Home > PM+: Technology is 'as much a part of the solution as the problem' in securing data privacy
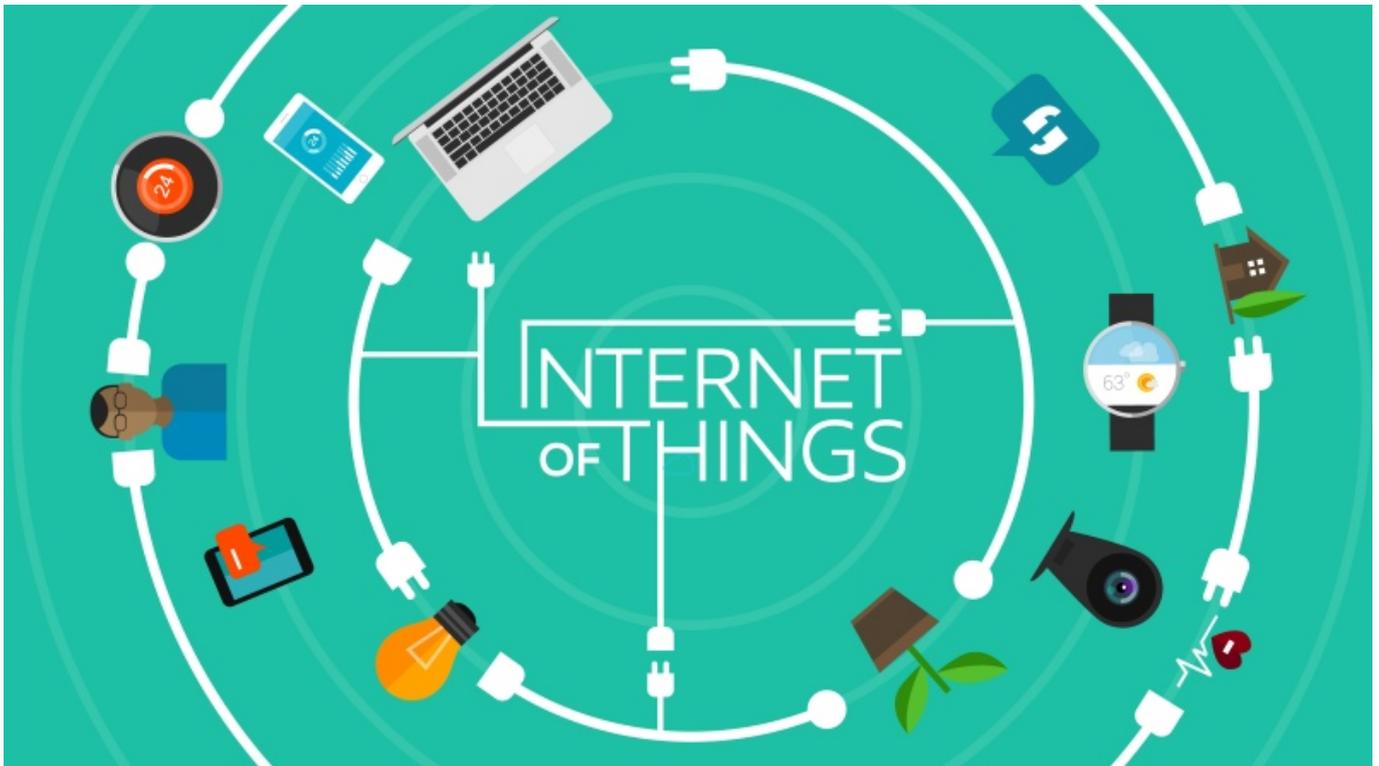
PM+: Technology is 'as much a part of the solution as the problem' in securing data privacy

Written by Ioannis Krontiris on 16 March 2015 in Opinion Plus
Opinion Plus

If we design 'with privacy in mind' we can embrace the internet of things as a step towards more, not less, individual freedom, writes Ioannis Krontiris.

The world is changing fast. More data is being collected, processed and transferred than ever before, leading to new economic and social value being created.

The future internet of things will, according to estimates, connect nearly 26 billion devices by 2020 and lead to many new applications. Cars, homes, buildings, along with whole cities, industries and large-scale infrastructure such as transport and energy networks will start collecting data to serve our needs better.

The new services enabled by these connections will reach into every aspect of our lives – from leisure (think fitness gear) to health and safety (think monitors for elderly people).

"The future internet of things will, according to estimates, connect nearly 26 billion devices by 2020 and lead to many new applications"

A large amount of this data will be collected passively via systems and sensors, without people realising or being able to control it. This will create massive privacy challenges, particularly from a data protection law perspective.

Let's take the case of mobile devices. With more than six billion people using them, an increasingly large variety of data is produced and linked to their identity.

Smartphones are now able to capture and track an individual's location patterns, while wearable personal-health devices can measure daily physical activities helping individuals set wellness targets, measure progress and engage more effectively in achieving healthier lifestyles.

So with all this sensing, we can 'see' so much more about people, leading unavoidably to several privacy challenges.

For example, the data could be forwarded to third parties (e.g. insurance companies or advertising companies) to create more granular profiles of people, or they could be used in other ways to divide and discriminate people.

From a technical point of view, two key aspects need to be considered early on if we want to reap the full benefits of the internet of things without compromising on privacy.

Progress does not necessarily involve choosing between innovation and privacy. On the contrary, rather than undermining established principles, technological advances will enable us to better safeguard them – by offering novel ways to protect data, or to control what we release.

Examples of this are innovative ways of obtaining a user's notice and consent, as well as advanced anonymisation algorithms.

The internet of things is being created to serve the individual, not the other way round. To address the new challenges of hyper-connectivity, we must move towards a user-centric approach where the individual ultimately determines the fate of their personal data.

"Progress does not necessarily involve choosing between innovation and privacy"

This triggers the fundamental question of what exactly is 'our' data. Many smart sensors and devices are very simple, and the data they collect is not personal.

However, personal information can be inferred from raw sensing data when later processed, as well as when aggregated with other datasets.

Faced with a complex ecosystem of market players (including data brokers, analysis companies, third party advertisement companies, and more) and large quantities of 'raw' data, how can we provide individuals with the ability to control their data?

Again, technology is as much a part of the solution as it is part of the problem. Appropriate regulatory frameworks and mechanisms to ensure compliance with these frameworks are crucial – but they are not enough.

Applications and services within the internet of things must be designed with privacy in mind from the beginning: this is what we call 'privacy by design'. Also, new and upcoming solutions that enable users to control the collection, management, and disclosure of their personal data can help increase transparency, awareness, and the engagement of users with their data.

If we can empower individuals to make conscious decisions about how they want to use their data, while ensuring that safeguards are in place to protect privacy, we can embrace the internet of things as a step towards more, not less, individual freedom.

About the author

Ioannis Krontiris is a privacy expert at Huawei's European research centre in Munich, Germany

Tags
[Digital Agenda](#) [1]
[Research and Innovation](#) [2]
Categories
[Science, technology and research](#) [3]

Site Sections

- [Home](#)
- [Content](#)
- [Policy](#)
- [Magazines](#)
- [PM+](#)
- [Thought Leader](#)
- [Climate Crisis](#)
- [Editorial Calendar](#)
- [Policy Events](#)
- [Event Coverage](#)
- [MEP Awards 2020](#)
- [Contact Us](#)

Services

[Dods People](#)[Dods Monitoring](#)[Dods Research](#)[Dods Events](#)[Dods Training](#)

Source URL: https://www.theparliamentmagazine.eu/articles/partner_article/pm-technology-much-part-solu-ion-problem-securing-data-privacy

Links
[1] https://www.theparliamentmagazine.eu/tags/digital-agenda
[2] https://www.theparliamentmagazine.eu/tags/research-and-innovation
[3] https://www.theparliamentmagazine.eu/categories/science-technology-and-research