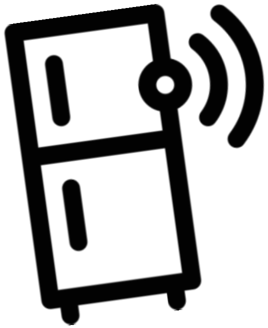
Department of Science, Technology, Engineering and Public Policy (STEaPP)

Who's Afraid of the Big Bad Smart Fridge: Governance Challenges of the Internet of Things



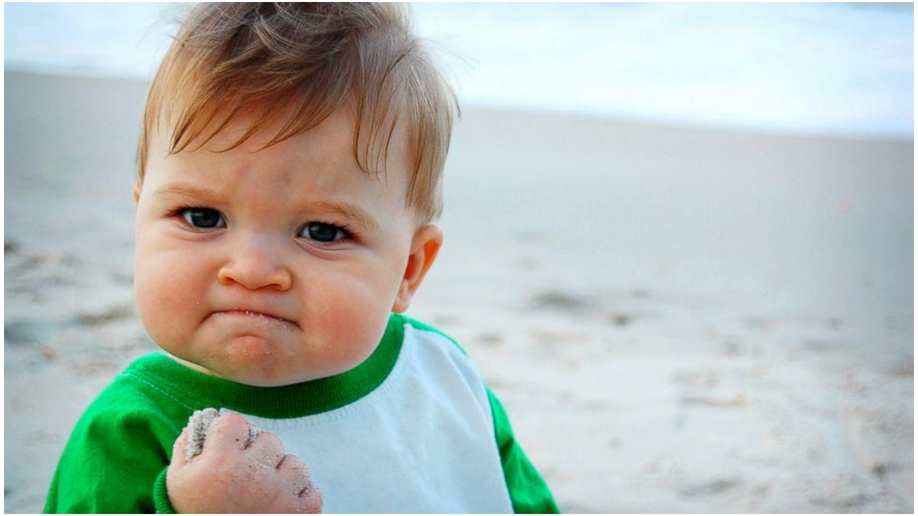
Dr Leonie Maria Tanczer
University College London
@leotanczt

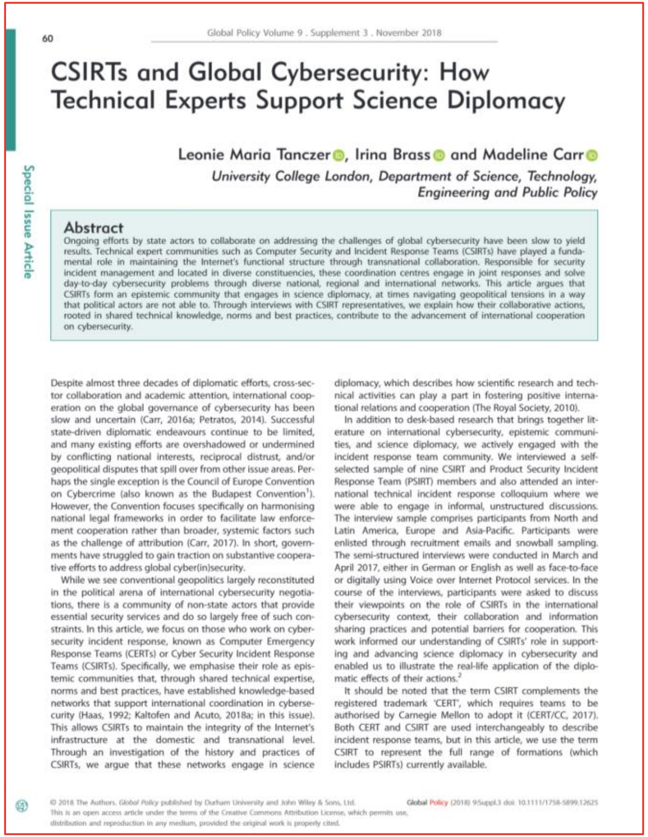
Dear XYZ,

I am, together with my colleagues, working on a study that aims to examine the practices of ***CSIRTs/PSIRTs****.*

Our team is, therefore, reaching out to CSIRTs/PSIRTs all over to world and would be delighted if you or someone in your team would be willing to conduct a ***brief interview with us****.*

We beat the peer-review!





Special Issue Article

CSIRTs and Global Cybersecurity: How Technical Experts Support Science Diplomacy

Leonie Maria Tanczer, Irina Brass and Madeline Carr

University College London, Department of Science, Technology, Engineering and Public Policy

Abstract

Ongoing efforts by state actors to collaborate on addressing the challenges of global cybersecurity have been slow to yield results. Technical expert communities such as Computer Security and Incident Response Teams (CSIRTs) have played a fundamental role in maintaining the Internet's functional structure through transnational collaboration. Responsible for security incident management and located in diverse constituencies, these coordination centres engage in joint responses and solve day-to-day cybersecurity problems through diverse national, regional and international networks. This article argues that CSIRTs form an epistemic community that engages in science diplomacy, at times navigating geopolitical tensions in a way that political actors are not able to. Through interviews with CSIRT representatives, we explain how their collaborative actions, rooted in shared technical knowledge, norms and best practices, contribute to the advancement of international cooperation on cybersecurity.

Despite almost three decades of diplomatic efforts, cross-sector collaboration and academic attention, international cooperation on the global governance of cybersecurity has been slow and uncertain (Carr, 2016a; Petratos, 2014). Successful state-driven diplomatic endeavours continue to be limited, and many existing efforts are overshadowed or undermined by conflicting national interests, reciprocal distrust, and/or geopolitical disputes that spill over from other issue areas. Perhaps the single exception is the Council of Europe Convention on Cybercrime (also known as the Budapest Convention[1]). However, the Convention focuses specifically on harmonising national legal frameworks in order to facilitate law enforcement cooperation rather than broader, systemic factors such as the challenge of attribution (Carr, 2017). In short, governments have struggled to gain traction on substantive cooperative efforts to address global cyber(in)security.

While we see conventional geopolitics largely reconstituted in the political arena of international cybersecurity negotiations, there is a community of non-state actors that provide essential security services and do so largely free of such constraints. In this article, we focus on those who work on cybersecurity incident response, known as Computer Emergency Response Teams (CERTs) or Cyber Security Incident Response Teams (CSIRTs). Specifically, we emphasise their role as epistemic communities that, through shared technical expertise, norms and best practices, have established knowledge-based networks that support international coordination in cybersecurity (Haas, 1992; Kaltofen and Acuto, 2018a; in this issue). This allows CSIRTs to maintain the integrity of the Internet's infrastructure at the domestic and transnational level. Through an investigation of the history and practices of CSIRTs, we argue that these networks engage in science diplomacy, which describes how scientific research and technical activities can play a part in fostering positive international relations and cooperation (The Royal Society, 2010).

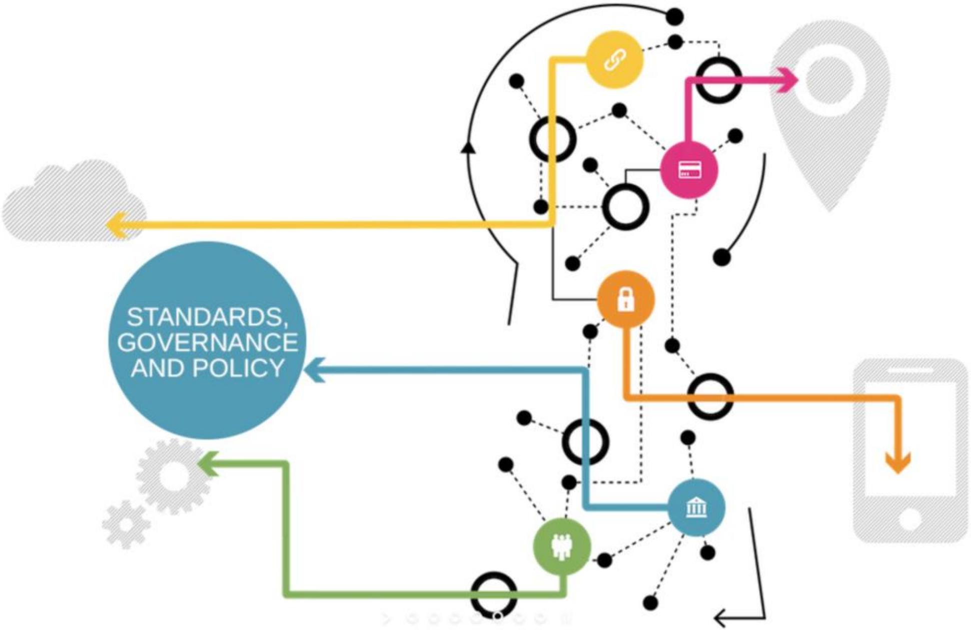
In addition to desk-based research that brings together literature on international cybersecurity, epistemic communities, and science diplomacy, we actively engaged with the incident response team community. We interviewed a self-selected sample of nine CSIRT and Product Security Incident Response Team (PSIRT) members and also attended an international technical incident response colloquium where we were able to engage in informal, unstructured discussions. The interview sample comprises participants from North and Latin America, Europe and Asia-Pacific. Participants were enlisted through recruitment emails and snowball sampling. The semi-structured interviews were conducted in March and April 2017, either in German or English as well as face-to-face or digitally using Voice over Internet Protocol services. In the course of the interviews, participants were asked to discuss their viewpoints on the role of CSIRTs in the international cybersecurity context, their collaboration and information sharing practices and potential barriers for cooperation. This work informed our understanding of CSIRTs' role in supporting and advancing science diplomacy in cybersecurity and enabled us to illustrate the real-life application of the diplomatic effects of their actions.[2]

It should be noted that the term CSIRT complements the registered trademark 'CERT', which requires teams to be authorised by Carnegie Mellon to adopt it (CERT/CC, 2017). Both CERT and CSIRT are used interchangeably to describe incident response teams, but in this article, we use the term CSIRT to represent the full range of formations (which includes PSIRTs) currently available.

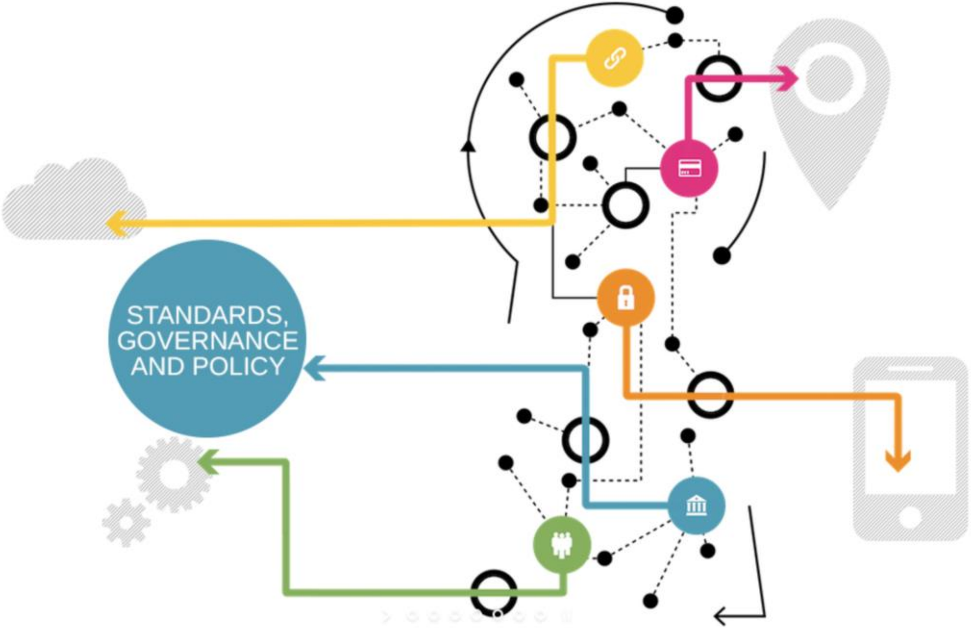
Global Policy (2018) 9:Suppl.3 doi: 10.1111/1758-5899.12625

Tanczer, L. M., Brass, I., & Carr, M. (2018). CSIRTs and Global Cybersecurity: How Technical Experts Support Science Diplomacy. *Global Policy*, *9*(S3), 60–66. https://doi.org/10.1111/1758-5899.12625

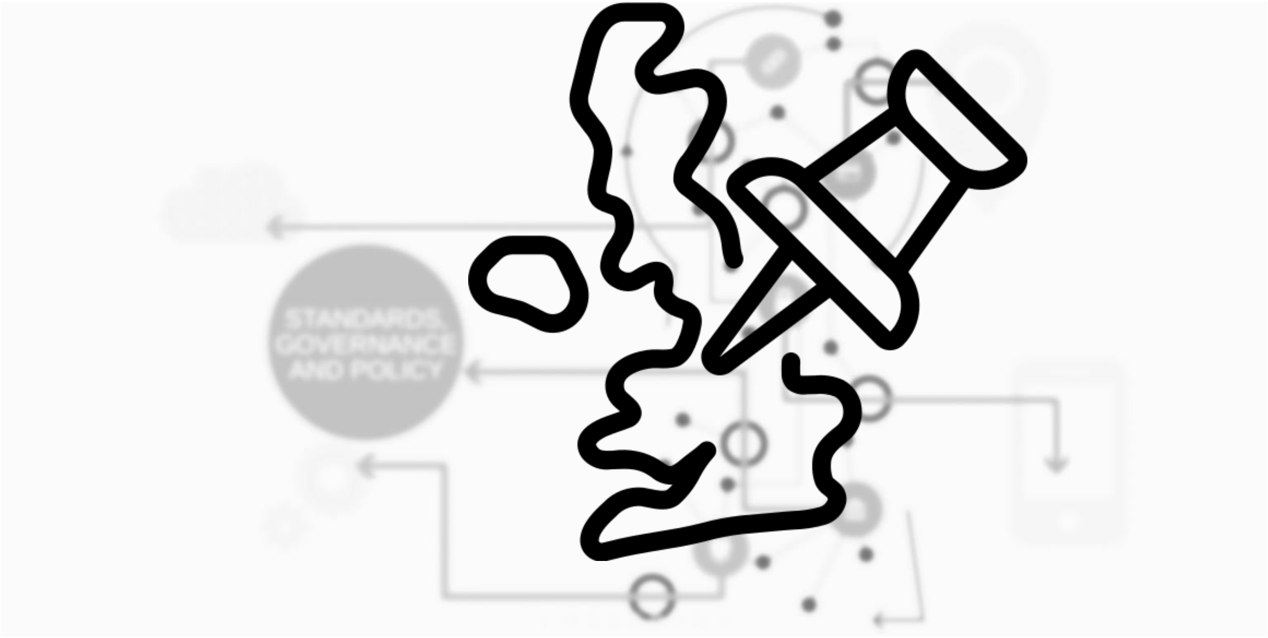
PETRAS IoT Hub



PETRAS National Centre of Excellence



PETRAS National Centre of Excellence



I will focus on…

Policy / Governance

Approaches / Initiatives

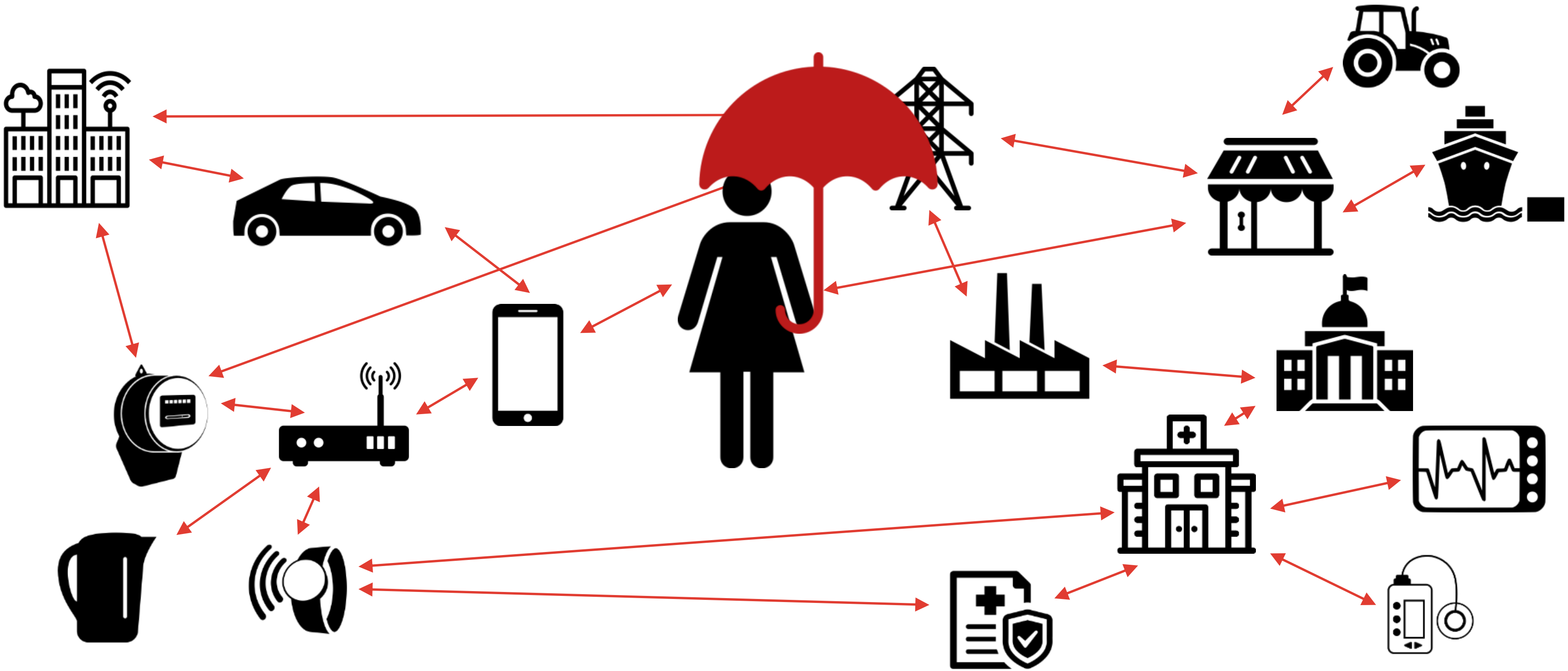
Human

Difficulties

Let’s start with the foundations…

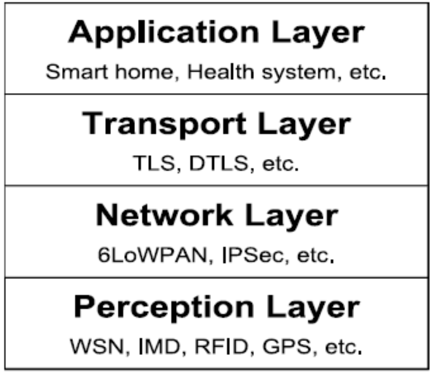
Department of Science, Technology, Engineering and Public Policy (STEaPP)

The Internet of What?



“Ubiquitous Computing”

- Coined by **Mark Weiser** in the early 1990s
- **Idea**: Internet extends into the “real world”



Application Layer
Smart home, Health system, etc.

Transport Layer
TLS, DTLS, etc.

Network Layer
6LoWPAN, IPSec, etc.

Perception Layer
WSN, IMD, RFID, GPS, etc.

Fig. 2. IoT layered analysis.

Mattern, F., & Flörkemeier, C. (2010). Vom Internet der Computer zum Internet der Dinge. Informatik-Spektrum, 33(2), 107–121. https://doi.org/10.1007/s00287-010-0417-7
Yang, Y., Wu, L., Yin, G., Li, L., & Zhao, H. (2017). A Survey on Security and Privacy Issues in Internet-of-Things. *IEEE Internet of Things Journal*, *4*(5), 1250–1258. https://doi.org/10.1109/JIOT.2017.2694844

“Ubiquitous Computing”

- Coined by **Mark Weiser** in the early 1990s
- **Idea**: Internet extends into the “real world”
- Yet, IoT does not only concern objects, but also the **relations** between these layers, everyday objects, and the surrounding **humans** themselves

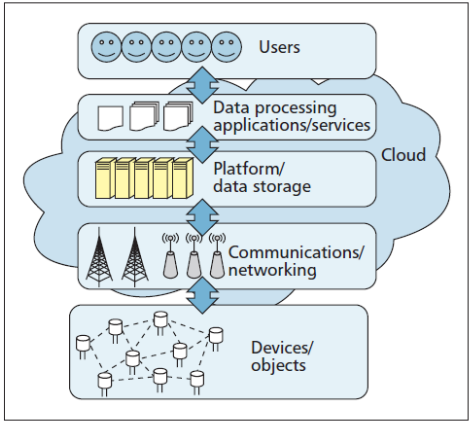

Users
Data processing applications/services
Platform/ data storage
Cloud
Communications/ networking
Devices/ objects

Figure 1. Internet of Things (IoT) representative model.

Niyato, D., Lu, X., Wang, P., Kim, D. I., & Han, Z. (2016). Economics of Internet of Things: An information market approach. *IEEE Wireless Communications*, *23*(4), 136–145. https://doi.org/10.1109/MWC.2016.7553037

Internet+

“It’s really the internet of things ***plus*** *the computers* ***plus*** *the services* ***plus*** *the large databases being built* ***plus*** *the internet companies* ***plus*** *us.*
I just shortened all this to ‘Internet+’.” (Schneier, 2018)

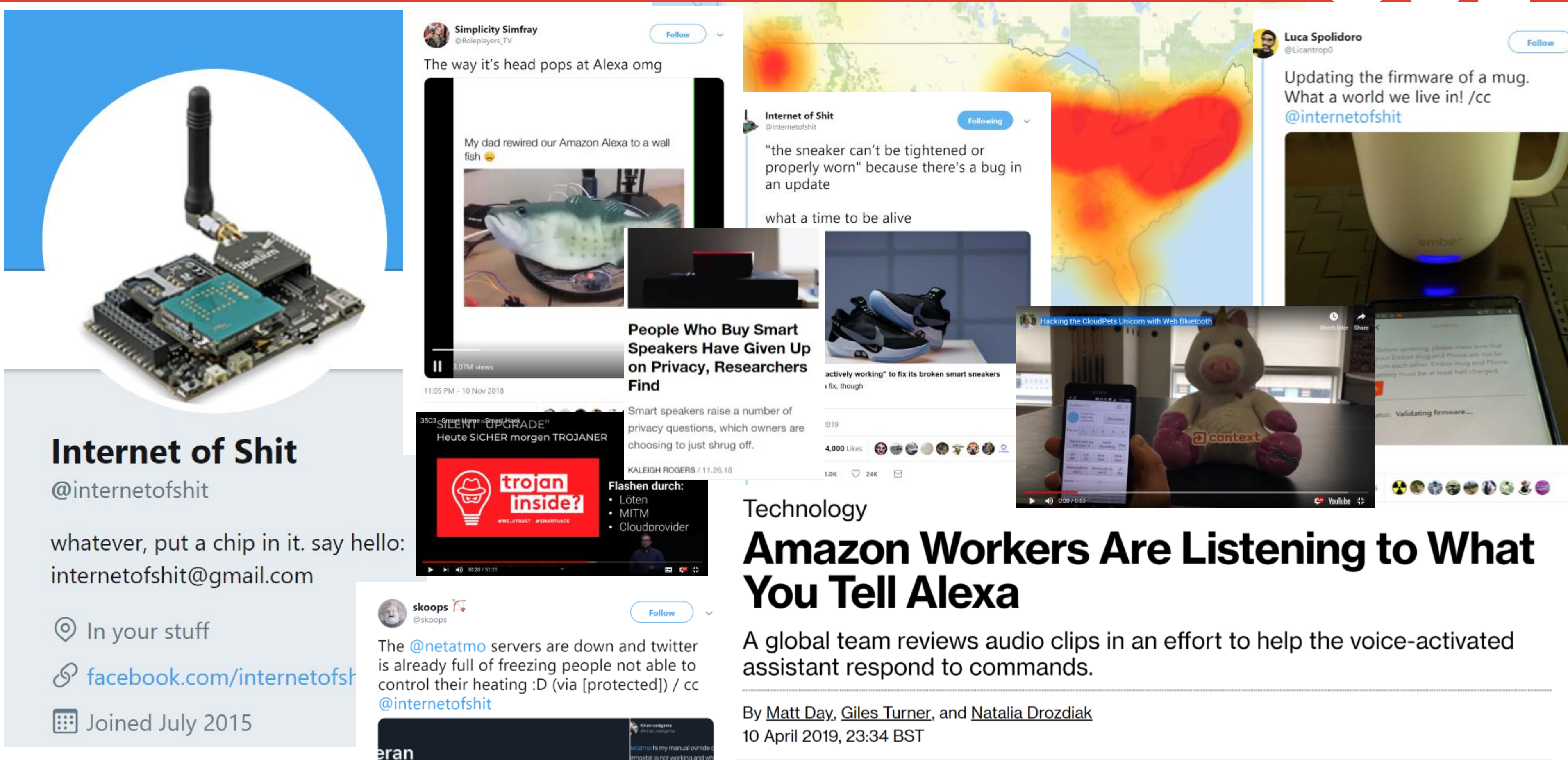
Giles, M. (2018, September 6). For safety’s sake, we must slow innovation in internet-connected things. Retrieved June 17, 2019, from MIT Technology Review website: https://www.technologyreview.com/s/611948/for-safetys-sake-we-must-slow-innovation-in-internet-connected-things/

Risks

Uncertainties

Opportunities

¯_(ツ)_/¯



Internet of Shit
@internetofshit

whatever, put a chip in it. say hello: internetofshit@gmail.com

In your stuff

facebook.com/internetofsh

Joined July 2015

Simplicity Simfray
@Roleplayers_TV

The way it's head pops at Alexa omg

My dad rewired our Amazon Alexa to a wall fish 😩

3.07M views

11:05 PM - 10 Nov 2018

Internet of Shit
@internetofshit

"the sneaker can't be tightened or properly worn" because there's a bug in an update

what a time to be alive

actively working" to fix its broken smart sneakers

a fix, though

2019

4,000 Likes

5.0K 24K

Luca Spolidoro
@Licantrop0

Updating the firmware of a mug. What a world we live in! /cc @internetofshit

Before updating, please make sure that your Ember mug and Phone are not far from each other. Ember mug and Phone battery must be at least half charged.

atus: Validating firmware...

People Who Buy Smart Speakers Have Given Up on Privacy, Researchers Find

Smart speakers raise a number of privacy questions, which owners are choosing to just shrug off.

KALEIGH ROGERS / 11.26.18

35C3 - Smart Home - Smart Hack

SILENT "UPGRADE"
Heute SICHER morgen TROJANER

trojan inside?

#MS_VTRUST #SMARTHACK

Flashen durch:
- Löten
- MITM
- Cloudprovider

30:20 / 51:21

Hacking the CloudPets Unicorn with Web Bluetooth

Watch later Share

context

0:08 / 0:53

skoops
@skoops

The @netatmo servers are down and twitter is already full of freezing people not able to control their heating :D (via [protected]) / cc @internetofshit

Kiran vadgama

netatmo hi my manual override

rmostat is not working and wh

eran

Technology

Amazon Workers Are Listening to What You Tell Alexa

A global team reviews audio clips in an effort to help the voice-activated assistant respond to commands.

By Matt Day, Giles Turner, and Natalia Drozdziak
10 April 2019, 23:34 BST

“Why do *we* want to connect everything?”

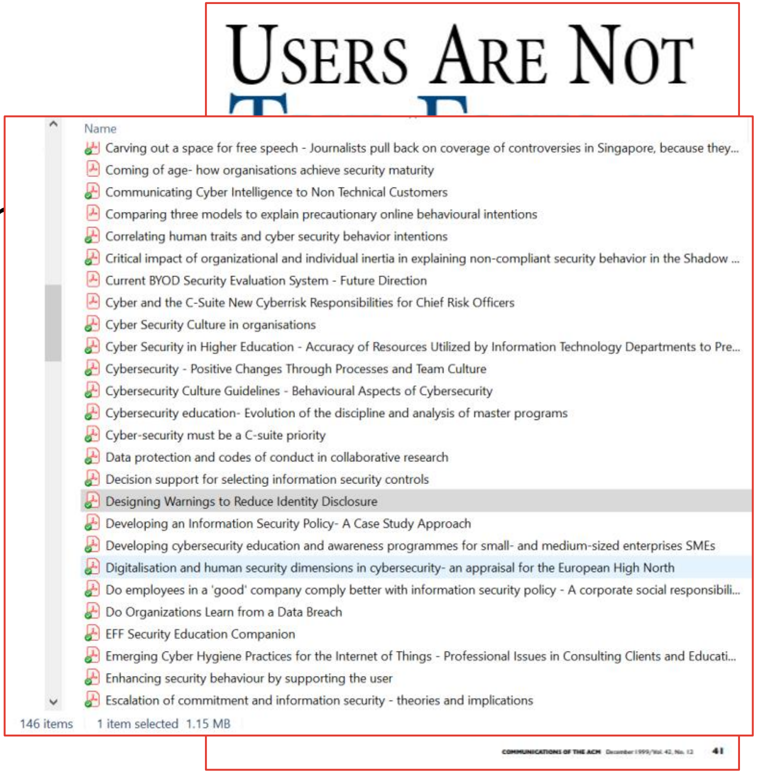
Don’t blame the user.

It’s kind of the industry’s problem.

But Leonie, why?

For one…

- …we don't expect users to be nutritional experts – rath the FSA ensures what enters the market
- For another, my whole "Culture of Security" reading folder will showcase you why it's not easy nor worth it



USERS ARE NOT

Name

- Carving out a space for free speech - Journalists pull back on coverage of controversies in Singapore, because they...
- Coming of age- how organisations achieve security maturity
- Communicating Cyber Intelligence to Non Technical Customers
- Comparing three models to explain precautionary online behavioural intentions
- Correlating human traits and cyber security behavior intentions
- Critical impact of organizational and individual inertia in explaining non-compliant security behavior in the Shadow ...
- Current BYOD Security Evaluation System - Future Direction
- Cyber and the C-Suite New Cyberrisk Responsibilities for Chief Risk Officers
- Cyber Security Culture in organisations
- Cyber Security in Higher Education - Accuracy of Resources Utilized by Information Technology Departments to Pre...
- Cybersecurity - Positive Changes Through Processes and Team Culture
- Cybersecurity Culture Guidelines - Behavioural Aspects of Cybersecurity
- Cybersecurity education- Evolution of the discipline and analysis of master programs
- Cyber-security must be a C-suite priority
- Data protection and codes of conduct in collaborative research
- Decision support for selecting information security controls
- Designing Warnings to Reduce Identity Disclosure
- Developing an Information Security Policy- A Case Study Approach
- Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises SMEs
- Digitalisation and human security dimensions in cybersecurity- an appraisal for the European High North
- Do employees in a 'good' company comply better with information security policy - A corporate social responsibili...
- Do Organizations Learn from a Data Breach
- EFF Security Education Companion
- Emerging Cyber Hygiene Practices for the Internet of Things - Professional Issues in Consulting Clients and Educati...
- Enhancing security behaviour by supporting the user
- Escalation of commitment and information security - theories and implications

146 items   1 item selected 1.15 MB

COMMUNICATIONS OF THE ACM December 1999/Vol. 42, No. 12   41

Adams, A., & Sasse, M. A. (1999). Users Are Not the Enemy. *Communications of the ACM*, *42*(12), 40–46. https://doi.org/10.1145/322796.322806

Privacy Paradox

- Although people might claim to value privacy, their behaviour can often appear misaligned:
    - Beresford et al. (2012) varied the prices of two online stores to explore privacy valuation. They discovered that **when the intrusive store was 1€ cheaper**, almost every user selected that option
    - Carrascal et al. (2013) used an auction to assess the value placed on personal data. They found **participants would sell their browsing history for 7€**
    - William et al. (2017) use survey and interviews to showcase how participants perceive IoT devices as **significantly less private** than non-IoT products. Many who recognised the risks, still purchased the products. Indeed, IoT owners both **cared** significantly less about their data and were significantly less able to **protect** it.

Williams, M., Nurse, J. R. C., & Creese, S. (2017). Privacy is the Boring Bit: User Perceptions and Behaviour in the Internet-of-Things. *2017 15th Annual Conference on Privacy, Security and Trust (PST)*, 181–18109. https://doi.org/10.1109/PST.2017.00029
Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. Computers & Security, 64, 122–134. https://doi.org/10.1016/j.cose.2015.07.002
Beresford, A. R., Kübler, D., & Preibusch, S. (2012). Unwillingness to pay for privacy: A field experiment. Economics Letters, 117(1), 25–27. https://doi.org/10.1016/j.econlet.2012.04.077
Carrascal, J. P., Riederer, C., Erramilli, V., Cherubini, M., & de Oliveira, R. (2013). Your Browsing Behavior for a Big Mac: Economics of Personal Information Online. Proceedings of the 22Nd International Conference on World Wide Web, 189–200. https://doi.org/10.1145/2488388.2488406
schraefel, m. c., & Gerding, E. (2013, 2017). Meaningful Consent in the Digital Economy. Retrieved July 29, 2017, from Meaningful Consent website: http://www.meaningfulconsent.org/

But again: This does *not* mean…

- … that people do not value their security and privacy (boyd & Hargittai, 2010)
- Simply: There are **severe cognitive problems** that undermine privacy self-management – shown through empirical and social science research (Solove, 2013)
- ***And industry should not exploit this.***

Nissenbaum, H. (2011). A Contextual Approach to Privacy Online. Dædalus: Journal of the American Academy of Arts & Sciences, (4), 32–48.
Bechmann, A. (2014). Non-Informed Consent Cultures: Privacy Policies and App Contracts on Facebook. Journal of Media Business Studies, 11(1), 21–38. https://doi.org/10.1080/16522354.2014.11073574
boyd, danah, & Hargittai, E. (2010). Facebook privacy settings: Who cares? Hargittai. First Monday, 15(8). Retrieved from https://firstmonday.org/article/view/3086/2589
Solove, D. (2013). Introduction: Privacy Self-Management and the Consent Dilemma. Harvard Law Review, 126, 1880–1903.

Ok, what are the governance issues then?

Where should I even start?!

- Privacy and data protection
- Security and safety
- Architecture
- Object identifiers
- IoT vs Internet Governance
- Harmonised standards
- Ethics
- …

40 | 3 The United Kingdom's Emerging Internet of Things (IoT) Policy Landscape

capacity to provide sufficient cybersecurity, with manufacturers frequently
to enforce password resets and automatic software updates. Industry actor
engage in trade-offs between adding security features and enhancing
attributes such as battery life and storage power. On the other hand, ma
devices were also easily compromised because users themselves reli
default factory passwords. The Mirai attack points therefore to some
threats and failures that an insecure and unregulated IoT market may po

Second, IoT devices and services are themselves targets of attacks, res
in implications for the privacy and security of data. Malicious actors can
security vulnerabilities at the device-, network-, and
take control over IoT-enabled cameras or connected a
for malicious intent, to compromise the security and p
innocent bystanders. Real-world examples include t
Barbie™ doll that allowed unauthorized third parties
nication, with the potential to expose users' account in
recorded by the doll.[18] Similarly, internet-connected
affected by a large-scale data breach that resulted in cr
for ransom.[19] These privacy concerns are exacerbated b
for security features at the product design stage,[20] ope
on IoT devices and services, which require proper secu
especially true for the complex, safety-critical IoT
industries as healthcare and infrastructure.

Third, the IoT creates new cyber–physical security
attack surface of devices overall. These risks differ fron
they couple software and hardware risks, resulting no
uncertain system surface but in growing attack vectors
tially life-threatening consequences. For instance, the
2016 allowed attackers to remotely control a car an
steering and braking system.[21] Similarly, the recall of ra
able cardiac pacemakers in 2017 highlighted the
landscape, as connected health devices were open to
ized users.[22] These examples showcase the cyber–p
with the IoT, and raises questions about the preparedn
approaches to vehicle safety, ownership and liabilit
cybersecurity.[23]

All of these outlined attack vectors are, of course,
and range of IoT-specific problems will change as Io
take off. However, these challenges are not limited t
attacks, but also include problems arising from po
interoperability problems, and generic technologi
leads to diverse and uncertain security challenges, a
responses that relate to an increasingly heterogeneo
and services.

COMPUTER LAW & SECURITY REVIEW 25 (2009) 522–527

available at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Internet of things – Need for a new legal environment?

Rolf H. Weber[a,b]

[a] University of Zurich, Switzerland
[b] University of Hong Kong, China

ABSTRACT

Keywords:
Internet of Things (IoT)
ONS and DNS
European Regulatory IoT-Initiatives

The Internet of Things as an emerging global, Internet-based information service architecture facilitating the exchange of goods in global supply chain networks is developing on the technical basis of the present Domain Name System; drivers are private actors. Learning from the experiences with the "traditional" Internet governance it is important to

COMPUTER LAW & SECURITY REVIEW 29 (2013) 341–347

Available online at www.sciencedirect.com

SciVerse ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Internet of things – Governance quo vadis?

CrossMark

Rolf H. Weber

University of Zurich, Zurich, Switzerland

ABSTRACT

Keywords:
Competition law
EU policy
International regulation
Particularities of IoT
Regulatory approaches
Substantive governance principles

The Internet of Things (IoT) as an emerging global Internet-based information architecture facilitating the exchange of goods and services is gradually developing. While the technical aspects are being discussed in detail a legal framework does not exist so far. The first supranational organization trying to work out an IoT governance framework has been the European Commission by appointing a large group of experts to examine the relevant aspects of a possible IoT governance regime. In the meantime, however, the activities have been degraded. Nevertheless, even if the differences between the IoT and the Internet have been overestimated at the beginning, many elements of the IoT differ in part from the corresponding problems in the Internet. Therefore, an analysis of the major IoT governance issues (legitimacy, transparency, accountability, anticompetitive behavior) seems to be worthwhile to conduct.

© 2013 Rolf H. Weber. Published by Elsevier Ltd. All rights reserved.

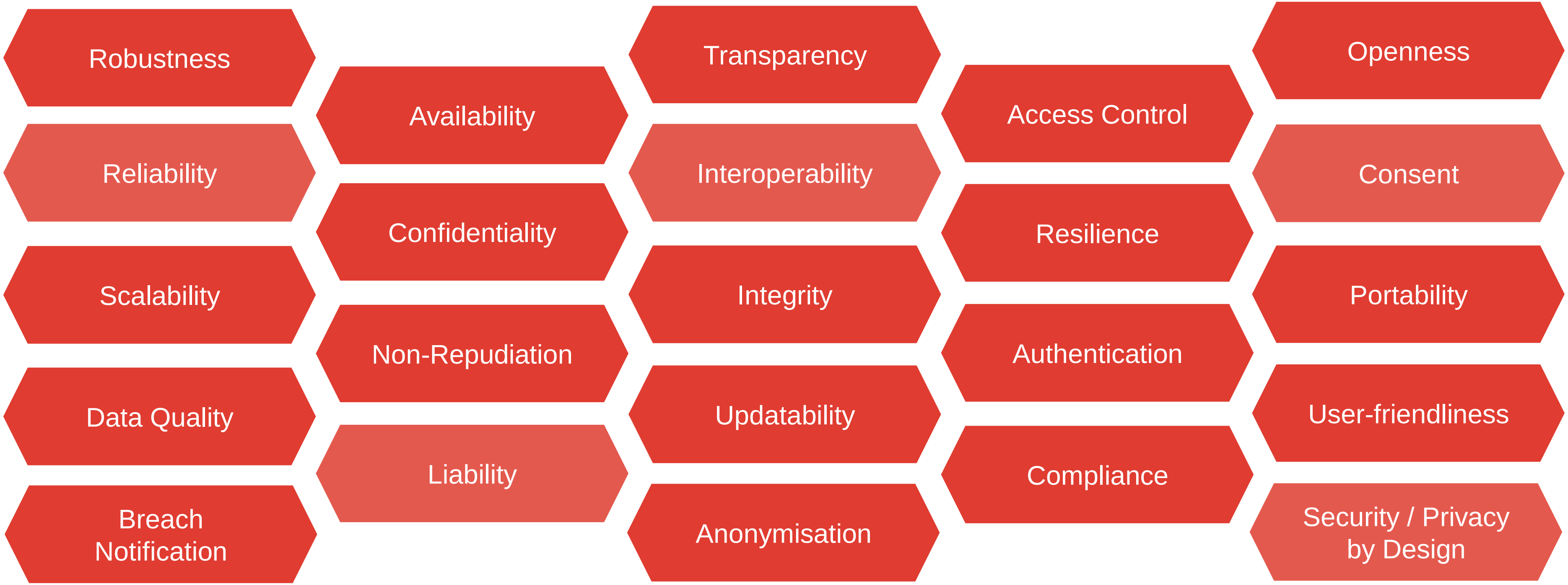
1. Introduction

For the time being, an authoritative definition of the Internet of Things (IoT) does not exist, notwithstanding the fact that several efforts have been taken to define the IoT. A commonly acknowledged definition stems from the ITU (2005), arguing

of institutions and the structure of authority to allocate resources and coordinate or control activities in the society. According to a definition of the World Bank governance "includes (i) the process by which those in authority are selected, monitored and replaced, (ii) the capacity of the governing body to effectively manage its resources and implement sound pol-

Weber, R. H. (2009). Internet of things – Need for a new legal environment? *Computer Law & Security Review*, *25*(6), 522–527. https://doi.org/10.1016/j.clsr.2009.09.002
Weber, R. H. (2010). Internet of Things – New security and privacy challenges. Computer Law & Security Review, 26(1), 23–30. https://doi.org/10.1016/j.clsr.2009.11.008
Weber, R. H. (2013). Internet of things–Governance quo vadis? Computer Law & Security Review, 29(4), 341–347.
Brass, I., Tanczer, L. M., Carr, M., & Blackstock, J. (2017). Regulating IoT: Enabling or Disabling the Capacity of the Internet of Things? Risk & Regulation Magazine of the Centre for Analysis of Risk and Regulation (CARR), 33(Summer), 12–15.
Tanczer, L. M., Brass, I., Elsden, M., Carr, M., & Blackstock, J. (2019). The United Kingdom's Emerging Internet of Things (IoT) Policy Landscape. In R. Ellis & V. Mohan (Eds.), Rewired: Cybersecurity Governance (pp. 37–56). Hoboken, New Jersey: Wiley.

What will we have to ensure?



Robustness

Reliability

Scalability

Data Quality

Breach Notification

Availability

Confidentiality

Non-Repudiation

Liability

Transparency

Interoperability

Integrity

Updatability

Anonymisation

Access Control

Resilience

Authentication

Compliance

Openness

Consent

Portability

User-friendliness

Security / Privacy by Design

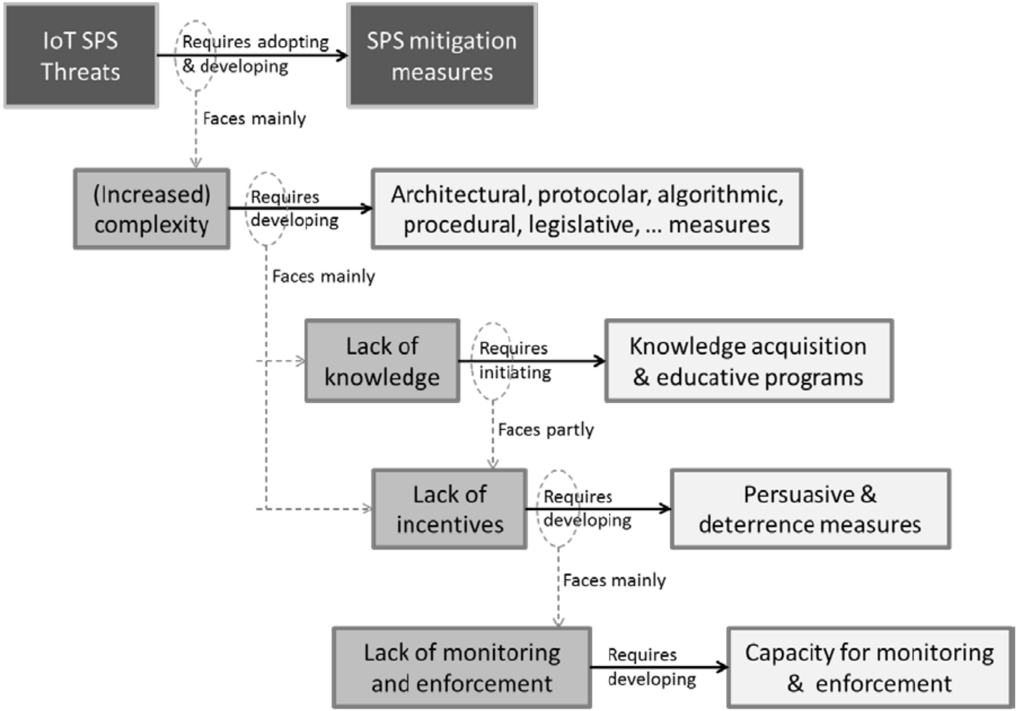
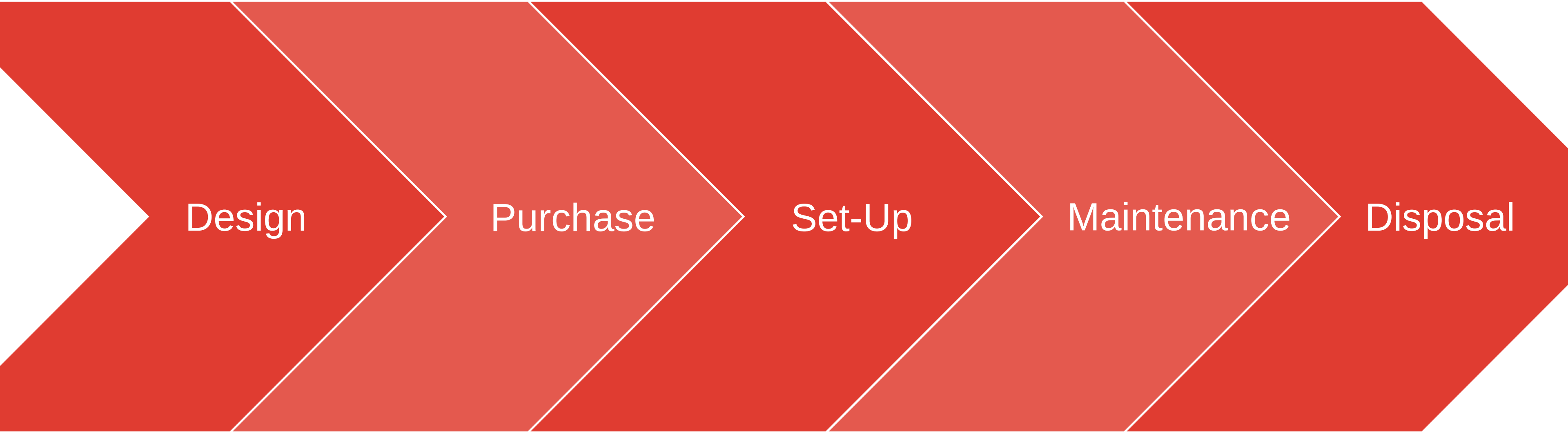

IoT SPS Threats
Requires adopting & developing
SPS mitigation measures
Faces mainly
(Increased) complexity
Requires developing
Architectural, protocolar, algorithmic, procedural, legislative, … measures
Faces mainly
Lack of knowledge
Requires initiating
Knowledge acquisition & educative programs
Faces partly
Lack of incentives
Requires developing
Persuasive & deterrence measures
Faces mainly
Lack of monitoring and enforcement
Requires developing
Capacity for monitoring & enforcement

Figure 1. Conceptual framework of the obstacles in addressing IoT SPS threats (boxes on left side), and solution directions to overcome them (boxes on the right side).

Harbers, M., Bargh, M. S., Pool, R., Berkel, J. V., Braak, S. W. van den, & Choenni, S. (2018). A Conceptual Framework for Addressing IoT Threats: Challenges in Meeting Challenges. HICSS, 2215–2224. https://doi.org/10.24251/hicss.2018.278

“Lifecycle” Problem



Design

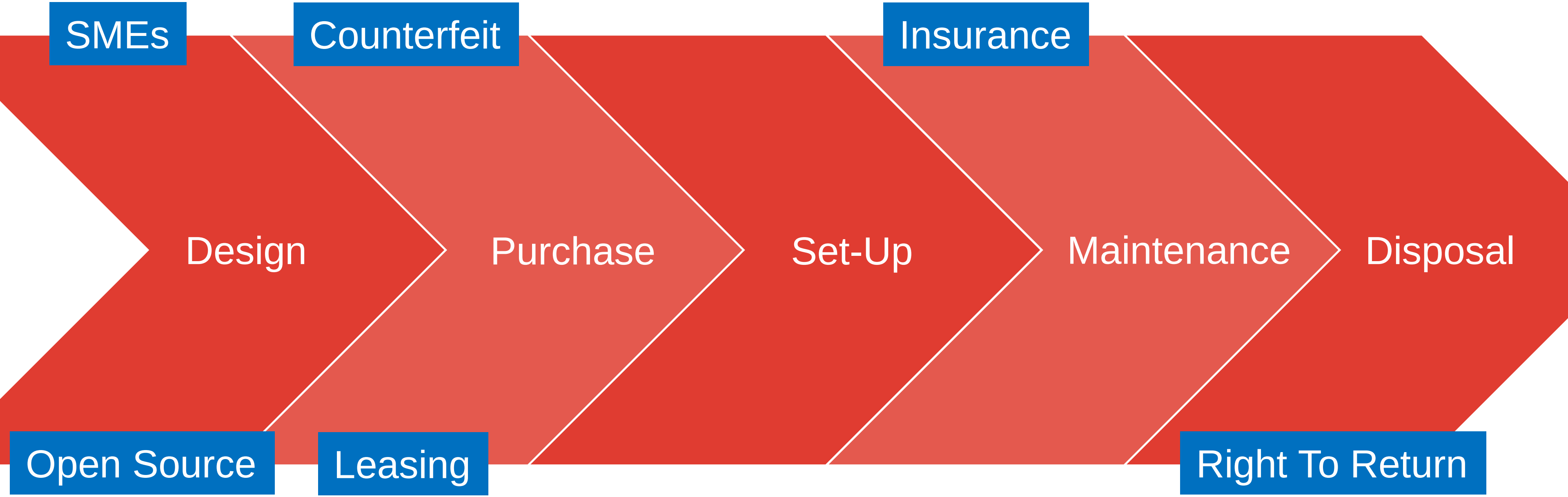
Purchase

Set-Up

Maintenance

Disposal

“Lifecycle” Problem



SMEs

Counterfeit

Insurance

Design

Purchase

Set-Up

Maintenance

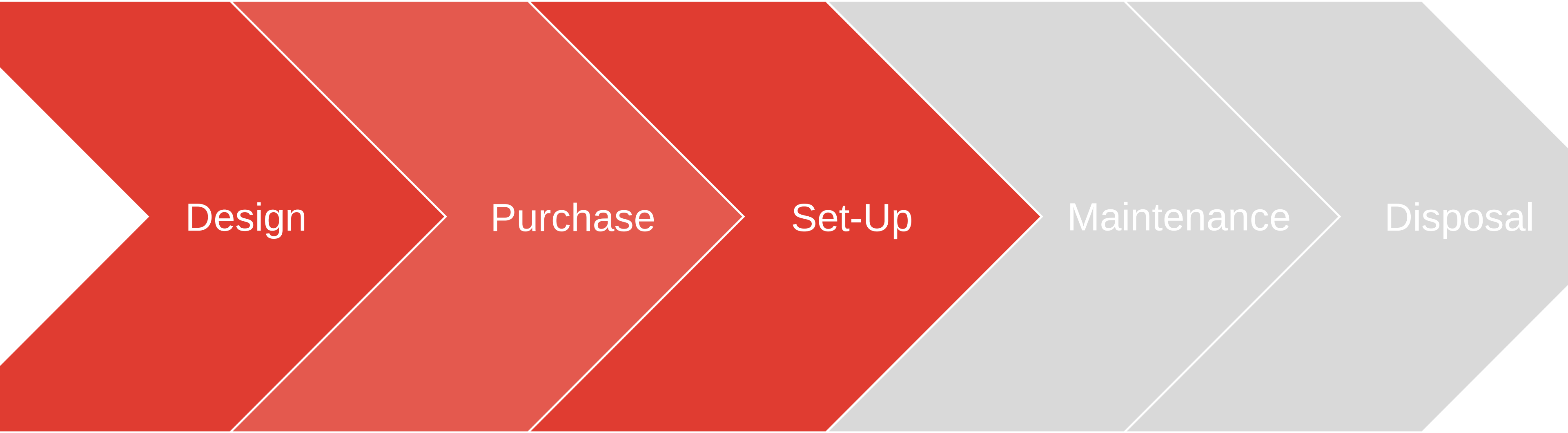
Disposal

Open Source

Leasing

Right To Return

“Lifecycle” Problem



Design

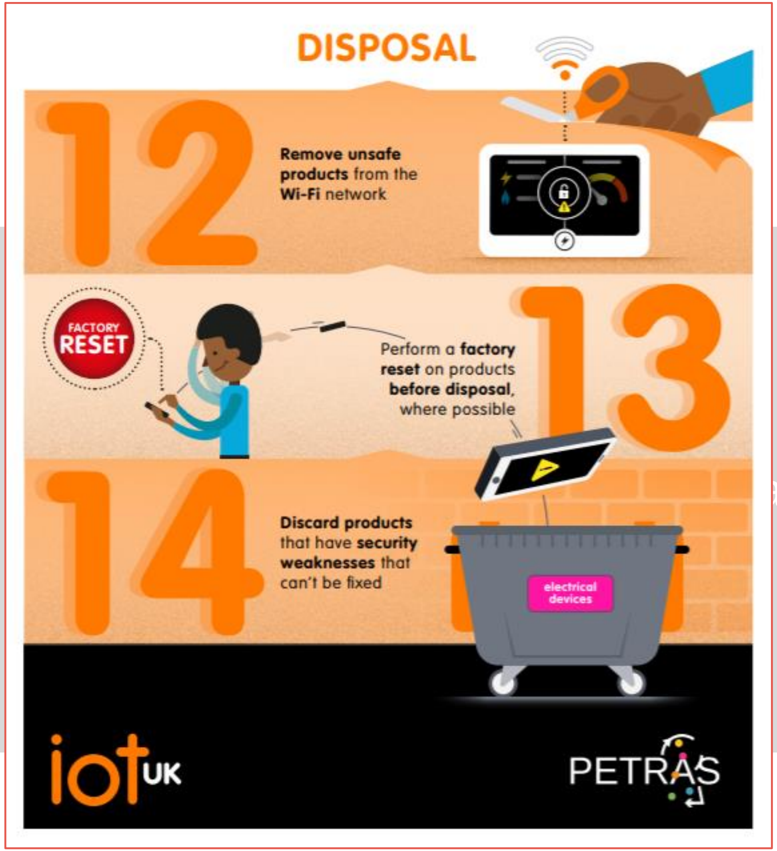
Purchase

Set-Up

Maintenance

Disposal

Design



DISPOSAL

12 **Remove unsafe products** from the **Wi-Fi** network

13 Perform a **factory reset** on products **before disposal**, where possible

14 **Discard products** that have **security weaknesses** that can't be fixed

aintenance

Disposal

Blythe, J., & Lefevre, C. (2018). *Cyberhygiene Insight Report* (pp. 1–12). Retrieved from IoTUK and PETRAS IoT Hub website: https://iotuk.org.uk/wp-content/uploads/2018/01/PETRAS-IoTUK-Cyberhygiene-Insight-Report.pdf

Product Safety

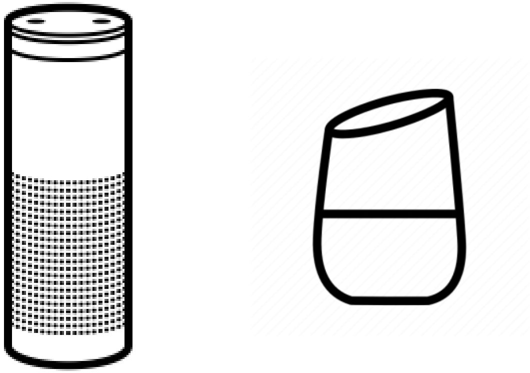
- Flammability of materials
- Lithium battery concerns
- Electric field exposure
- Biocompatibility
- Light-emitting diode
- Washability

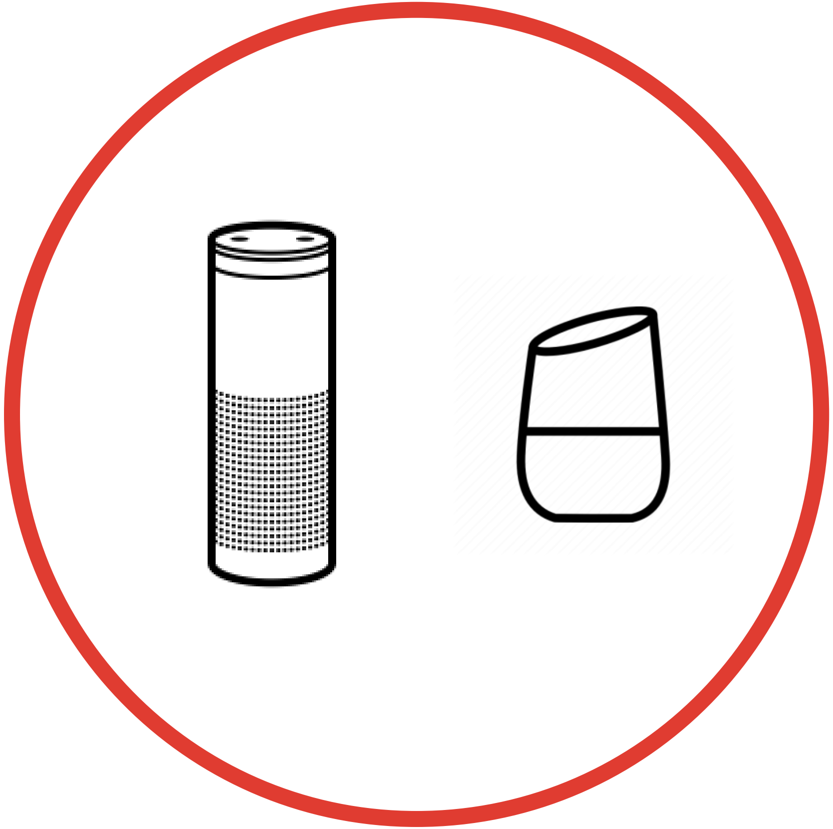
Bisenius, B. (2017). Product Safety of the Internet of Things [Product Safety Perspectives]. *IEEE Consumer Electronics Magazine*, *6*(3), 137–139. https://doi.org/10.1109/MCE.2017.2685018

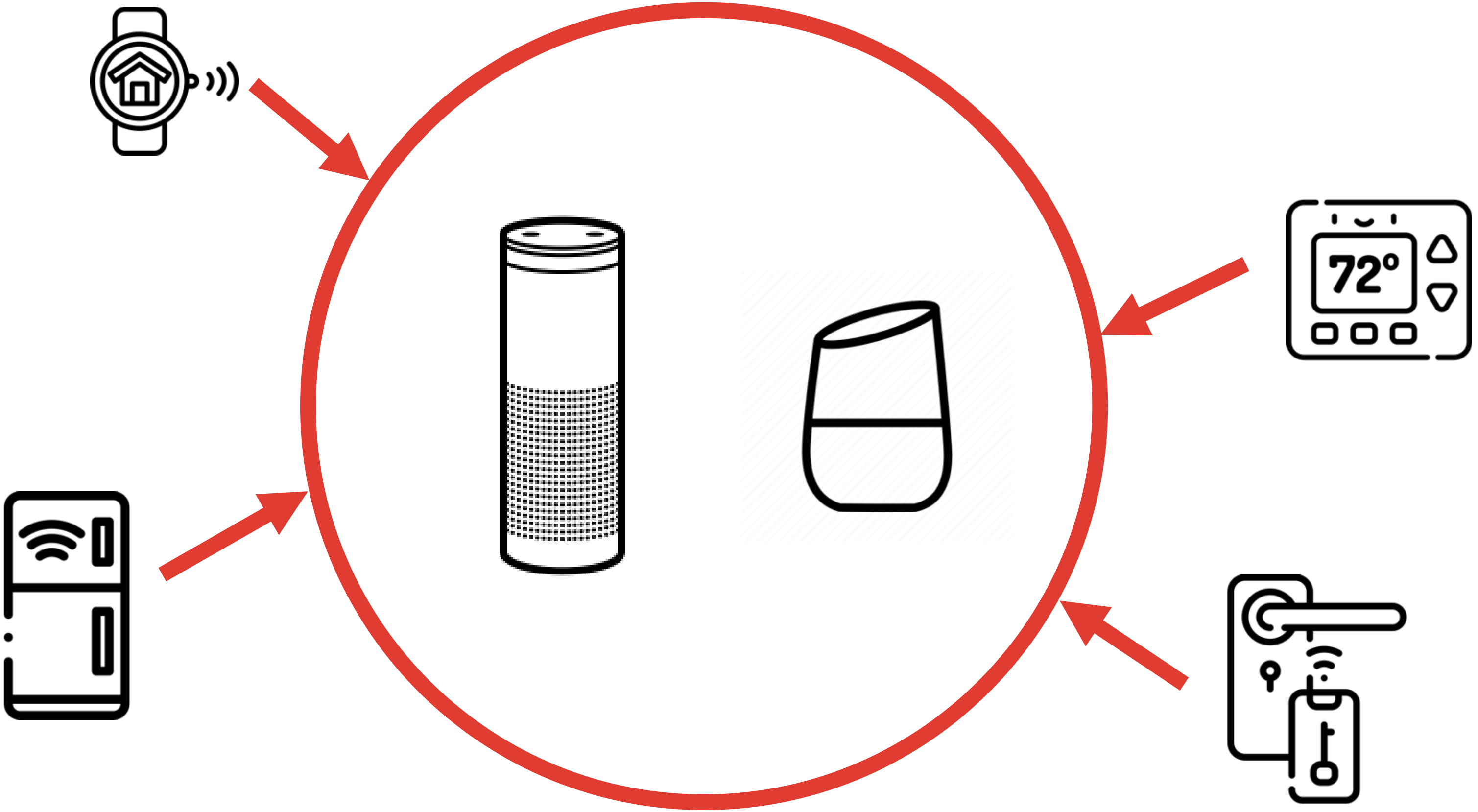
Clash of safety versus security?

Bisenius, B. (2017). Product Safety of the Internet of Things [Product Safety Perspectives]. *IEEE Consumer Electronics Magazine*, *6*(3), 137–139. https://doi.org/10.1109/MCE.2017.2685018

A big worry:







Arcep. (2018). *Smartphones, tablets, voice assistants... Devices, the weak link in achieving an open internet* (pp. 1–65). Retrieved from Autorité de Régulation des Communications Électroniques et des Postes website: https://www.arcep.fr/uploads/tx_gspublication/rapport-terminaux-fev2018-ENG.pdf

Can’t we just regulate this?!

Let’s be honest.

Geographically limited national legislation does not seem appropriate in this context.

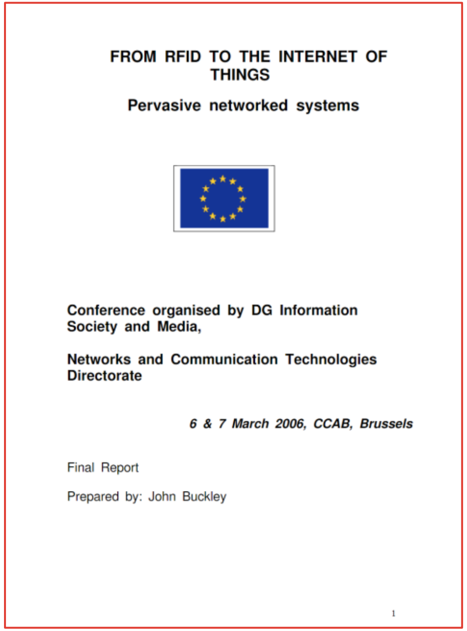
Let’s be honest.

“Stifle Innovation”

van Lieshout, M., & Emmert, S. (2018). RESPECT4U – Privacy as Innovation Opportunity. In M. Medina, A. Mitrakas, K. Rannenberg, E. Schweighofer, & N. Tsouroulas (Eds.), *Privacy Technologies and Policy* (pp. 43–60). Springer International Publishing.
Ziegler, S., Evequoz, E., & Huamani, A. M. P. (2019). The Impact of the European General Data Protection Regulation (GDPR) on Future Data Business Models: Toward a New Paradigm and Business Opportunities. In A. Aagaard (Ed.), Digital Business Models: Driving Transformation and Innovation (pp. 201–226). https://doi.org/10.1007/978-3-319-96902-2_8

Haunts us already for quite some time...

The need to **tackle regulatory issues** of the IoT governance has been recognized by the EU Commission already in **2006**, particularly at the occasion of a workshop entitled "*From RFID to the Internet of Things*" (Weber, 2009)



FROM RFID TO THE INTERNET OF THINGS

Pervasive networked systems

Conference organised by DG Information Society and Media,

Networks and Communication Technologies Directorate

6 & 7 March 2006, CCAB, Brussels

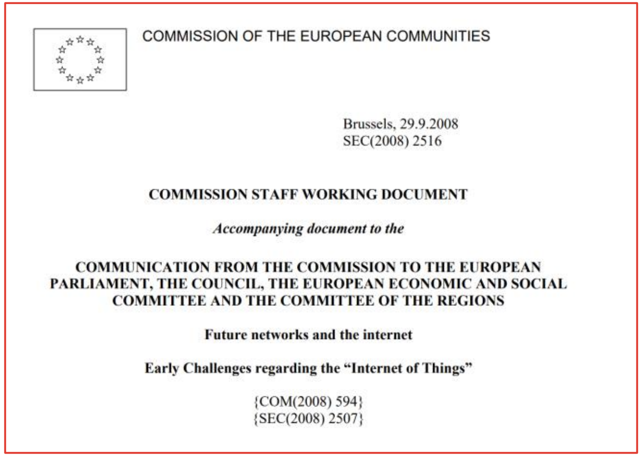
Final Report

Prepared by: John Buckley

1

Weber, R. H. (2009). Internet of things – Need for a new legal environment? *Computer Law & Security Review*, *25*(6), 522–527. https://doi.org/10.1016/j.clsr.2009.09.002

“*The European Commission has intended to be* ***frontrunner*** *in the efforts of implementing an adequate governance framework for the new IoT technology.*” (Weber, 2013)



COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 29.9.2008
SEC(2008) 2516

COMMISSION STAFF WORKING DOCUMENT

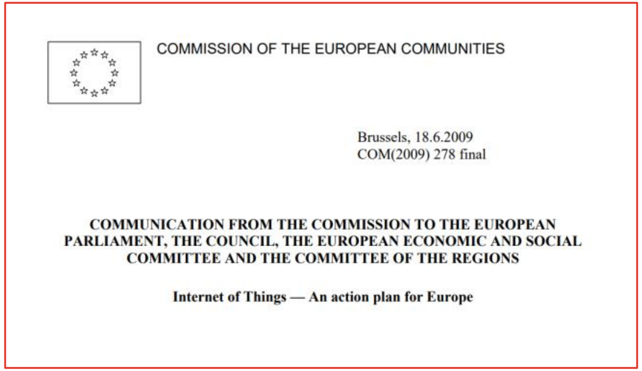
Accompanying document to the

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

Future networks and the internet

Early Challenges regarding the “Internet of Things”

{COM(2008) 594}
{SEC(2008) 2507}



COMMISSION OF THE EUROPEAN COMMUNITIES

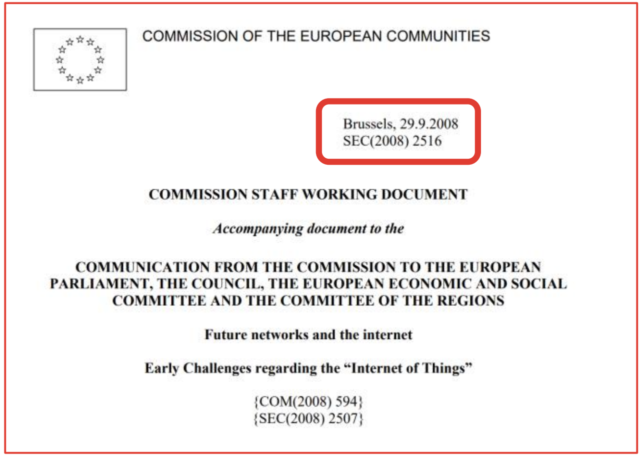
Brussels, 18.6.2009
COM(2009) 278 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

Internet of Things — An action plan for Europe

Weber, R. H. (2013). Internet of things–Governance quo vadis? *Computer Law & Security Review*, *29*(4), 341–347.

In **2008** the EU Commission is still in favour of **self-regulation.**



COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 29.9.2008
SEC(2008) 2516

COMMISSION STAFF WORKING DOCUMENT

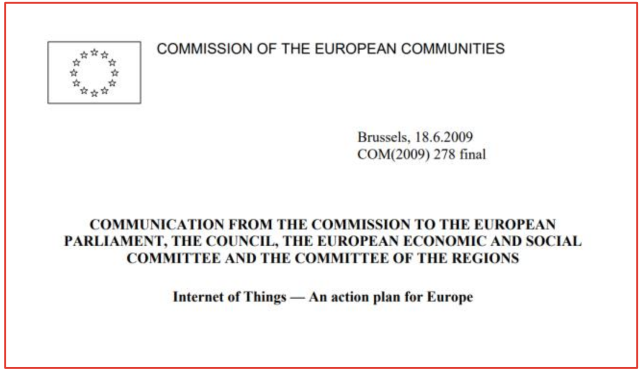
Accompanying document to the

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

Future networks and the internet

Early Challenges regarding the "Internet of Things"

{COM(2008) 594}
{SEC(2008) 2507}



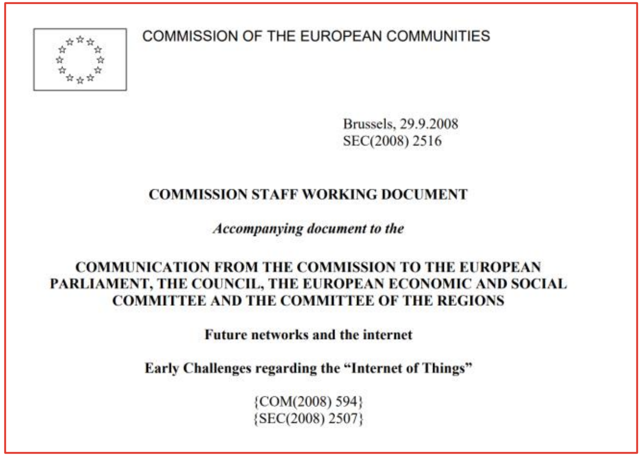
COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 18.6.2009
COM(2009) 278 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

Internet of Things — An action plan for Europe

But already in its **Communication of 18 June** 2009, the EU Commission expresses the opinion that the development of IoT **cannot be left to the private sector** and to other world regions alone.



COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 29.9.2008
SEC(2008) 2516

COMMISSION STAFF WORKING DOCUMENT

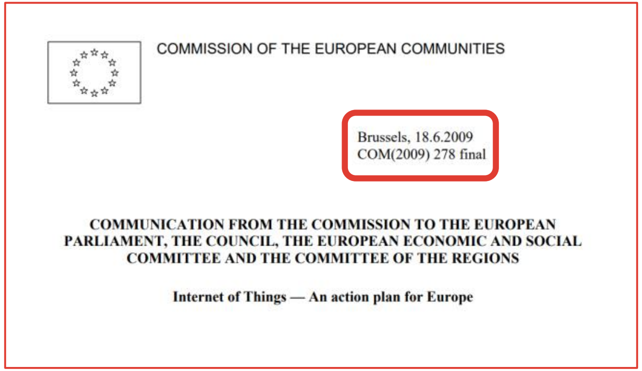
Accompanying document to the

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

Future networks and the internet

Early Challenges regarding the "Internet of Things"

{COM(2008) 594}
{SEC(2008) 2507}



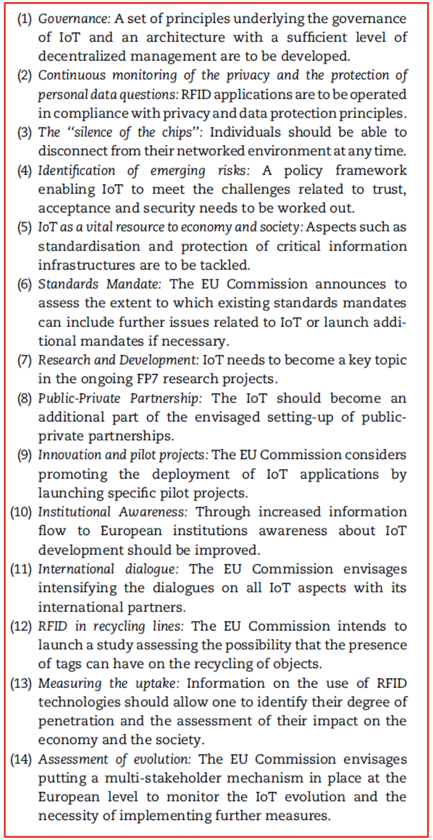
COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 18.6.2009
COM(2009) 278 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

Internet of Things — An action plan for Europe

14 Lines of Actions



(1) *Governance:* A set of principles underlying the governance of IoT and an architecture with a sufficient level of decentralized management are to be developed.

(2) *Continuous monitoring of the privacy and the protection of personal data questions:* RFID applications are to be operated in compliance with privacy and data protection principles.

(3) *The "silence of the chips":* Individuals should be able to disconnect from their networked environment at any time.

(4) *Identification of emerging risks:* A policy framework enabling IoT to meet the challenges related to trust, acceptance and security needs to be worked out.

(5) *IoT as a vital resource to economy and society:* Aspects such as standardisation and protection of critical information infrastructures are to be tackled.

(6) *Standards Mandate:* The EU Commission announces to assess the extent to which existing standards mandates can include further issues related to IoT or launch additional mandates if necessary.

(7) *Research and Development:* IoT needs to become a key topic in the ongoing FP7 research projects.

(8) *Public-Private Partnership:* The IoT should become an additional part of the envisaged setting-up of public-private partnerships.

(9) *Innovation and pilot projects:* The EU Commission considers promoting the deployment of IoT applications by launching specific pilot projects.

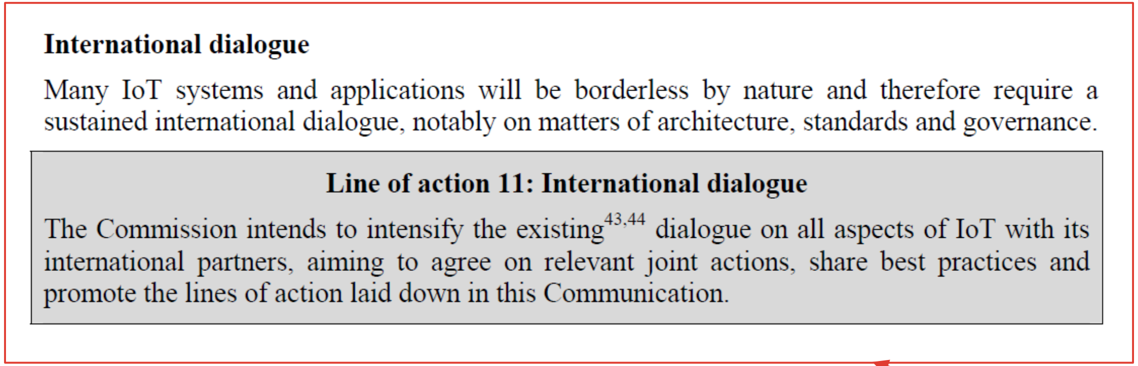
(10) *Institutional Awareness:* Through increased information flow to European institutions awareness about IoT development should be improved.

(11) *International dialogue:* The EU Commission envisages intensifying the dialogues on all IoT aspects with its international partners.

(12) *RFID in recycling lines:* The EU Commission intends to launch a study assessing the possibility that the presence of tags can have on the recycling of objects.

(13) *Measuring the uptake:* Information on the use of RFID technologies should allow one to identify their degree of penetration and the assessment of their impact on the economy and the society.

(14) *Assessment of evolution:* The EU Commission envisages putting a multi-stakeholder mechanism in place at the European level to monitor the IoT evolution and the necessity of implementing further measures.



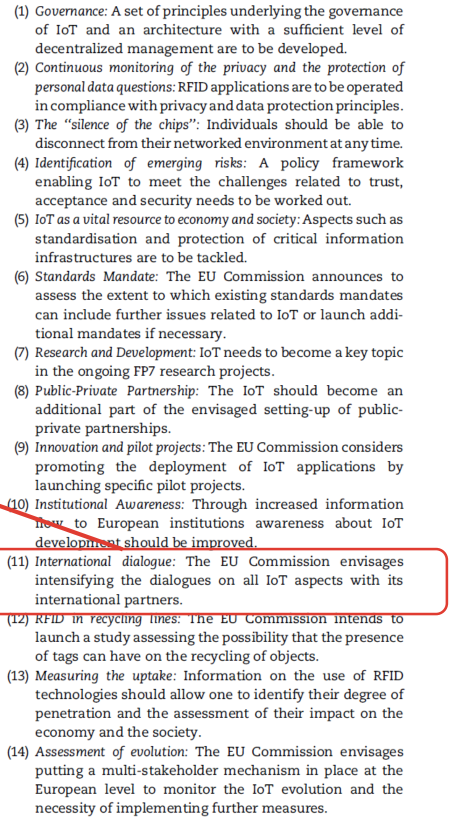
International dialogue

Many IoT systems and applications will be borderless by nature and therefore require a sustained international dialogue, notably on matters of architecture, standards and governance.

Line of action 11: International dialogue

The Commission intends to intensify the existing[43,44] dialogue on all aspects of IoT with its international partners, aiming to agree on relevant joint actions, share best practices and promote the lines of action laid down in this Communication.

14 Lines of Actions



(1) *Governance:* A set of principles underlying the governance of IoT and an architecture with a sufficient level of decentralized management are to be developed.

(2) *Continuous monitoring of the privacy and the protection of personal data questions:* RFID applications are to be operated in compliance with privacy and data protection principles.

(3) *The "silence of the chips":* Individuals should be able to disconnect from their networked environment at any time.

(4) *Identification of emerging risks:* A policy framework enabling IoT to meet the challenges related to trust, acceptance and security needs to be worked out.

(5) *IoT as a vital resource to economy and society:* Aspects such as standardisation and protection of critical information infrastructures are to be tackled.

(6) *Standards Mandate:* The EU Commission announces to assess the extent to which existing standards mandates can include further issues related to IoT or launch additional mandates if necessary.

(7) *Research and Development:* IoT needs to become a key topic in the ongoing FP7 research projects.

(8) *Public-Private Partnership:* The IoT should become an additional part of the envisaged setting-up of public-private partnerships.

(9) *Innovation and pilot projects:* The EU Commission considers promoting the deployment of IoT applications by launching specific pilot projects.

(10) *Institutional Awareness:* Through increased information flow to European institutions awareness about IoT development should be improved.

(11) *International dialogue:* The EU Commission envisages intensifying the dialogues on all IoT aspects with its international partners.

(12) *RFID in recycling lines:* The EU Commission intends to launch a study assessing the possibility that the presence of tags can have on the recycling of objects.

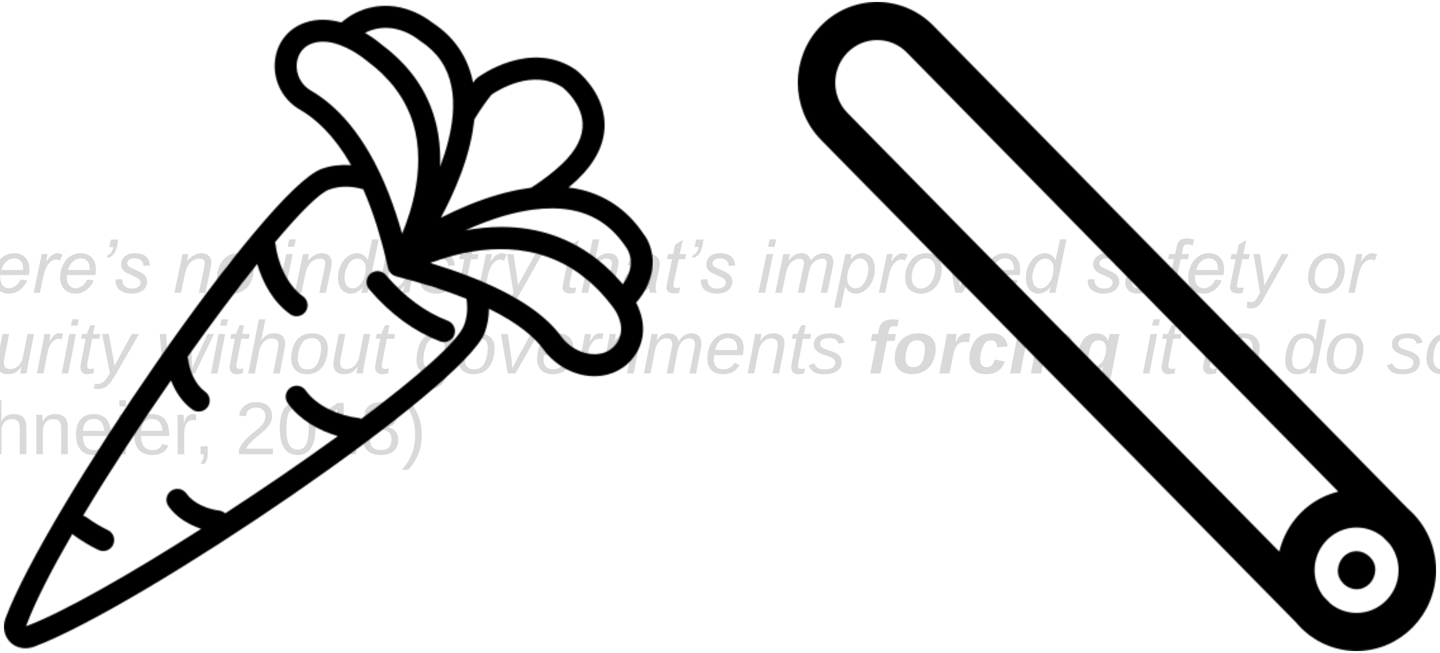
(13) *Measuring the uptake:* Information on the use of RFID technologies should allow one to identify their degree of penetration and the assessment of their impact on the economy and the society.

(14) *Assessment of evolution:* The EU Commission envisages putting a multi-stakeholder mechanism in place at the European level to monitor the IoT evolution and the necessity of implementing further measures.

We still up for self-regulation?

“*There’s no industry that’s improved safety or security without governments* ***forcing*** *it to do so.*” (Schneier, 2018)

“There’s no industry that’s improved safety or security without governments ***forcing*** *it to do so.”*
(Schneier, 2018)



European Union

enisa

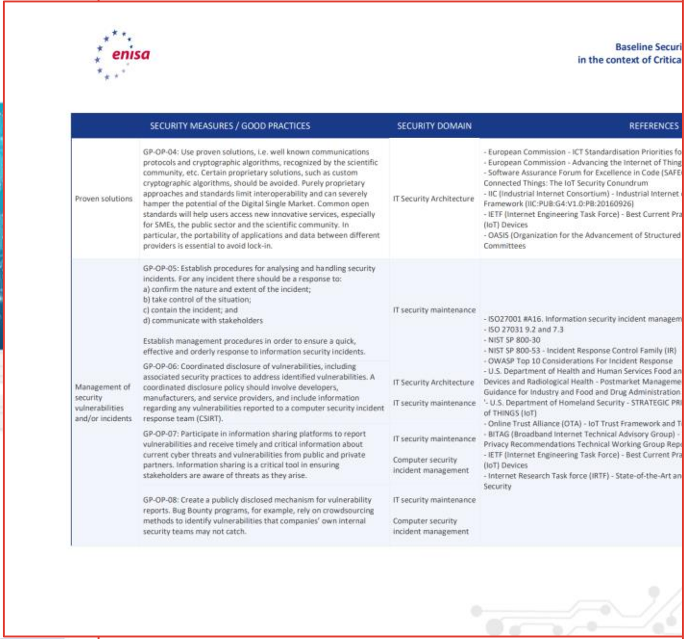
Baseline Security Recommendations for IoT

in the context of Critical Information Infrastructures

NOVEMBER 2017

www.enisa.europa.eu

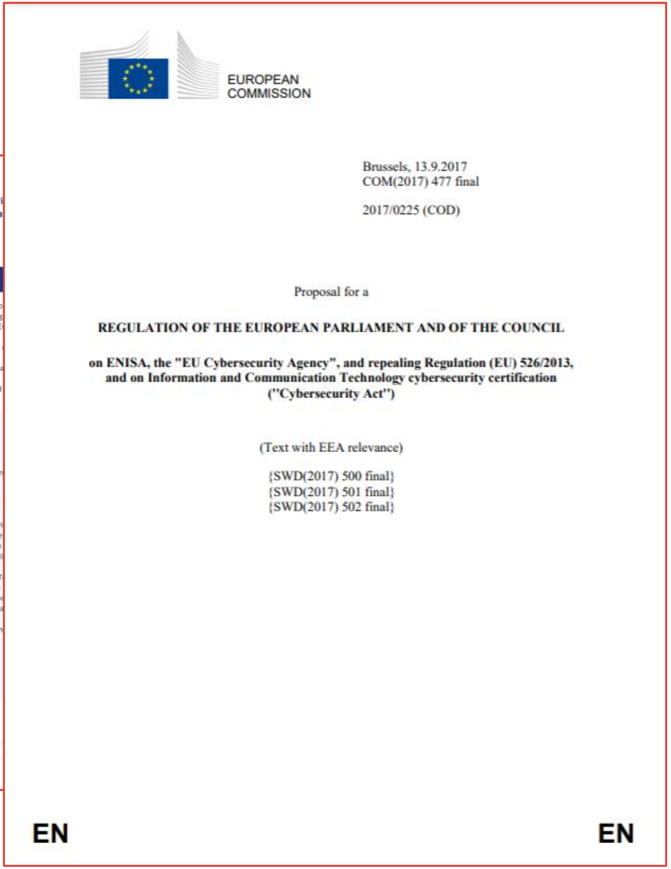
European Union Agency For Network And Information Security



enisa

Baseline Securi
in the context of Critica

SECURITY MEASURES / GOOD PRACTICES		SECURITY DOMAIN	REFERENCES
Proven solutions	GP-OP-04: Use proven solutions, i.e. well known communications protocols and cryptographic algorithms, recognized by the scientific community, etc. Certain proprietary solutions, such as custom cryptographic algorithms, should be avoided. Purely proprietary approaches and standards limit interoperability and can severely hamper the potential of the Digital Single Market. Common open standards will help users access new innovative services, especially for SMEs, the public sector and the scientific community. In particular, the portability of applications and data between different providers is essential to avoid lock-in.	IT Security Architecture	- European Commission - ICT Standardisation Priorities fo - European Commission - Advancing the Internet of Thing - Software Assurance Forum for Excellence in Code (SAFE Connected Things: The IoT Security Conundrum - IIC (Industrial Internet Consortium) - Industrial Internet Framework (IIC:PUB:G4:V1.0:PB:20160926) - IETF (Internet Engineering Task Force) - Best Current Pra (IoT) Devices - OASIS (Organization for the Advancement of Structured Committees
Management of security vulnerabilities and/or incidents	GP-OP-05: Establish procedures for analysing and handling security incidents. For any incident there should be a response to: a) confirm the nature and extent of the incident; b) take control of the situation; c) contain the incident; and d) communicate with stakeholders Establish management procedures in order to ensure a quick, effective and orderly response to information security incidents.	IT security maintenance	- ISO27001 #A16. Information security incident managem - ISO 27031 9.2 and 7.3 - NIST SP 800-30 - NIST SP 800-53 - Incident Response Control Family (IR) - OWASP Top 10 Considerations For Incident Response - U.S. Department of Health and Human Services Food an Devices and Radiological Health - Postmarket Manageme Guidance for Industry and Food and Drug Administration '- U.S. Department of Homeland Security - STRATEGIC PRI of THINGS (IoT) - Online Trust Alliance (OTA) - IoT Trust Framework and T - BITAG (Broadband Internet Technical Advisory Group) - Privacy Recommendations Technical Working Group Rep - IETF (Internet Engineering Task Force) - Best Current Pra (IoT) Devices - Internet Research Task force (IRTF) - State-of-the-Art an Security
	GP-OP-06: Coordinated disclosure of vulnerabilities, including associated security practices to address identified vulnerabilities. A coordinated disclosure policy should involve developers, manufacturers, and service providers, and include information regarding any vulnerabilities reported to a computer security incident response team (CSIRT).	IT Security Architecture IT security maintenance	
	GP-OP-07: Participate in information sharing platforms to report vulnerabilities and receive timely and critical information about current cyber threats and vulnerabilities from public and private partners. Information sharing is a critical tool in ensuring stakeholders are aware of threats as they arise.	IT security maintenance Computer security incident management	
	GP-OP-08: Create a publicly disclosed mechanism for vulnerability reports. Bug Bounty programs, for example, rely on crowdsourcing methods to identify vulnerabilities that companies' own internal security teams may not catch.	IT security maintenance Computer security incident management	



EUROPEAN COMMISSION

Brussels, 13.9.2017
COM(2017) 477 final

2017/0225 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

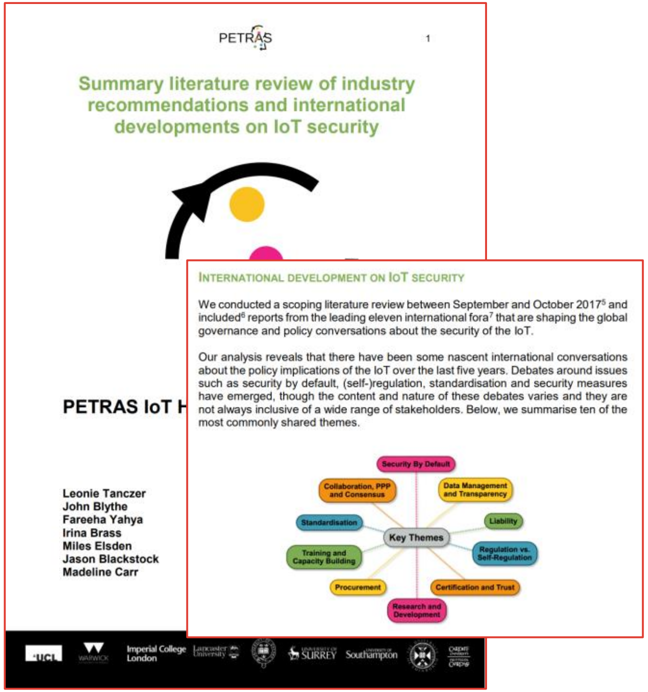
on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act")

(Text with EEA relevance)

{SWD(2017) 500 final}
{SWD(2017) 501 final}
{SWD(2017) 502 final}

EN EN

United Kingdom



PETRAS 1

Summary literature review of industry recommendations and international developments on IoT security

PETRAS IoT H

Leonie Tanczer
John Blythe
Fareeha Yahya
Irina Brass
Miles Elsden
Jason Blackstock
Madeline Carr

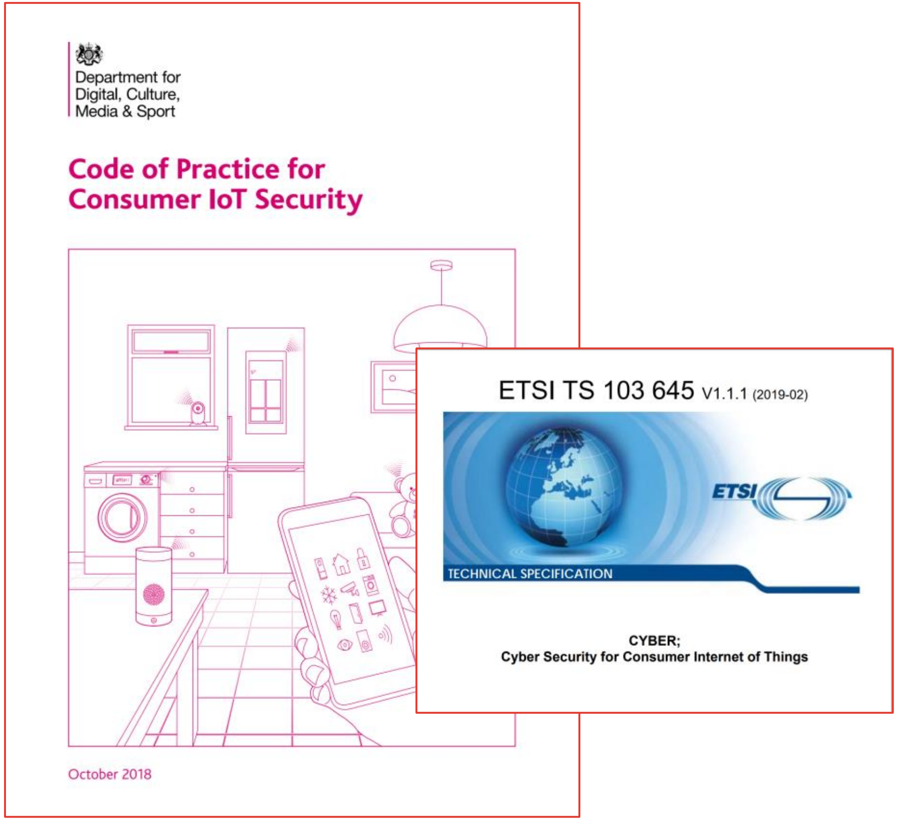
UCL WARWICK Imperial College London Lancaster University SURREY Southampton CARDIFF

INTERNATIONAL DEVELOPMENT ON IOT SECURITY

We conducted a scoping literature review between September and October 2017[5] and included[6] reports from the leading eleven international fora[7] that are shaping the global governance and policy conversations about the security of the IoT.

Our analysis reveals that there have been some nascent international conversations about the policy implications of the IoT over the last five years. Debates around issues such as security by default, (self-)regulation, standardisation and security measures have emerged, though the content and nature of these debates varies and they are not always inclusive of a wide range of stakeholders. Below, we summarise ten of the most commonly shared themes.

Security By Default
Collaboration, PPP and Consensus
Data Management and Transparency
Standardisation
Liability
Key Themes
Training and Capacity Building
Regulation vs. Self-Regulation
Procurement
Certification and Trust
Research and Development



Department for Digital, Culture, Media & Sport

Code of Practice for Consumer IoT Security

October 2018

ETSI TS 103 645 V1.1.1 (2019-02)

CYBER;
Cyber Security for Consumer Internet of Things

Tanczer, L. M., Blythe, J., Yahya, F., Brass, I., Elsden, M., Blackstock, J., & Carr, M. (2018). *Summary literature review of industry recommendations and international developments on IoT security* (pp. 1–18).

United Kingdom

1) No default passwords

2) Implement a vulnerability disclosure policy

3) Keep software updated

4) Securely store credentials and security-sensitive data

5) Communicate securely

6) Minimise exposed attack surfaces

7) Ensure software integrity

8) Ensure that personal data is protected

9) Make systems resilient to outages

10) Monitor system telemetry data

11) Make it easy for consumers to delete personal data

12) Make installation and maintenance of devices easy

13) Validate input data

United Kingdom

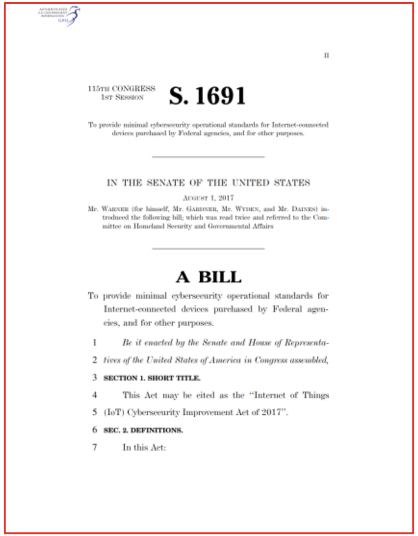
1) No default passwords
2) Implement a vulnerability disclosure policy
3) Keep software updated
4) Securely store credentials and security-sensitive data
5) Communicate securely
6) Minimise exposed attack surfaces
7) Ensure software integrity
8) Ensure that personal data is protected
9) Make systems resilient to outages
10) Monitor system telemetry data
11) Make it easy for consumers to delete personal data
12) Make installation and maintenance of devices easy
13) Validate input data

Rest of the World?

IoT Cybersecurity Improvement Act

It’s about **government procurement**

2017



II

115TH CONGRESS
1ST SESSION

S. 1691

To provide minimal cybersecurity operational standards for Internet-connected devices purchased by Federal agencies, and for other purposes.

IN THE SENATE OF THE UNITED STATES

AUGUST 1, 2017

Mr. WARNER (for himself, Mr. GARDNER, Mr. WYDEN, and Mr. DAINES) introduced the following bill; which was read twice and referred to the Committee on Homeland Security and Governmental Affairs

A BILL

To provide minimal cybersecurity operational standards for Internet-connected devices purchased by Federal agencies, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

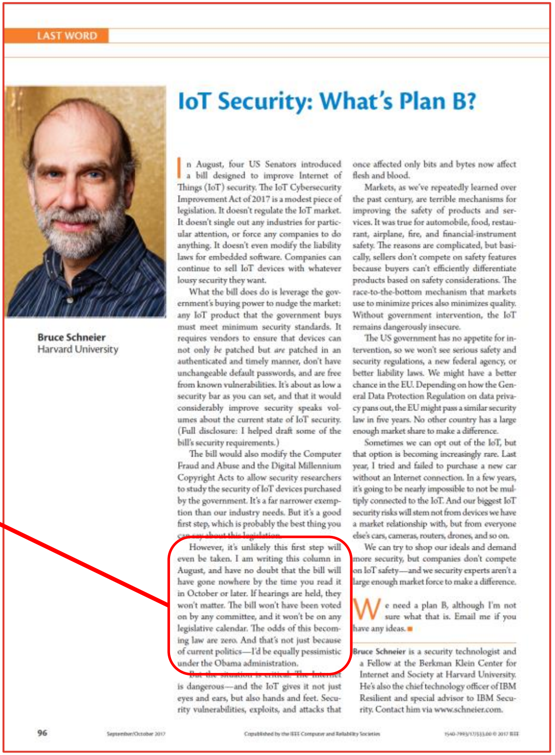
This Act may be cited as the “Internet of Things (IoT) Cybersecurity Improvement Act of 2017”.

SEC. 2. DEFINITIONS.

In this Act:

IoT Cybersecurity Improvement Act

“I am writing this column in August, and have no doubt that ***the bill will have gone nowhere by the time you read*** *it in October or later. If hearings are held, they won’t matter. The bill won’t have been voted on by any committee, and it won’t be on any legislative calendar.* ***The odds of this becoming law are zero****.”*



LAST WORD

IoT Security: What’s Plan B?

Bruce Schneier
Harvard University

In August, four US Senators introduced a bill designed to improve Internet of Things (IoT) security. The IoT Cybersecurity Improvement Act of 2017 is a modest piece of legislation. It doesn't regulate the IoT market. It doesn't single out any industries for particular attention, or force any companies to do anything. It doesn't even modify the liability laws for embedded software. Companies can continue to sell IoT devices with whatever lousy security they want.

What the bill does do is leverage the government's buying power to nudge the market: any IoT product that the government buys must meet minimum security standards. It requires vendors to ensure that devices can not only *be* patched but *are* patched in an authenticated and timely manner, don't have unchangeable default passwords, and are free from known vulnerabilities. It's about as low a security bar as you can set, and that it would considerably improve security speaks volumes about the current state of IoT security. (Full disclosure: I helped draft some of the bill's security requirements.)

The bill would also modify the Computer Fraud and Abuse and the Digital Millennium Copyright Acts to allow security researchers to study the security of IoT devices purchased by the government. It's a far narrower exemption than our industry needs. But it's a good first step, which is probably the best thing you can say about this legislation.

However, it's unlikely this first step will even be taken. I am writing this column in August, and have no doubt that the bill will have gone nowhere by the time you read it in October or later. If hearings are held, they won't matter. The bill won't have been voted on by any committee, and it won't be on any legislative calendar. The odds of this becoming law are zero. And that's not just because of current politics—I'd be equally pessimistic under the Obama administration.

But the situation is critical. The Internet is dangerous—and the IoT gives it not just eyes and ears, but also hands and feet. Security vulnerabilities, exploits, and attacks that once affected only bits and bytes now affect flesh and blood.

Markets, as we've repeatedly learned over the past century, are terrible mechanisms for improving the safety of products and services. It was true for automobile, food, restaurant, airplane, fire, and financial-instrument safety. The reasons are complicated, but basically, sellers don't compete on safety features because buyers can't efficiently differentiate products based on safety considerations. The race-to-the-bottom mechanism that markets use to minimize prices also minimizes quality. Without government intervention, the IoT remains dangerously insecure.

The US government has no appetite for intervention, so we won't see serious safety and security regulations, a new federal agency, or better liability laws. We might have a better chance in the EU. Depending on how the General Data Protection Regulation on data privacy pans out, the EU might pass a similar security law in five years. No other country has a large enough market share to make a difference.

Sometimes we can opt out of the IoT, but that option is becoming increasingly rare. Last year, I tried and failed to purchase a new car without an Internet connection. In a few years, it's going to be nearly impossible to not be multiply connected to the IoT. And our biggest IoT security risks will stem not from devices we have a market relationship with, but from everyone else's cars, cameras, routers, drones, and so on.

We can try to shop our ideals and demand more security, but companies don't compete on IoT safety—and we security experts aren't a large enough market force to make a difference.

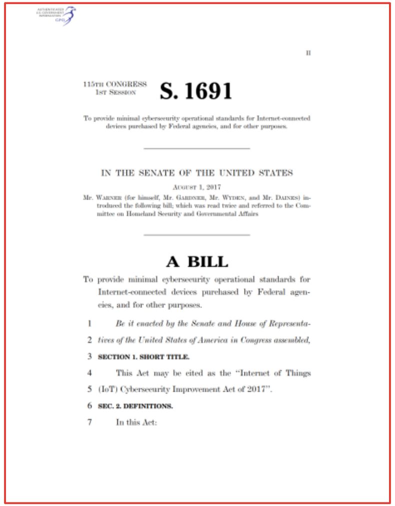
We need a plan B, although I'm not sure what that is. Email me if you have any ideas. ■

Bruce Schneier is a security technologist and a Fellow at the Berkman Klein Center for Internet and Society at Harvard University. He's also the chief technology officer of IBM Resilient and special advisor to IBM Security. Contact him via www.schneier.com.

96 September/October 2017 Copublished by the IEEE Computer and Reliability Societies 1540-7993/17/$33.00 © 2017 IEEE

Schneier, B. (2017). IoT Security: What’s Plan B? *IEEE Security Privacy*, *15*(5), 96–96. https://doi.org/10.1109/MSP.2017.3681066

IoT Cybersecurity Improvement Act (2017, 2018, 2019)



II

115th CONGRESS
1st Session

S. 1691

To provide minimal cybersecurity operational standards for Internet-connected devices purchased by Federal agencies, and for other purposes.

IN THE SENATE OF THE UNITED STATES

August 1, 2017

Mr. Warner (for himself, Mr. Gardner, Mr. Wyden, and Mr. Daines) introduced the following bill; which was read twice and referred to the Committee on Homeland Security and Governmental Affairs

A BILL

To provide minimal cybersecurity operational standards for Internet-connected devices purchased by Federal agencies, and for other purposes.

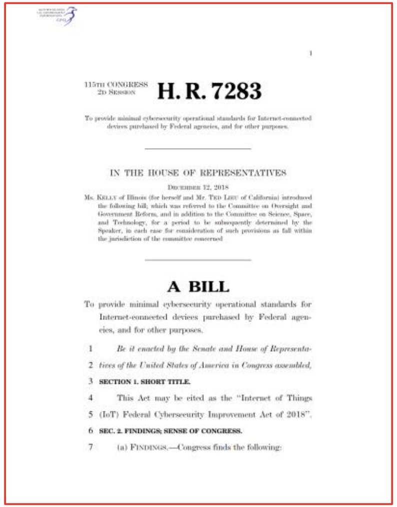
Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Internet of Things (IoT) Cybersecurity Improvement Act of 2017".

SEC. 2. DEFINITIONS.

In this Act:



I

115th CONGRESS
2d Session

H. R. 7283

To provide minimal cybersecurity operational standards for Internet-connected devices purchased by Federal agencies, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

December 12, 2018

Ms. Kelly of Illinois (for herself and Mr. Ted Lieu of California) introduced the following bill; which was referred to the Committee on Oversight and Government Reform, and in addition to the Committee on Science, Space, and Technology, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

A BILL

To provide minimal cybersecurity operational standards for Internet-connected devices purchased by Federal agencies, and for other purposes.

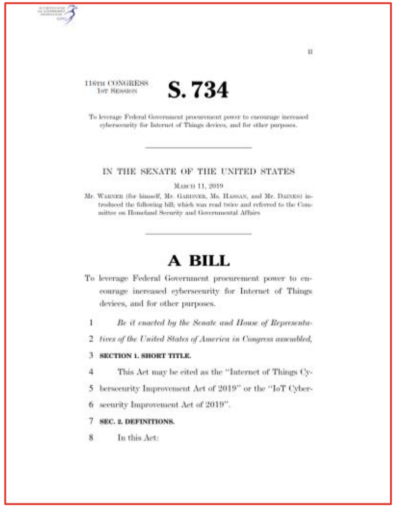
Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Internet of Things (IoT) Federal Cybersecurity Improvement Act of 2018".

SEC. 2. FINDINGS; SENSE OF CONGRESS.

(a) Findings.—Congress finds the following:



II

116th CONGRESS
1st Session

S. 734

To leverage Federal Government procurement power to encourage increased cybersecurity for Internet of Things devices, and for other purposes.

IN THE SENATE OF THE UNITED STATES

March 11, 2019

Mr. Warner (for himself, Mr. Gardner, Ms. Hassan, and Mr. Daines) introduced the following bill; which was read twice and referred to the Committee on Homeland Security and Governmental Affairs

A BILL

To leverage Federal Government procurement power to encourage increased cybersecurity for Internet of Things devices, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

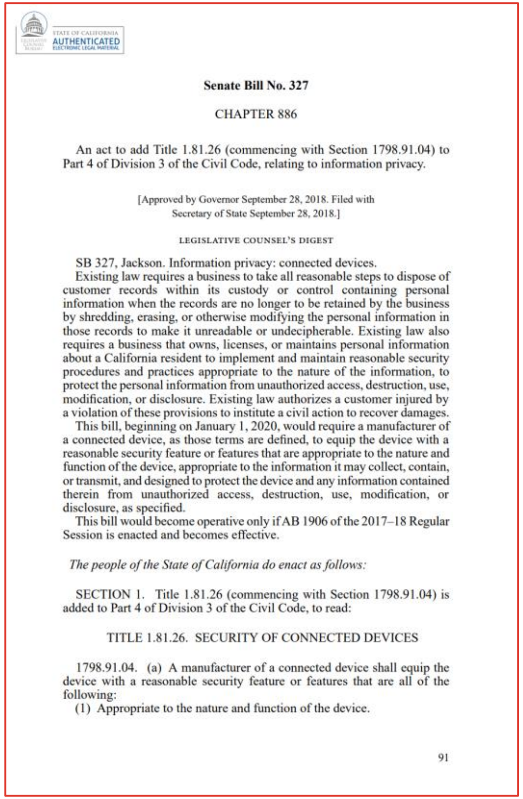
This Act may be cited as the "Internet of Things Cybersecurity Improvement Act of 2019" or the "IoT Cybersecurity Improvement Act of 2019".

SEC. 2. DEFINITIONS.

In this Act:

California

“*It’s based on the misconception of adding security features. It’s like dieting, where people insist you should eat more kale, which does little to address the problem you are pigging out on potato chips. The key to dieting is not eating more but eating less. The same is true of cybersecurity, where* ***the point is not to add “security features” but to remove “insecure features***”. (Graham, 2018)



STATE OF CALIFORNIA
AUTHENTICATED
ELECTRONIC LEGAL MATERIAL

Senate Bill No. 327

CHAPTER 886

An act to add Title 1.81.26 (commencing with Section 1798.91.04) to Part 4 of Division 3 of the Civil Code, relating to information privacy.

[Approved by Governor September 28, 2018. Filed with
Secretary of State September 28, 2018.]

LEGISLATIVE COUNSEL’S DIGEST

SB 327, Jackson. Information privacy: connected devices.

Existing law requires a business to take all reasonable steps to dispose of customer records within its custody or control containing personal information when the records are no longer to be retained by the business by shredding, erasing, or otherwise modifying the personal information in those records to make it unreadable or undecipherable. Existing law also requires a business that owns, licenses, or maintains personal information about a California resident to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure. Existing law authorizes a customer injured by a violation of these provisions to institute a civil action to recover damages.

This bill, beginning on January 1, 2020, would require a manufacturer of a connected device, as those terms are defined, to equip the device with a reasonable security feature or features that are appropriate to the nature and function of the device, appropriate to the information it may collect, contain, or transmit, and designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure, as specified.

This bill would become operative only if AB 1906 of the 2017–18 Regular Session is enacted and becomes effective.

The people of the State of California do enact as follows:

SECTION 1. Title 1.81.26 (commencing with Section 1798.91.04) is added to Part 4 of Division 3 of the Civil Code, to read:

TITLE 1.81.26. SECURITY OF CONNECTED DEVICES

1798.91.04. (a) A manufacturer of a connected device shall equip the device with a reasonable security feature or features that are all of the following:

(1) Appropriate to the nature and function of the device.

91

Graham, R. (2018, September 10). California’s bad IoT law. Retrieved June 18, 2019, from Errata Security website: https://blog.erratasec.com/2018/09/californias-bad-iot-law.html#.W6EV2KZKg2w

Wait! – Will we be responsible?!

CSIRTs Role in IIoT Vulnerabilities

- Alongside the Network and Information Systems (NIS) Directive, both the UK/EU Cybersecurity Strategies cite the **importance of CERTs** in quickly addressing cybersecurity risks
- Hence, in conjunction with ENISA, CERTs will have a key role in:
  - Training exercises, issuing guidance, ensuring cooperation across border, raising awareness, and finding strategies to address nascent IoT security risks (Urquhart & McAuley, 2018)

Urquhart, L., & McAuley, D. (2018). Avoiding the internet of insecure industrial things. *Computer Law & Security Review*, *34*(3), 450–466. https://doi.org/10.1016/j.clsr.2017.12.004

Magnitude of Risks

- "Constituency will become ten, ten times bigger than it is now" (P12)
- Some sectors more affected than others
- However, still not a big topic in the CSIRT community

PSIRTs' Importance

- Do something, states are currently still ill-equipped to do: Cooperation / Trust

  IoT = "PSIRT problem" (P16)
- CSIRTs have to "cooperate with them" (P12) more
- Requires vendor buy-in

Fine, but what else is there?

Next to mandatory baseline requirements & best practices…

(1) Certify!

- The proposal also includes the creation of the first **voluntary** EU cybersecurity certification framework for ICT products, which will include IoT
- But how to make this “**dynamic**”?

EUROPEAN
COMMISSION

Brussels, 13.9.2017
COM(2017) 477 final

2017/0225 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act")

(Text with EEA relevance)

{SWD(2017) 500 final}
{SWD(2017) 501 final}
{SWD(2017) 502 final}

LLOYD'S

Emerging Risk Report 2018
Technology

Networked world
Risks and opportunities in the Internet of Things

Standardisation and Certification of the ‘Internet of Things’

Éireann Leverett[1] Richard Clayton[2] Ross Anderson[3]

May 22, 2017

Abstract

We report on a research project for the European Commission into what will happen to safety regulation once computers are embedded invisibly everywhere. The European Union already regulates many aspects of the safety of vehicles, medical devices, electrical equipment, domestic appliances and even toys. As these devices and systems are recruited to ‘The Internet of Things’, their vulnerabilities (whether old or new) may be remotely exploited, with consequent risks. Many regulators who previously thought only in terms of safety will have to start thinking of security as well. The systems and devices that are starting to expose their security and safety vulnerabilities to the whole Internet are certified under a disparate range of European, national, industry and other schemes. In this paper we describe the problems and outline the opportunities for governments, industry and researchers. The EU is already the world's main privacy regulator, as Washington doesn't care and nobody else is big enough to matter; it should aim to become the main safety regulator too – or risk compromising the safety mission it already has. To deliver, it will need to coordinate the ‘rows’ of liability, transparency and privacy principles with the ‘columns’ of specific industry regulations on safety and testing. We identify missing institutional resources and suggest a strategy for filling the gap. Above all, the European institutions and regulatory networks need cybersecurity expertise to support safety, privacy, consumer protection and competition, rather than having policy in these areas overshadowed or even pre-empted by Member States' national security concerns. For industry and practitioners, the main message is that safety and security are merging: safety engineers are going to have to learn all about security, and vice versa. This affects everyone from working engineers to the folks in the test labs and the regulators' committees that set the standards to which they test. Researchers will have lots of new topics, from the design of the next generation of regulatory institutions to technical topics such as sustainability of software and the toolchains that support it. How do we write code for which security patches must be made available for the next 30 years? This poses many fascinating new combinations of problems in both engineering and economics.

[1] Privacy International: eireann@privacyinternational.org
[2] Computer Laboratory, University of Cambridge: richard.clayton@cl.cam.ac.uk
[3] Computer Laboratory, University of Cambridge: ross.anderson@cl.cam.ac.uk

1

enisa

Overview of ICT certification laboratories

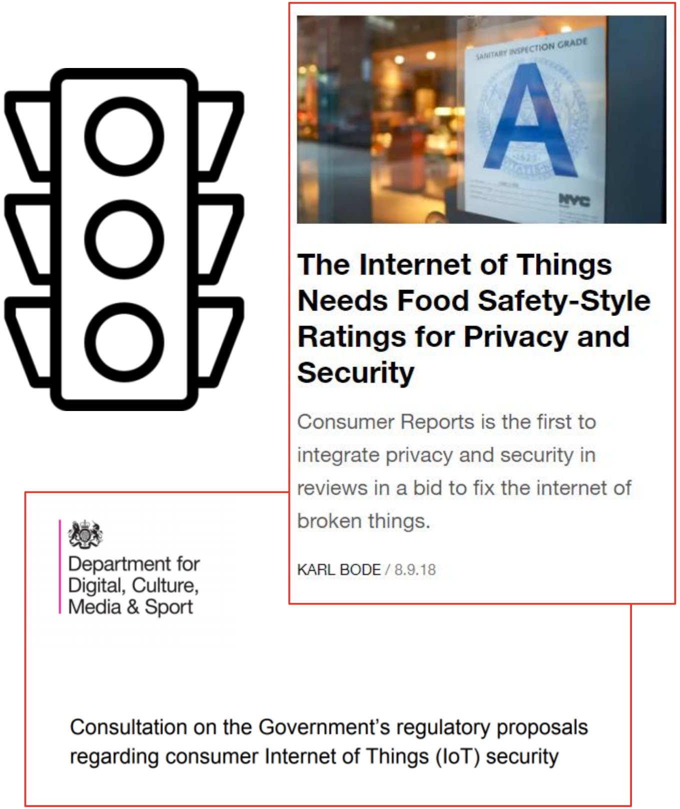
FINAL
V1.1
JANUARY 2018

www.enisa.europa.eu European Union Agency For Network and Information Security

Leverett, E., Clayton, R., & Anderson, R. (2017). Standardisation and Certification of the ‘Internet of Things.’ *Proceedings of WEIS*, 1–24. Retrieved from https://pdfs.semanticscholar.org/f61d/7dc82a4a7687c921e8e01661761328e66bc9.pdf
Kleinhans, J.-P., & Schmitz, P. (2018, July 11). Eine Zertifizierung reicht bei der IT-Sicherheit nicht aus! [Security Insider]. Retrieved June 18, 2019, from https://www.security-insider.de/eine-zertifizierung-reicht-bei-der-it-sicherheit-nicht-aus-a-771056/

(2) Label!

- Emami-Naeini et al. (2019) showed that surveyed participants **approved of labelling** schemes for IoT devices.
- According to Baldini et al. (2016) a label should be associated with the following **dimensions**:
  a) Level of assurance e.g., at what level a system was tested;
  b) Domain e.g., energy, road, transportation
  c) Certification type e.g., self-certification, third-party certification etc.
- Johnson et al. (2019) studied consumers' **willingness to pay** for graded label schemes and outlined the strengths and weakness of different designs.



The Internet of Things Needs Food Safety-Style Ratings for Privacy and Security

Consumer Reports is the first to integrate privacy and security in reviews in a bid to fix the internet of broken things.

KARL BODE / 8.9.18

Department for Digital, Culture, Media & Sport

Consultation on the Government's regulatory proposals regarding consumer Internet of Things (IoT) security

Emami-Naeini, P., Dixon, H., Agarwal, Y., & Cranor, L. F. (2019). Exploring How Privacy and Security Factor into IoT Device Purchase Behavior. *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, 534:1–534:12. https://doi.org/10.1145/3290605.3300764
Baldini, G., Skarmeta, A., Fourneret, E., Neisse, R., Legeard, B., & Gall, F. L. (2016). Security certification and labelling in Internet of Things. 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT), 627–632. https://doi.org/10.1109/WF-IoT.2016.7845514
Johnson, S., Blythe, J. M., Manning, M., & Wong, G. (2019). The impact of IoT security labelling on consumer product choice and willingness to pay [Preprint]. https://doi.org/10.31235/osf.io/4yxp2

(3) Liability!

- **Software liability** can increase the accountability and responsibility of manufacturers and creates incentives to internalise external costs.

OR

- Internalise negative externalities for the distributor by increasing the accountability and responsibility of the distributor through **distributor liability**.

Kleinhans, J.-P. (2017). *Internet of Insecure Things. Can Security Assessment Cure Market Failures?* Retrieved from Stiftung Neue Verantwortung website: https://www.stiftung-nv.de/sites/default/files/internet_of_insecure_things.pdf

Also…

Personalised Privacy Assistants

Intelligent agents capable of learning the **privacy preferences** of their users over time, **semi-automatically configuring many settings**, and making many privacy decisions on their behalf.

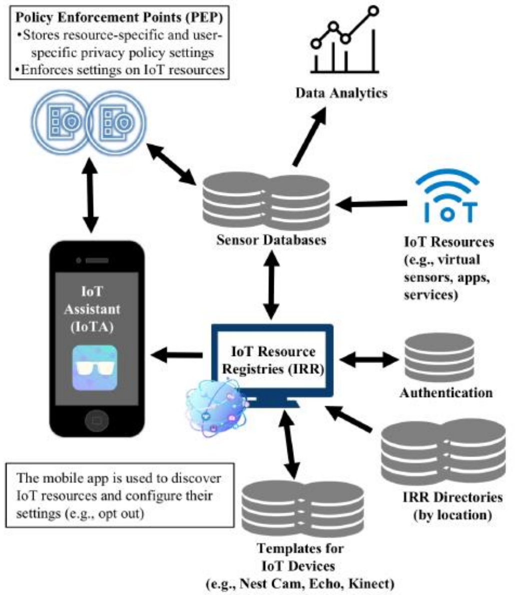

Policy Enforcement Points (PEP)
•Stores resource-specific and user-specific privacy policy settings
•Enforces settings on IoT resources
Data Analytics
Sensor Databases
IoT
IoT Resources (e.g., virtual sensors, apps, services)
IoT Assistant (IoTA)
IoT Resource Registries (IRR)
Authentication
IRR Directories (by location)
The mobile app is used to discover IoT resources and configure their settings (e.g., opt out)
Templates for IoT Devices (e.g., Nest Cam, Echo, Kinect)

Figure 3: Interaction among components of our proposed system. The privacy assistant discovers IoT resources through IoT Resource Registries (IRR), and preferences are enforced through Policy Enforcement Points (PEP).

Das, A., Degeling, M., Smullen, D., & Sadeh, N. (2018). Personalized Privacy Assistants for the Internet of Things: Providing Users with Notice and Choice. *IEEE Pervasive Computing*, *17*(3), 35–46. https://doi.org/10.1109/MPRV.2018.03367733

Databox

Open-source **personal networked device**, augmented by cloud-hosted services, that collates, curates, and mediates access to an individual’s personal data by verified and audited third party applications and services

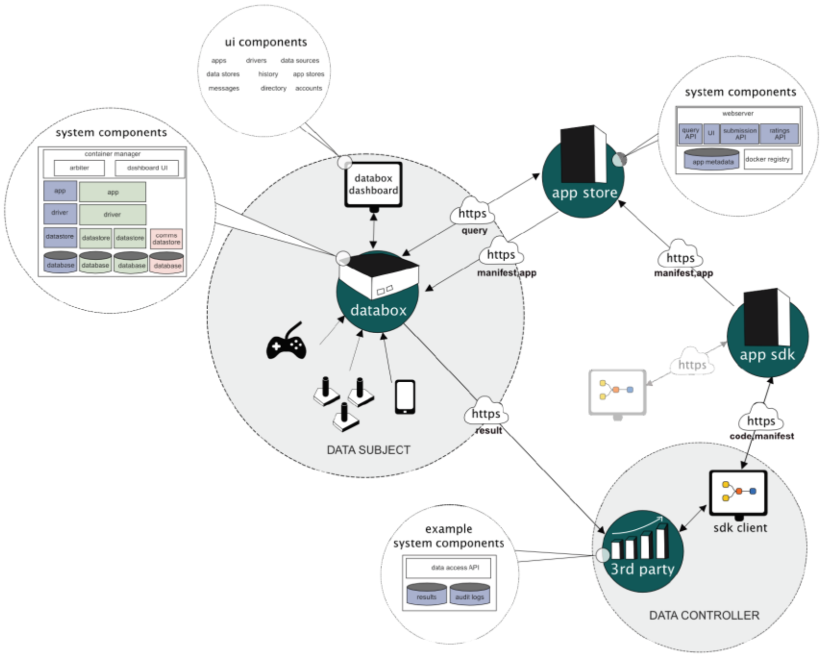
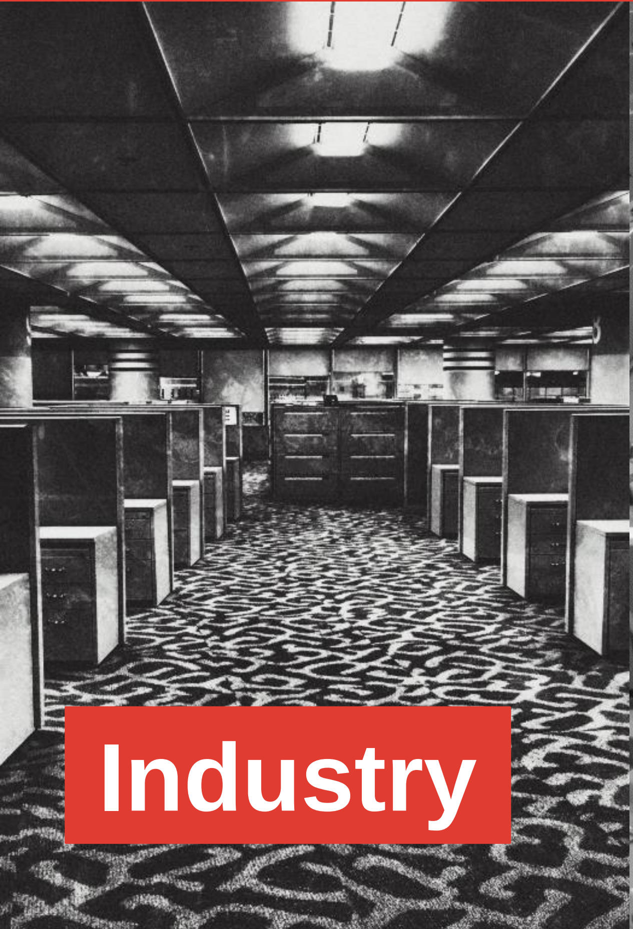


Figure 1. The IoT Databox Model.

Urquhart, L., Lodge, T., & Crabtree, A. (2018). *Demonstrably Doing Accountability in the Internet of Things* (pp. 1–31). Retrieved from https://arxiv.org/abs/1801.07168

Someone will have to be responsible.

Department of Science, Technology, Engineering and Public Policy (STEaPP)



Industry

Politics

Society

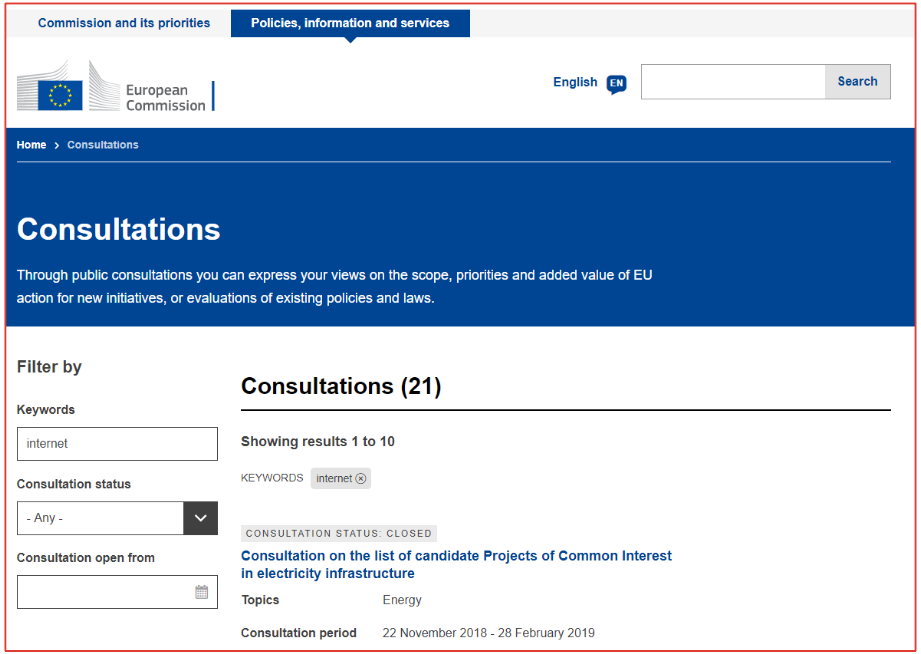
Arguments brought forward…

- World Trade Organization (**WTO**)
- Organization for Economic Co-Operation and Development (**OECD**)
- World Economic Forum (**WEF**)

…could be responsible.

Join the… debate

Submit Evidence to Consultations



Commission and its priorities
Policies, information and services
European Commission
English EN
Search
Home › Consultations

Consultations

Through public consultations you can express your views on the scope, priorities and added value of EU action for new initiatives, or evaluations of existing policies and laws.

Filter by

Keywords: internet

Consultation status: - Any -

Consultation open from

Consultations (21)

Showing results 1 to 10

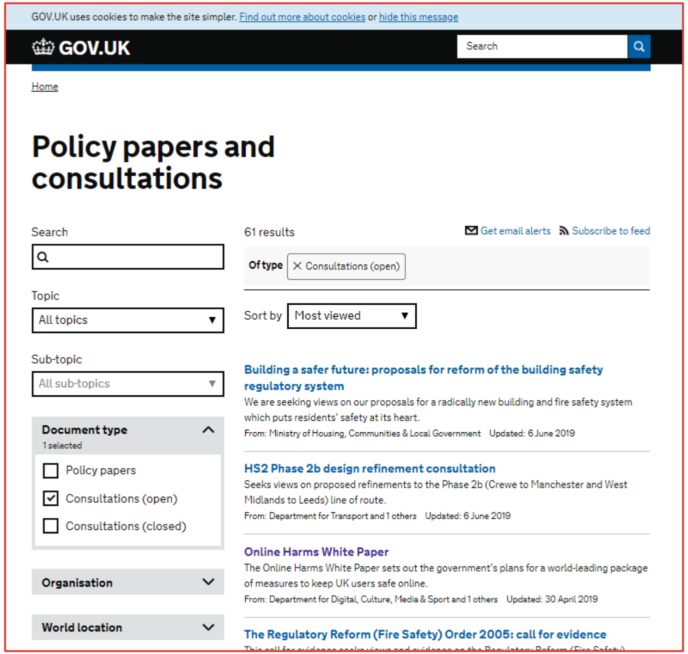
KEYWORDS internet ⊗

CONSULTATION STATUS: CLOSED

Consultation on the list of candidate Projects of Common Interest in electricity infrastructure

Topics: Energy

Consultation period: 22 November 2018 - 28 February 2019



GOV.UK uses cookies to make the site simpler. Find out more about cookies or hide this message
GOV.UK
Search
Home

Policy papers and consultations

Search

Topic: All topics

Sub-topic: All sub-topics

Document type
1 selected

□ Policy papers
☑ Consultations (open)
□ Consultations (closed)

Organisation

World location

61 results

Get email alerts Subscribe to feed

Of type ✕ Consultations (open)

Sort by: Most viewed

Building a safer future: proposals for reform of the building safety regulatory system
We are seeking views on our proposals for a radically new building and fire safety system which puts residents' safety at its heart.
From: Ministry of Housing, Communities & Local Government   Updated: 6 June 2019

HS2 Phase 2b design refinement consultation
Seeks views on proposed refinements to the Phase 2b (Crewe to Manchester and West Midlands to Leeds) line of route.
From: Department for Transport and 1 others   Updated: 6 June 2019

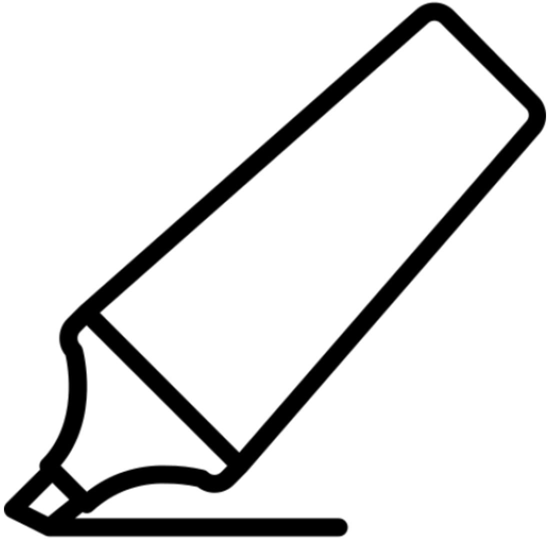
Online Harms White Paper
The Online Harms White Paper sets out the government's plans for a world-leading package of measures to keep UK users safe online.
From: Department for Digital, Culture, Media & Sport and 1 others   Updated: 30 April 2019

The Regulatory Reform (Fire Safety) Order 2005: call for evidence

https://ec.europa.eu/info/consultations_en
https://www.gov.uk/search/policy-papers-and-consultations

Promise, we are close to the end!

I hope I could highlight today…

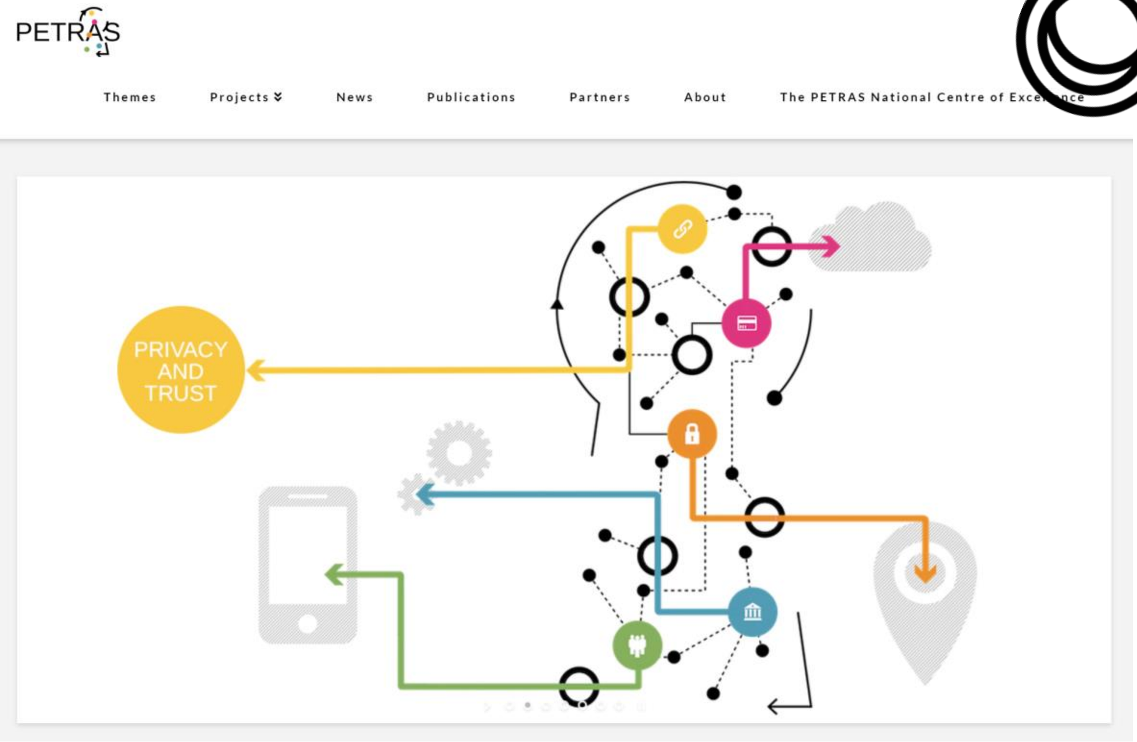


I hope I could highlight today…

- Why the IoT / Internet+ / or whatever we want to call it **matters** (esp. as it does not seem to go away)
- Some **policy / governance** developments that are underway (and have happened for quite some time)
- How the **user** fits into this whole framework
- That **CSIRTs / PSIRTs** will (continue to!) matter in the IoT ecosystem
- And that, in the end **not all hope is (probably) lost!**

If all of this makes you want to hear more…

Have a look at…



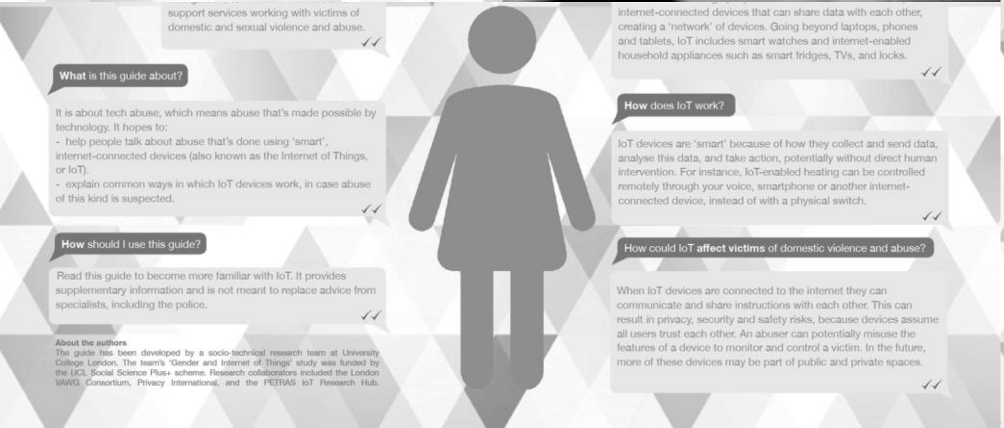
Department of Science, Technology, Engineering and Public Policy (STEaPP)

UCL

SMART ABUSE

UCL STEaPP 2nd floor, Boston House, 36-38 Fitzroy Square, London, W1T 6EY, United Kingdom
00.00
July 2018
https://www.ucl.ac.uk/steapp
PETRAS
London VAWG Consortium
TECH ABUSE
UCL

How internet-connected devices can affect victims of gender-based domestic and sexual violence and abuse



support services working with victims of domestic and sexual violence and abuse.

What is this guide about?

It is about tech abuse, which means abuse that's made possible by technology. It hopes to:

- help people talk about abuse that's done using 'smart', internet-connected devices (also known as the Internet of Things, or IoT).
- explain common ways in which IoT devices work, in case abuse of this kind is suspected.

How should I use this guide?

Read this guide to become more familiar with IoT. It provides supplementary information and is not meant to replace advice from specialists, including the police.

About the authors
The guide has been developed by a socio-technical research team at University College London. The team's 'Gender and Internet of Things' study was funded by the UCL Social Science Plus+ scheme. Research collaborators included the London VAWG Consortium, Privacy International, and the PETRAS IoT Research Hub.

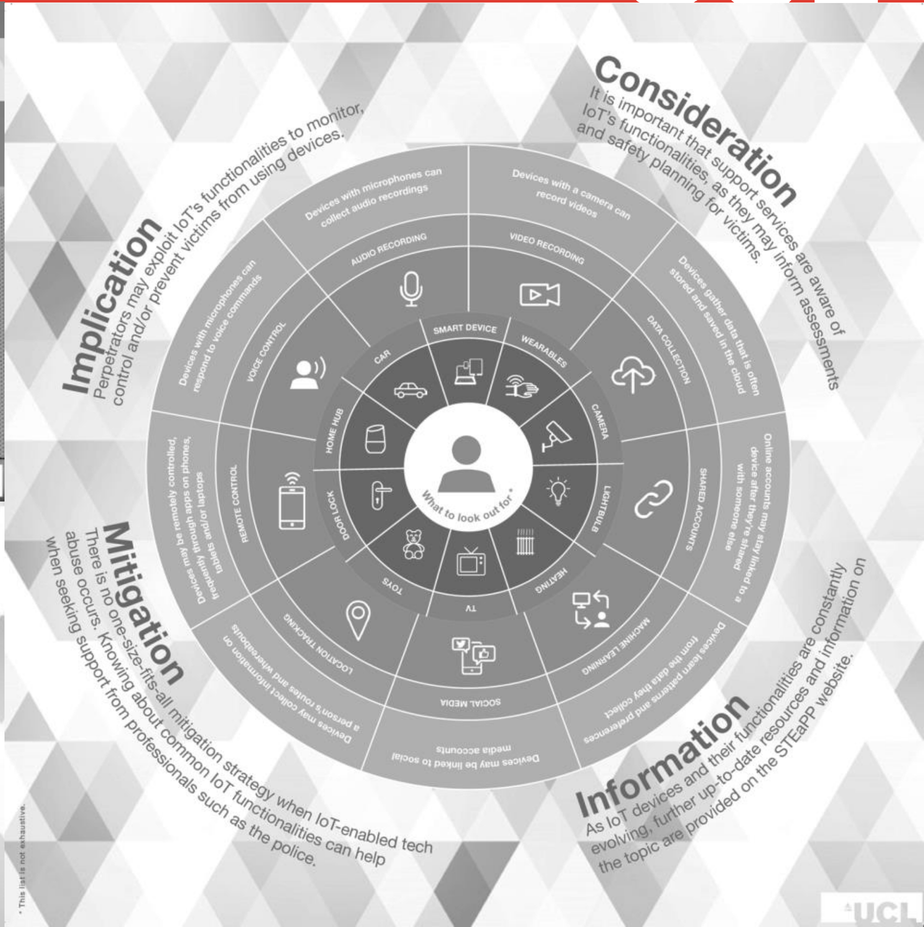
internet-connected devices that can share data with each other, creating a 'network' of devices. Going beyond laptops, phones and tablets, IoT includes smart watches and internet-enabled household appliances such as smart fridges, TVs, and locks.

How does IoT work?

IoT devices are 'smart' because of how they collect and send data, analyse this data, and take action, potentially without direct human intervention. For instance, IoT-enabled heating can be controlled remotely through your voice, smartphone or another internet-connected device, instead of with a physical switch.

How could IoT **affect victims** of domestic violence and abuse?

When IoT devices are connected to the internet they can communicate and share instructions with each other. This can result in privacy, security and safety risks, because devices assume all users trust each other. An abuser can potentially misuse the features of a device to monitor and control a victim. In the future, more of these devices may be part of public and private spaces.



Devices with microphones can collect audio recordings

Devices with a camera can record videos

Devices gather data that is often stored and saved in the cloud

Online accounts may stay linked to a device after they're shared with someone else

Devices learn patterns and preferences from the data they collect

Devices may be linked to social media accounts

Devices may collect information on a person's routes and whereabouts

Devices may be remotely controlled, frequently through apps on phones, tablets and/or laptops

Devices with microphones can respond to voice commands

Implication
Perpetrators may exploit IoT's functionalities to monitor, control and/or prevent victims from using devices.

Consideration
It is important that support services are aware of IoT's functionalities, as they may inform assessments and safety planning for victims.

Information
As IoT devices and their functionalities are constantly evolving, further up-to-date resources and information on the topic are provided on the STEaPP website.

Mitigation
There is no one-size-fits-all mitigation strategy when IoT-enabled tech abuse occurs. Knowing about common IoT functionalities can help when seeking support from professionals such as the police.

* This list is not exhaustive.

Department of Science, Technology, Engineering and Public Policy (STEaPP)

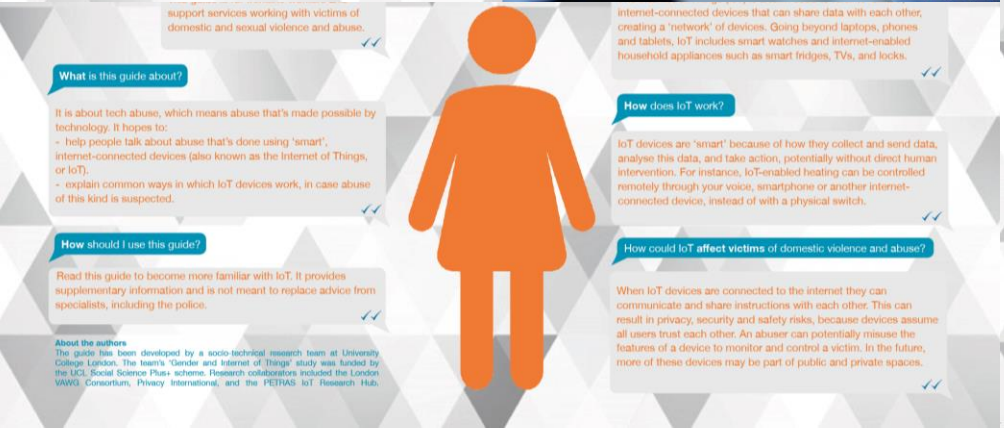
UCL STEaPP 2nd floor, Boston House, 36-38 Fitzroy Square, London, W1T 6EY, United Kingdom

00.00
July 2018

https://www.ucl.ac.uk/steapp

TECH ABUSE

How internet-connected devices can affect victims of gender-based domestic and sexual violence and abuse



support services working with victims of domestic and sexual violence and abuse.

What is this guide about?

It is about tech abuse, which means abuse that's made possible by technology. It hopes to:

- help people talk about abuse that's done using 'smart', internet-connected devices (also known as the Internet of Things, or IoT).
- explain common ways in which IoT devices work, in case abuse of this kind is suspected.

How should I use this guide?

Read this guide to become more familiar with IoT. It provides supplementary information and is not meant to replace advice from specialists, including the police.

About the authors
The guide has been developed by a socio-technical research team at University College London. The team's 'Gender and Internet of Things' study was funded by the UCL Social Science Plus+ scheme. Research collaborators included the London VAWG Consortium, Privacy International, and the PETRAS IoT Research Hub.

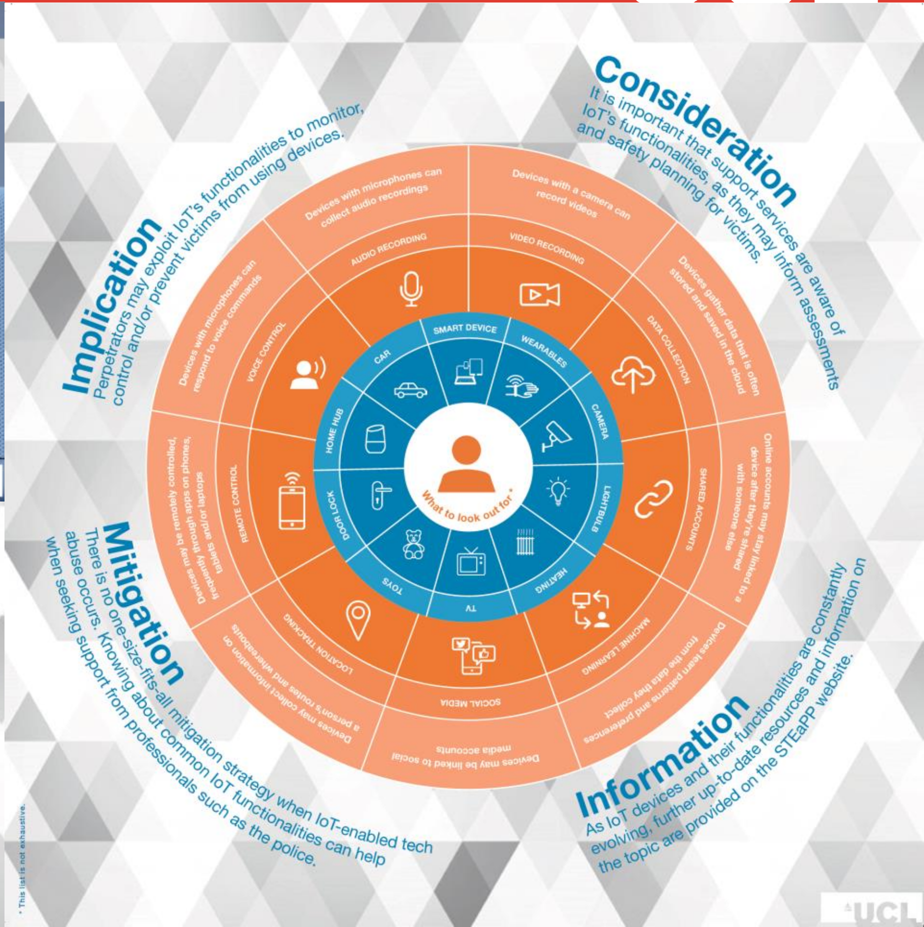
internet-connected devices that can share data with each other, creating a 'network' of devices. Going beyond laptops, phones and tablets, IoT includes smart watches and internet-enabled household appliances such as smart fridges, TVs, and locks.

How does IoT work?

IoT devices are 'smart' because of how they collect and send data, analyse this data, and take action, potentially without direct human intervention. For instance, IoT-enabled heating can be controlled remotely through your voice, smartphone or another internet-connected device, instead of with a physical switch.

How could IoT **affect victims** of domestic violence and abuse?

When IoT devices are connected to the internet they can communicate and share instructions with each other. This can result in privacy, security and safety risks, because devices assume all users trust each other. An abuser can potentially misuse the features of a device to monitor and control a victim. In the future, more of these devices may be part of public and private spaces.



Implication
Perpetrators may exploit IoT's functionalities to monitor, control and/or prevent victims from using devices.

Consideration
It is important that support services are aware of IoT's functionalities, as they may inform assessments and safety planning for victims.

Mitigation
There is no one-size-fits-all mitigation strategy when IoT-enabled tech abuse occurs. Knowing about common IoT functionalities can help when seeking support from professionals such as the police.

Information
As IoT devices and their functionalities are constantly evolving, further up-to-date resources and information on the topic are provided on the STEaPP website.

AUDIO RECORDING: Devices with microphones can collect audio recordings

VIDEO RECORDING: Devices with a camera can record videos

DATA COLLECTION: Devices gather data that is often stored and saved in the cloud

SHARED ACCOUNTS: Online accounts may stay linked to a device after they're shared with someone else

MACHINE LEARNING: Devices learn patterns and preferences from the data they collect

SOCIAL MEDIA: Devices may be linked to social media accounts

LOCATION TRACKING: Devices may collect information on a person's routes and whereabouts

REMOTE CONTROL: Devices may be remotely controlled, frequently through apps on phones, tablets and/or laptops

VOICE CONTROL: Devices with microphones can respond to voice commands

* This list is not exhaustive.

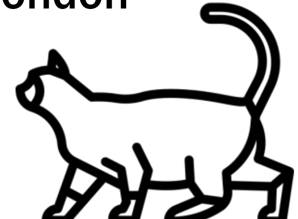
Speak to me, please!

a) I want to know what happens on IoT in **your country**!

b) I *_really_* would love to speak to CSIRTs/PSIRTs and conduct **semi-structured, unattributed interviews** for my research study on the incident response community.

Thank you.

Dr Leonie Maria Tanczer
University College London
@leotanczt



References

- Tanczer, L. M., Brass, I., & Carr, M. (2018). CSIRTs and Global Cybersecurity: How Technical Experts Support Science Diplomacy. *Global Policy*, *9*(S3), 60–66. https://doi.org/10.1111/1758-5899.12625
- Mattern, F., & Flörkemeier, C. (2010). Vom Internet der Computer zum Internet der Dinge. Informatik-Spektrum, 33(2), 107–121. https://doi.org/10.1007/s00287-010-0417-7
- Yang, Y., Wu, L., Yin, G., Li, L., & Zhao, H. (2017). A Survey on Security and Privacy Issues in Internet-of-Things. IEEE Internet of Things Journal, 4(5), 1250–1258. https://doi.org/10.1109/JIOT.2017.2694844
- Niyato, D., Lu, X., Wang, P., Kim, D. I., & Han, Z. (2016). Economics of Internet of Things: An information market approach. IEEE Wireless Communications, 23(4), 136–145. https://doi.org/10.1109/MWC.2016.7553037
- Giles, M. (2018, September 6). For safety's sake, we must slow innovation in internet-connected things. Retrieved June 17, 2019, from MIT Technology Review website: https://www.technologyreview.com/s/611948/for-safetys-sake-we-must-slow-innovation-in-internet-connected-things/

References

- Arcep. (2018). *Smartphones, tablets, voice assistants... Devices, the weak link in achieving an open internet* (pp. 1–65). Retrieved from Autorité de Régulation des Communications Électroniques et des Postes website: https://www.arcep.fr/uploads/tx_gspublication/rapport-terminaux-fev2018-ENG.pdf
- Williams, M., Nurse, J. R. C., & Creese, S. (2017). Privacy is the Boring Bit: User Perceptions and Behaviour in the Internet-of-Things. 2017 15th Annual Conference on Privacy, Security and Trust (PST), 181–18109. https://doi.org/10.1109/PST.2017.00029
- Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, *64*, 122–134. https://doi.org/10.1016/j.cose.2015.07.002
- Beresford, A. R., Kübler, D., & Preibusch, S. (2012). Unwillingness to pay for privacy: A field experiment. *Economics Letters*, *117*(1), 25–27. https://doi.org/10.1016/j.econlet.2012.04.077
- Carrascal, J. P., Riederer, C., Erramilli, V., Cherubini, M., & de Oliveira, R. (2013). Your Browsing Behavior for a Big Mac: Economics of Personal Information Online. Proceedings of the 22Nd International Conference on World Wide Web, 189–200. https://doi.org/10.1145/2488388.2488406

References

- Adams, A., & Sasse, M. A. (1999). Users Are Not the Enemy. *Communications of the ACM*, *42*(12), 40–46. https://doi.org/10.1145/322796.322806
- van der Zeeuw, A., van Deursen, A. J., & Jansen, G. (2019). Inequalities in the social use of the Internet of things: A capital and skills perspective. New Media & Society, 21(6), 1344–1361. https://doi.org/10.1177/1461444818821067
- Nissenbaum, H. (2011). A Contextual Approach to Privacy Online. Dædalus: Journal of the American Academy of Arts & Sciences, (4), 32–48.
- Bechmann, A. (2014). Non-Informed Consent Cultures: Privacy Policies and App Contracts on Facebook. Journal of Media Business Studies, 11(1), 21–38. https://doi.org/10.1080/16522354.2014.11073574
- boyd, danah, & Hargittai, E. (2010). Facebook privacy settings: Who cares? Hargittai. First Monday, 15(8). Retrieved from https://firstmonday.org/article/view/3086/2589
- Solove, D. (2013). Introduction: Privacy Self-Management and the Consent Dilemma. Harvard Law Review, 126, 1880–1903.

References

- Weber, R. H. (2009). Internet of things – Need for a new legal environment? Computer Law & Security Review, 25(6), 522–527. https://doi.org/10.1016/j.clsr.2009.09.002
- Weber, R. H. (2010). Internet of Things – New security and privacy challenges. Computer Law & Security Review, 26(1), 23–30. https://doi.org/10.1016/j.clsr.2009.11.008
- Weber, R. H. (2013). Internet of things–Governance quo vadis? Computer Law & Security Review, 29(4), 341–347.
- Brass, I., Tanczer, L. M., Carr, M., & Blackstock, J. (2017). Regulating IoT: Enabling or Disabling the Capacity of the Internet of Things? Risk & Regulation Magazine of the Centre for Analysis of Risk and Regulation (CARR), 33(Summer), 12–15.
- Tanczer, L. M., Brass, I., Elsden, M., Carr, M., & Blackstock, J. (2019). The United Kingdom’s Emerging Internet of Things (IoT) Policy Landscape. In R. Ellis & V. Mohan (Eds.), Rewired: Cybersecurity Governance (pp. 37–56). Hoboken, New Jersey: Wiley.
- Lopez, J., Rios, R., Bao, F., & Wang, G. (2017). Evolving privacy: From sensors to the Internet of Things. *Future Generation Computer Systems*, *75*(Supplement C), 46–57. https://doi.org/10.1016/j.future.2017.04.045

References

- Harbers, M., Bargh, M. S., Pool, R., Berkel, J. V., Braak, S. W. van den, & Choenni, S. (2018). A Conceptual Framework for Addressing IoT Threats: Challenges in Meeting Challenges. HICSS, 2215–2224. https://doi.org/10.24251/hicss.2018.278
- Bisenius, B. (2017). Product Safety of the Internet of Things [Product Safety Perspectives]. *IEEE Consumer Electronics Magazine*, *6*(3), 137–139. https://doi.org/10.1109/MCE.2017.2685018
- Zubiaga, A., Procter, R., & Maple, C. (2018). A Longitudinal Analysis of the Public Perception of the Opportunities and Challenges of the Internet of Things. PLOS ONE, 13(12), 1–18. https://doi.org/10.1371/journal.pone.0209472
- schraefel, m. c., & Gerding, E. (2013, 2017). Meaningful Consent in the Digital Economy. Retrieved July 29, 2017, from Meaningful Consent website: http://www.meaningfulconsent.org/
- Tanczer, L. M., Steenmans, I., Elsden, M., Blackstock, J., & Carr, M. (2018). Emerging risks in the IoT ecosystem: Who's afraid of the big bad smart fridge? Living in the Internet of Things: Cybersecurity of the IoT - 2018. Presented at the Living in the Internet of Things: Cybersecurity of the IoT - 2018, London, UK. https://doi.org/10.1049/cp.2018.0033
- Tanczer, L., Steenmans, I., Brass, I., & Carr, M. (2018). Networked World: Risks and Opportunities in the Internet of Things. London: Lloyds's of London. https://www.lloyds.com/news-and-risk-insight/risk-reports/library/technology/networked-world

References

- Beneteau, E., Richards, O. K., Zhang, M., Kientz, J. A., Yip, J., & Hiniker, A. (2019). Communication Breakdowns Between Families and Alexa. *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems - CHI '19*, 1–13. https://doi.org/10.1145/3290605.3300473
- Blythe, J., & Lefevre, C. (2018). *Cyberhygiene Insight Report* (pp. 1–12). Retrieved from IoTUK and PETRAS IoT Hub website: https://iotuk.org.uk/wp-content/uploads/2018/01/PETRAS-IoTUK-Cyberhygiene-Insight-Report.pdf
- Graham, R. (2018, September 10). California's bad IoT law. Retrieved June 18, 2019, from Errata Security website: https://blog.erratasec.com/2018/09/californias-bad-iot-law.html#.W6EV2KZKg2w
- Kleinhans, J.-P. (2017). *Internet of Insecure Things. Can Security Assessment Cure Market Failures?* Retrieved from Stiftung Neue Verantwortung website: https://www.stiftung-nv.de/sites/default/files/internet_of_insecure_things.pdf
- Kleinhans, J.-P. (2018). *Improving IoT security in the EU: Why pre-market certification is not enough and how to fix it*. Retrieved from Stiftung Neue Verantwortung website: https://www.stiftung-nv.de/en/publication/improving-iot-security-eu

References

- van Lieshout, M., & Emmert, S. (2018). RESPECT4U – Privacy as Innovation Opportunity. In M. Medina, A. Mitrakas, K. Rannenberg, E. Schweighofer, & N. Tsouroulas (Eds.), *Privacy Technologies and Policy* (pp. 43–60). Springer International Publishing.
- Ziegler, S., Evequoz, E., & Huamani, A. M. P. (2019). The Impact of the European General Data Protection Regulation (GDPR) on Future Data Business Models: Toward a New Paradigm and Business Opportunities. In A. Aagaard (Ed.), *Digital Business Models: Driving Transformation and Innovation* (pp. 201–226). https://doi.org/10.1007/978-3-319-96902-2_8
- Schneier, B. (2017). IoT Security: What's Plan B? IEEE Security Privacy, 15(5), 96–96. https://doi.org/10.1109/MSP.2017.3681066
- Urquhart, L., & McAuley, D. (2018). Avoiding the internet of insecure industrial things. *Computer Law & Security Review*, *34*(3), 450–466. https://doi.org/10.1016/j.clsr.2017.12.004
- Tanczer, L. M., Blythe, J., Yahya, F., Brass, I., Elsden, M., Blackstock, J., & Carr, M. (2018). *Summary literature review of industry recommendations and international developments on IoT security* (pp. 1–18). Retrieved from Department for Digital, Culture, Media & Sport; PETRAS IoT Hub website: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/686090/PETRAS_Literature_Review_of_Industry_Recommendations_and_International_Developments_on_IoT_Security.pdf
- Urquhart, L., Lodge, T., & Crabtree, A. (2018). Demonstrably Doing Accountability in the Internet of Things (pp. 1–31). Retrieved from https://arxiv.org/abs/1801.07168

References

- Leverett, E., Clayton, R., & Anderson, R. (2017). Standardisation and Certification of the ‘Internet of Things.’ *Proceedings of WEIS*, 1–24. Retrieved from https://pdfs.semanticscholar.org/f61d/7dc82a4a7687c921e8e01661761328e66bc9.pdf
- Kleinhans, J.-P., & Schmitz, P. (2018, July 11). Eine Zertifizierung reicht bei der IT-Sicherheit nicht aus! [Security Insider]. Retrieved June 18, 2019, from https://www.security-insider.de/eine-zertifizierung-reicht-bei-der-it-sicherheit-nicht-aus-a-771056/
- Payne, B. R., & Abegaz, T. T. (2018). Securing the Internet of Things: Best Practices for Deploying IoT Devices. In *Computer and Network Security Essentials* (pp. 493–506). https://doi.org/10.1007/978-3-319-58424-9_28
- Lee, M. (2018). An Empirical Study of Home IoT Services in South Korea: The Moderating Effect of the Usage Experience. *International Journal of Human–Computer Interaction:*, *35*(7), 535–547. https://doi.org/10.1080/10447318.2018.1480121
- Emami-Naeini, P., Dixon, H., Agarwal, Y., & Cranor, L. F. (2019). Exploring How Privacy and Security Factor into IoT Device Purchase Behavior. *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, 534:1–534:12. https://doi.org/10.1145/3290605.3300764
- Das, A., Degeling, M., Smullen, D., & Sadeh, N. (2018). Personalized Privacy Assistants for the Internet of Things: Providing Users with Notice and Choice. *IEEE Pervasive Computing*, *17*(3), 35–46. https://doi.org/10.1109/MPRV.2018.03367733