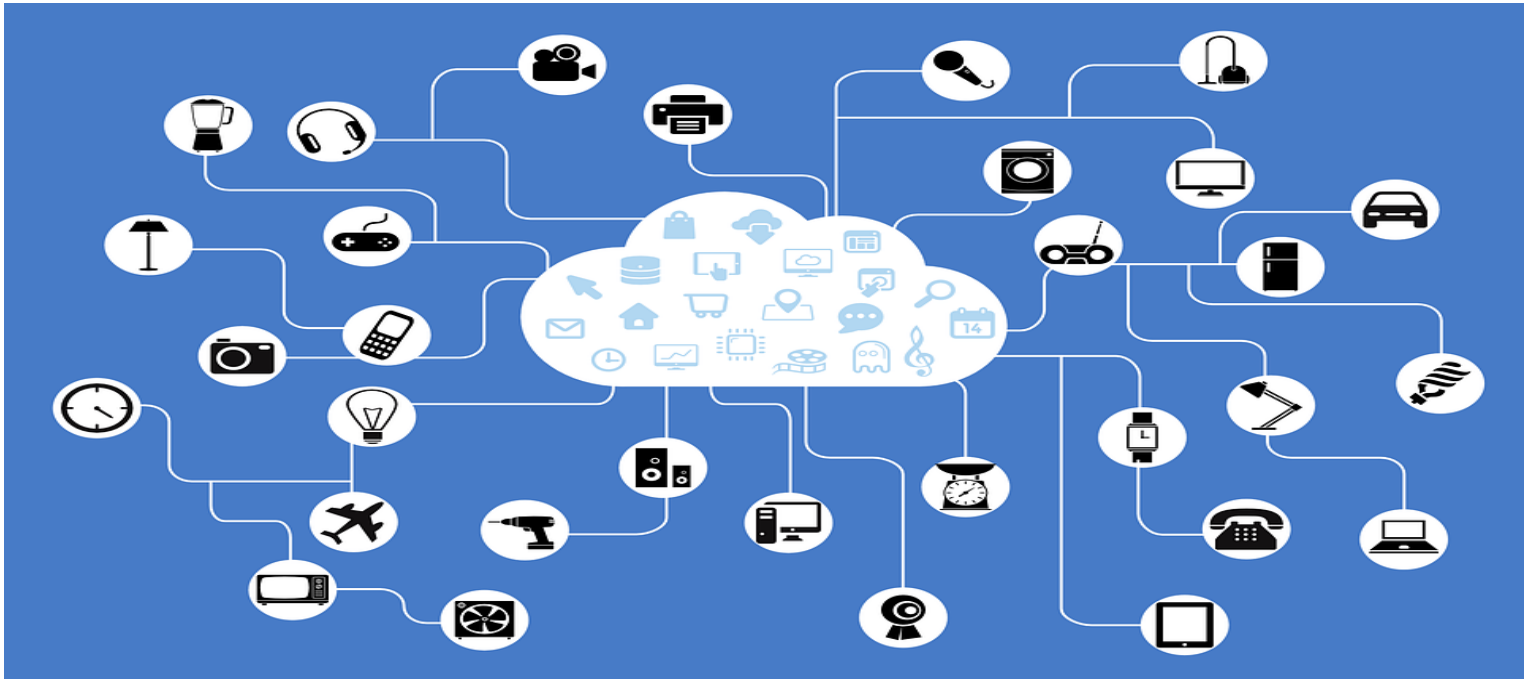
EU data protection issues in the Internet-of-Things (IoT) (or Internet of Everything)

Francesca Giannoni-Crystal (fgiannoni-crystal@cgcfirm.com)



IoT is subject to the general data protection law

- Currently: **Directive 95/46/EC** (“Directive”), available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML
- Soon: General Data Protection Regulation (“GDPR”), expected entry into force Spring 2018, available at http://data.consilium.europa.eu/doc/document/ST-5455-2016-INIT/en/pdf

EU Authorities on IoT

WP29's Opinion 8/2014 on the Recent Developments on the Internet of Things, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf

Privacy challenges in the IoT (as identified by the WP29)

- 1. *Lack of control and information asymmetry*

  – IoT, with its pervasive and “unobtrusive” presence, might cause data subjects to lose control under several perspectives and result basically in a “third-party monitoring.”

Privacy challenges in the IoT (as identified by the WP29)

- 2. *Quality of the user's consent*

  – EU law requires consent for the legitimate processing of personal data (save exceptions). Consent is a major problem with the IoT because often (i) often users are not aware that a specific object is collecting data (ii) the possibility to decline certain services or features of an IoT device is more theoretical than real.

Privacy challenges in the IoT (as identified by the WP29)

- 3. *Inferences derived from data and repurposing of original processing*

  – The problem is that data collected by a specific device might be insignificant (e.g. accelerometers and gyroscope of smartphones), but this raw information might allow the controller to “infer” much more significant information (for example, driving habits)

Privacy challenges in the IoT (as identified by the WP29)

- 4. *Intrusive bringing out of behavior patterns and profiling*
  - Due to the "proliferation of sensors," a vast amount of separate (maybe insignificant) pieces of information will be collected and continuously cross-matched with one another, which "reveal specific aspects of individual's habits, behaviours and preferences." IoT stakeholders will be able to create general profiles of users.

Privacy challenges in the IoT (as identified by the WP29)

- 5. *Limitations on the possibility to remain anonymous when using services*.
  - With the IoT everyone is traceable
  - Why? Think of wearable devices (e.g., smart watches), used in close proximity to data subjects so that they are able to collect “identifiers” (e.g., MAC addresses of other devices) that can track the location of users.

Privacy challenges in the IoT (as identified by the WP29)

- 6. *Security risks*

Privacy challenges in the IoT (as identified by the WP29)

- 6. Why cybersecurity risk is higher in IoT environment?
  - Manufacturers prefer battery efficiency over security;
  - the number of “security targets” will dramatically increase;
  - Need of multilevel cybersecurity multilevel, which involve securing devices, “communication links, storage infrastructure” and the entire IoT “ecosystem”
  - Since more IoT stakeholders involved to provide a service, need to provide cybersecurity coordination among them.

Privacy challenges in the IoT (as identified by the WP29)

– Above IoT challenges are not uniquely European.

Relevant EU data protection principles

- Data from things is often “personal data” (therefore subject to the general data protection) pursuant to Article 2(a) of Directive 95/46/EC because individuals are likely to be identified from that data.
- Also in case of pseudonymisation or anonymisation because “the large amount of data processed automatically in the context of IoT entails risks of re-identification.” Opinion on IoT at 10.

Relevant EU data protection principles

– Data subjects are not only the subscribers of an IoT service or the users of a device but also individuals that are neither subscribers nor users, such as people whose data is collected by wearables (such as smart glasses), sometimes without being aware of.

Relevant EU data protection principles

- At least the following provisions of Directive 95/46/EC are relevant:
- - *Article 7 (legitimate data processing).* Opinion on IoT at 14-16. Note that “Lawfulness of processing” is in Article 6 of the new GDPR.
  - The main avenue for a legitimate data processing is data subject consent. Article 7(a). Consent must have the characteristics specified by WP29’s Opinion 15/2011.
  - Alternatives to consent possible.

Relevant EU data protection principles

- *Article 6 (fair and lawful data collection and processing)*.
  - "minimization" principle
- *Article 8 (processing of sensitive data).*

  - "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and … concerning health or sex life". Consent required (very limited exceptions).

  - Under GDPR wider definition - now includes genetic and biometric data.

Relevant EU data protection principles

- *Articles 10 and 11 (transparency requirements).*
  - Data controllers must provide users with a privacy policy in a "clear and comprehensible manner."
    - Challenging with the IoT and might require new methods of delivery. Opinion on IoT at 18. E.g., on the object itself using the wireless connectivity to broadcast the information.

See Article 14 and 14(a) GDPR. The characteristics of the information are listed in Article 12 GDPR.

Relevant EU data protection principles

Article 17 (security requirements).

- Any data controller remains fully responsible for security of the data processing even when more than one IoT stakeholder intervenes in the delivery of service.
- New security principles from GDPR (Article 30)
  - (i) security breach: data controller responsible if breach results from poor design or maintenance of device;
  - (ii) security assessments: “of system as a whole, including at components’ level.” Opinion on IoT at 18.
  - Data breach notification duty to the supervisory authority within 72 hours (Article 31).

Relevant EU data protection principles

Cybersecurity recommendations from WP29:

- Data controllers must supervise subcontractors that design and manufacture devices which are not processors (not bound by Article 17) and must seek “high security standards with regard to privacy.”
- Use of principle of “data minimization”;
- “Network restrictions, disabling by default noncritical functionalities, preventing use of un-trusted software update sources” ;
- adherence to a “privacy by design” principle.

Relevant EU data protection principles

Cybersecurity recommendations from WP29 (cont'd)

- automatic updates to patch vulnerabilities always available to users OR alternatives offered (e.g., open-source) AND and notification to users of vulnerability.
- Security of IoT devices tracking health values must be particularly protected.
- Data breach notification policies useful to contain the consequences of vulnerabilities in software and design.

Relevant EU data protection principles

- Rights of data subjects: the same they have in non-IoT environment (*e.g.*, Articles 12 and 14), particularly the right of access, the right to withdraw consent, and the right to oppose the processing.
  - Access to raw data should be granted to users. Opinion on IoT at 20. Access to data is to switch to another provider (avoiding the lock-in).
  - GDPR provides a "right to portability". Article 18 GDPR:
    - The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured and commonly used and machine readable format and have the right to transmit those data to another controller without hindrance from the controller to which the data have been provided.

Relevant EU data protection principles

- IoT stakeholders must also comply with Article 5(3) of Directive 2002/58/EC (consent to storage in E-Privacy Directive).
  - Unless storage or access (by IoT stakeholder) is “strictly necessary in order to provide a service explicitly requested by the subscriber or user,” consent is necessary.

Mauritius Declaration and other important authorities

Mauritius Declaration on the Internet of Things. adopted on October 14, 2014 inside the 36th International Conference of Data Protection and Privacy Commissioners ("Mauritius Declaration"), http://www.privacyconference2014.org/media/16596/Mauritius-Declaration.pdf.

Mauritius Declaration and other important authorities

Mauritius Declaration highlights:

- individuals' right to self-determination;
- drawing of broader and more sensitive inferences form the huge quantity of data;
- Identifiability;
- ubiquitous connectivity which requires trust in a connected world. To maintain trust, transparency is key.

Mauritius Declaration and other important authorities

Concerns of Commissioners:

- Lack of clarity of information (which data is collected, for which purpose and retention policy);
  - informed consent;
- privacy by design and by default still not use
- Lack of encryption. End-to-end encryption necessary.

Mauritius Declaration and other important authorities

- ENISA, *Privacy and Data Protection by Design – from policy to engineering December 2014,* available at https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-and-data-protection-by-design.
  - privacy needs to be considered from the very beginning of system development. For this reason, [Dr. Ann] Cavoukian [former Information and Privacy Commissioner of Ontario, Canada] coined the term “Privacy by Design”, that is, privacy should be taken into account throughout the entire engineering process from the earliest design stages to the operation of the productive system.

Mauritius Declaration and other important authorities

- Report discusses also
  - "privacy/data protection by default," meaning that "in the default setting the user is already protected against privacy risks."
  - "privacy design strategies"
  - several privacy techniques including authentication, attribute based credentials, secure private communications like encryption, and communications anonymity and pseudonymity.

Mauritius Declaration and other important authorities

DPAs' positions on IoT:

- Italian DPA (Garante per la Protezione dei Dati Personali), *Avvio della Consultazione Pubblica su Internet delle Cose (Internet of Things)* - Deliberazione del 26 marzo 2015, doc. web n. 3898704, available in Italian at http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3898704
- UK DPA (ICO), *The Information Commissioner's Office response to the Competition & Markets Authority's call for information on the commercial use of consumer data*, https://ico.org.uk/media/about-the-ico/consultation-responses/2015/1043461/ico-response-to-cma-call-for-evidence-on-consumer-data-20150306.pdf.

Mauritius Declaration and other important authorities

DPAs' positions on IoT (cont'd):

- Spanish DPA, *Resolución de 20 de noviembre de 2015, de la Agencia Española de Protección de Datos, por la que se aprueba el Plan Estratégico 2015-2019*, available in Spanish at http://www.agpd.es/portalwebAGPD/LaAgencia/common/Resolucion_Plan_Estrategico.pdf.
- French DPA (Commission Nationale de L'informatique et des Libertés – CNIL), Rapport d'Activite' 2014, in French at https://www.cnil.fr/sites/default/files/typo/document/CNIL-35e_rapport_annuel_2014.pdf.pdf, discussing smart cars and smart cities.

More information

- Francesca Giannoni-Crystal & Allyson Haynes Stuart, *The Internet-of-Things (#IoT) (or Internet of Everything) – privacy and data protection issues in the EU and the US*, Information Law Journal, Spring 2016, volume 7 issue 2, available at http://apps.americanbar.org/dch/committee.cfm?com=ST230002

- www.technethics.com (TAG IoT: http://www.technethics.com/tag/iot/)

Contacts

✧**Francesca Giannoni-Crystal** (NY, DC, Italy, and SC foreign legal consultant- not a member of SC Bar)

Crystal & Giannoni-Crystal, LLC
(www.cgcfirm.com)
fgiannoni-crystal@cgcfirm.com

Crystal

Lawyers for Lawyers and International Matters