European ePrivacy Reform

Security considerations

EP, LIBE hearing, 11th April

Ilias Chantzos

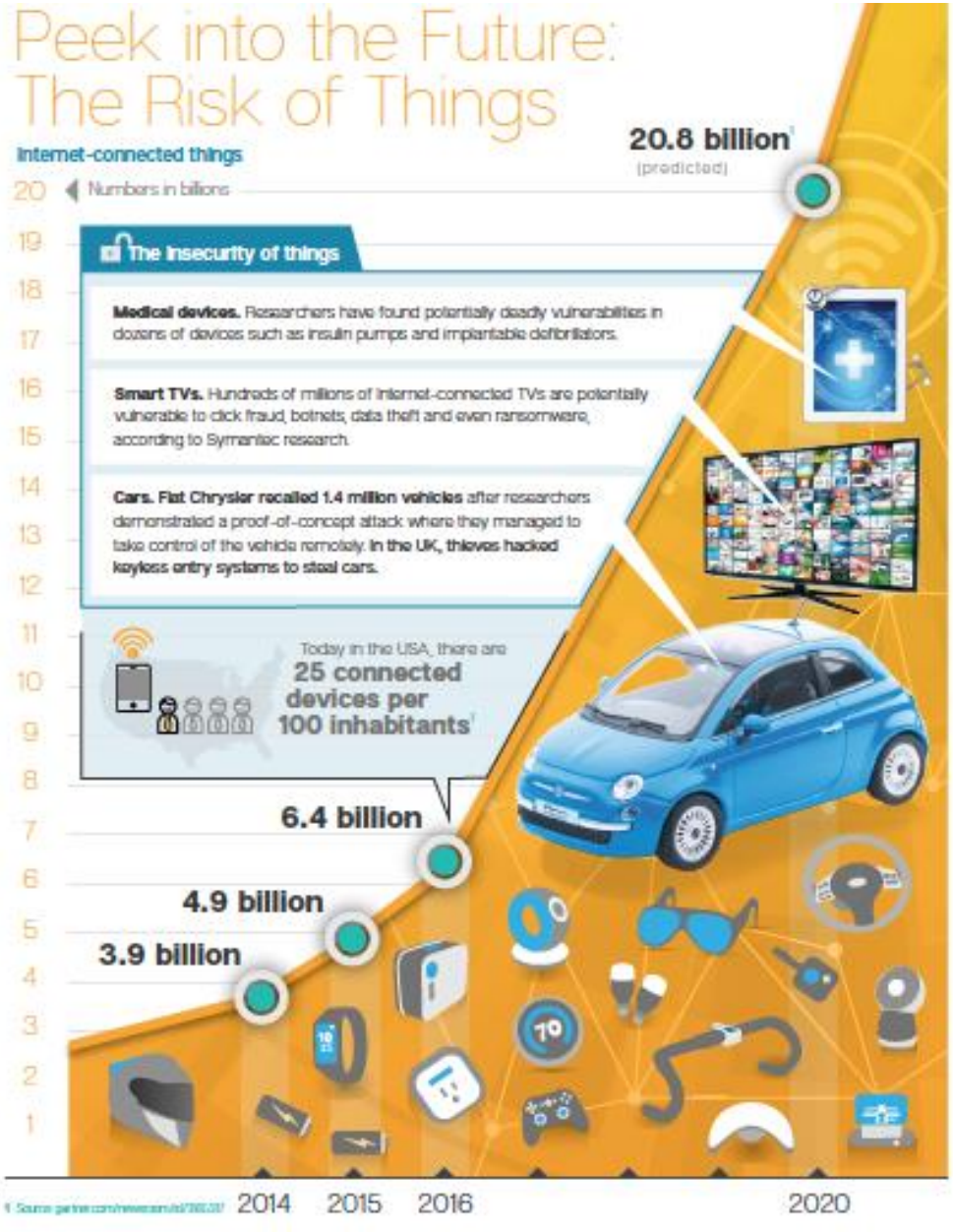
Senior Director, Government Affairs EMEA & APJ

Does ePrivacy still serve a public policy objective?

Information security is about protecting….

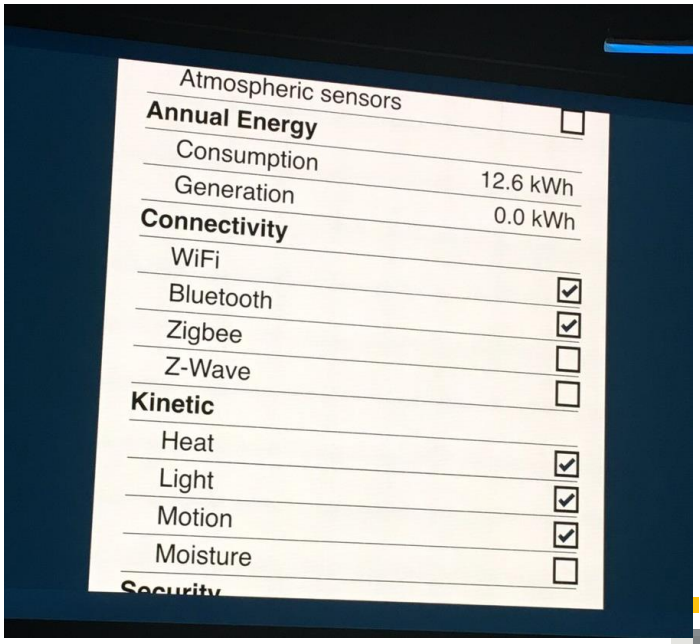
- Information/Data = GDPR
- Infrastructure = NIS
- Identities= eIDAS
- Interactions= ??
- If ePrivacy is focused on protecting **interactions= confidentiality** it has a role to play in the security architecture
- To be effective however it needs to target appropriately and to be consistent with other instruments

Is IoT/M2M security necessary? Absolutely!!!



Security and transparency are essential features of product quality…..

- ePrivacy covers M2H
- ePrivacy labeling, certification and AIOTI



Browsers, cookies and managing privacy settings (*article 10)*

- Cookies provision proved ineffective
- Nothing wrong with being able to manage privacy settings via tools
- Do not create a browser only “gateway” to privacy settings – encourages oligopolies and monocultures
- Besides we access more and more the internet without relying on browsers
- The notion of 1st party and 3rd party content is problematic – Everything that comes from the browser is 1st party, therefore by definition good?

What should you improve in ePrivacy?

Cybersecurity processing of data (*article 6)*

- Categories of data processed for security purposes:
  - Personal data (e.g. IP address of infected PC/device)
  - Metadata (e.g Network infrastructure of botnet C&C server)
  - Content (e.g. URLs contained in a phishing email that infected the device)
- Not possible to protect effectively without access to all these categories
- Under GDPR there is a legal basis to process **personal data** for security for: controllers, processors, telecoms, security providers, CERTs
- Under ePrivacy access to **content data and metadata** is restricted for security purposes only to OTTs and Telecoms
- The **perverse effect** of ePrivacy is that everyone has an incentive to be more privacy intrusive (collect personal data) because only OTTs and Telecoms are allowed to collect metadata and content data
- **Less protection** because fewer organisations can collect security relevant info (security providers and CERTs are not included)
- Major problem in M2M communications when there is **no personal data involved** (e.g. factory environment) – so the GDPR rules cannot apply
- **ePrivacy should align here with GDPR as did ePrivacy (2009 version)**

Access to data for security purposes - comparison

ePrivacy 2009 Directive – (Recital 53 2009/136/EC)	**GDPR** (Recital 49 & Article 6par1F)	**New ePrivacy Regulation** (Articles 4& 6)
The processing of **traffic data** to the extent strictly necessary **for the purposes of ensuring network and information security**, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data, and the security of the related services offered by, or accessible via, these networks and systems**, by providers of security technologies and services when acting as data controllers is subject to Article 7(f) of Directive 95/46/EC**. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems. ***Achieves better security***	The processing of **personal data** to the extent strictly necessary and proportionate **for the purposes of ensuring network and information security**, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and the security of the related services offered by, or accessible via, those networks and systems, **by public authorities, by computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), by providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the data controller concerned.** This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems. ***Achieves better security***	***Article 4*** 'electronic communications data' means **electronic communications content and electronic communications metadata**; ***Article 6*** *Permitted processing of electronic communications data* **Providers of electronic communications networks and services** may process **electronic communications data** if: (b) **it is necessary to maintain or restore the security of electronic communications networks and services**, or detect technical faults and/or errors in the transmission of electronic communications, for the duration necessary for that purpose ***Weakens security***

Could the security provisions be improved? (*article 5)*

- Yes
- Focus needs to be on capabilities to be achieved to deliver security as opposed to a generic obligation to deliver a “confidential” environment
- **Security requires also access remotely to the endpoint to allow effective protection** (*article 8)*
  - Your smart-meter or home router upgrades happen remotely not because the user has decided it is time to update the firmware
- Is Article 17 (notification or risk of breach) needed?
  - Probably not

Other important considerations

Who has access to the data and for what purpose?

(Articles 6, 7 and 9)

- **<u>This is not a security relevant consideration but important to bear in mind</u>**
- GDPR justifies personal data processing for a number of purposes
- ePrivacy limits this to consent for all meta-data that may or may not be personal (e.g. may not justify GDPR level of protection)
- The more restrictive the framework is for metadata the less likely is for EU businesses to grow in new/big data sectors
- Less growth= less jobs, less innovation, less competitiveness
- Decision for the policy makers but need to be clear on its impact

Law enforcement access *(Article 11)*

- ePrivacy continues the tradition of its predecessors (1997, 2002, 2009) in foreseeing a law enforcement access exemption
- Correct decision given the circumstances in Europe
- Multiple ECJ judgments defining the conditions for surveillance
- What happens when the exemption is used is left to the Member States
- Parallel discussions/calls for data retention, e-evidence, access to encrypted traffic
- Need for harmonized approach for doing business in Europe

Thank you!

Ilias_chantzos@symantec.com