

Privacy Challenges in the Internet of Things (IoT) – a European Perspective



Alicja Gniewek, PhD Student
Interdisciplinary Centre for Security, Reliability and Trust
Weicker Building, Université du Luxembourg
Postal Address 4, rue Alphonse Weicker
L-2721 Luxembourg
Email alicja.gniewek@uni.lu
Telephone (+352) 46 66 44 5834

Internet of Things – new and dangerous?

- ❑ 25 billion Internet-connected devices by 2015
- ❑ 40% of data will come from sensors by 2020
- ❑ Bringing convenience in all areas: car industry, health, home appliances, clothes etc.
- ❑ Solving societal problems: managing energy consumption, traffic, enable advancements in health care...

Internet of Things – new and dangerous?

INTERNET

'Internet of Things' holds promise, but sparks privacy concerns

Kitchens ordering food, washing machines turning on when energy demand on the grid is



Daniel Newman
Contributor

CMO NETWORK 8/20/2014 @ 10:15AM | 3,062 views

There Is No Privacy On The Internet Of Things

+ Comment Now + Follow Comments

Over the last month there has been an unfathomable amount of



Home | Video | Themen | Forum | English | DER SPIEGEL | SPIEGEL TV | Abo | Shop | Schlagzeilen | Wetter

SPIEGEL ONLINE NETZWELT

Politik | Wirtschaft | Panorama | Sport | Kultur | Netzwelt | Wissenschaft | Gesundheit | einestages | Karriere | Uni | Reise | Aut

Nachrichten > Netzwelt > Web > Internet der Dinge > Kühlschrank verschickt Spam: Botnet-Angriff aus dem Internet der Dinge

Internet der Dinge: Kühlschrank verschickte Spam-Mails

Von Matthias Kremp

Sécurité : de l'Internet des objets à l'Internet des vulnérabilités ?
Nous entrons tout doucement dans l'ère des objets connectés, de l'Internet des objets. Et il serait temps, peut être, de se soucier de la question de la sécurité de ces objets.
Par Fabien Soyez @FabienSoyez / vendredi 17 janvier 2014

Obwieszeni elektroniką. Jak przedmioty zarządzają ludźmi
Gazeta Wyborcza / Artykuły
Krzysztof Majdan / 02.06.2014 - aktualizacja 07.06.2014 15:20

AAA

Problematic areas – legal perspective

Huge amounts of data

Sensitive data

Detailed profiles

Constant 'surveillance'

Invisible 'tracking'

Control over
data

Consent

Purpose
of data
processing

Re-use of data

Anonymity
and security

Question of control in the IoT



- Loss of control as a result of diminished transparency of data processing
- Massive amounts of different data → how to handle them?
- Automatic communications between objects → no place for traditional control
- Outcome: Loss of control over data and their subsequent use

Consent and IoT?



- No place for the *informed consent* in the situation of 'no-control'
- Problem of „invisible” objects: e.g. wearable computing (signposting?)
- No opt-out (full or partial) for certain services
- Problem of obtaining consent (place and form for implementing consent mechanisms)

Secondary use of data



- Secondary use of data (and inconsistency with primary purpose)
- Getting new kinds of data via aggregation and advanced analysis (process unknown to the data subject?)

Profiling and behavioural pattern



- Aggregating trivial and anonymous data (+profiles)
- Detection of additional data via analytics
- Other: Influence on the people's behaviour

Anonymity?



- Numerous data available as „fingerprints” of individuals that may be later combined with other data
- Increasing difficulty of being anonymous
- Increased security problems – breaches, leakages, hacking etc.

EU data protection law

Current state: Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

+ Member States' implementations

Discussed: Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)

Selected principles of data processing:

- Data shall be collected and processed fairly and lawfully
- Data can only be collected for specified, explicit and legitimate purposes (purpose limitation)
- Collected data shall be strictly necessary for the determined purpose (data minimisation) and kept no longer than it is necessary



securityandtrust.lu

EU law: Article 29 Working Party

*The **Article 29 Data Protection Working Party** was set up under the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the **protection of individuals** with regard to the processing of personal data and on the **free movement** of such data. It has **advisory** status and acts **independently**.*

(http://ec.europa.eu/justice/data-protection/article-29/index_en.htm)

Opinion 8/2014 on the Recent Developments on the Internet of Things, adopted on 16 September 2014

Recommendations for all the stakeholders

Delete as soon as possible
all raw data and use only
data required for your
processing

Allow users to fully
exercise their rights
and be „in control”

Apply principles of
Privacy by Design and
Privacy by Default

Inform about the data
processing (e.g. policies) in
a user-friendly way

Design devices in a way
that will enable informing
users about data
processing

Recommendations for the manufacturer

Inform about the types of data collected and received as well as about the processing and combining

Inform about the change of user's consent

Security by design
(+ key cryptography)

Allow user to make choice (granularity)

Disable wireless interfaces or use random identifiers (no fingerprinting)

Changing raw data to aggregated data already on the device

Enable user's access to data (format, user-friendly interface)

Develop tools to inform users about vulnerabilities (info of no further updates)

Allow to locally read, edit and modify data before transferring them to controller (+ data portability)

Work towards standards

Enable personal privacy proxies

Enable differentiation between different users of one device

Recommendations for the application developers

Frequent users' notices and warnings about data collection

Enable data-subjects to export raw and aggregated data (standard and usable format)

Enable full exercise of right of access, modification and deletion of personal data

Pay attention to the types and sensitivity of data (also inferred)

Apply the data minimisation principle (provider should not have an access to the raw data if it is possible)

Follow Privacy by Design principle

IoT device owners/3rd parties

Consent must be
informed and freely given

Data subject should be able
to administrate the device

No economic or other
penalties for the opt-out
(partial or full)

Non-users should be
informed about the IoT
devices and types of data
collected

Conclusions – EU approach

EU approach underlines:

- Privacy by Design principles need to be integrated
- Application of ‘purpose limitation’ and ‘data minimisation’ principle
- User should be informed fully about the processing (data/processing itself)
- User should be ‘in control’ (administration, opt-out etc.)

General conclusion: Article 29 WP applies rather rigidly the EU law to the new situation of data processing. They rely on the assumption that the privacy principles will be integrated in the design of the IT solutions.

Conclusions – US approach

FTC underlines best practices (see: FTC 2012 Privacy Report):

- Privacy by Design
- Deidentification + public commitment not to try to re-identify data
- Effective transparency of developers

Future Privacy Forum (An US think tank) suggests:

- Traditional application of FIPPs is not practical
- Need for flexibility with regards to ‘notice and choice’ (no notice in case of the known context of processing, processing on own device, notice available after start of the processing)
- Need for data anonymization
- Transparency, automated accountability mechanisms, codes of conduct, reasonable access to data



Thank you
for your attention.

Alicja Gniewek
alicja.gniewek@uni.lu