



Personal data protection – Specific cases I

Smart everything

MVV1368K Privacy and Personal Data
František Kasl

Structure of the seminar

- **1) Essays**
 - Basic info + readings
- **2) Topics**
 - Smart home, still my home?
 - Smart city for proper citizens only?
 - Privacy by design in smart environments
- **3) Slides**
 - Title – Question – Discussion - Information

Essays - Topics

- **Essay Deadline: 18 December, 8:00 AM**
- approx. 10 500 - 16 000 characters long (+ footnotes) = 5-8 pages
- **For further essay requirements see interactive syllabus**
- **Presentation day** (only students with **Presentation No. 3**): 19 December

- Smart home, still my home?: How ubiquitous sensory data collection sneaks upon spatial privacy
- Smart industry, customized surveillance?: How do personalized products and individualized production process personal data?
- Privacy by design and other instruments of the current European legal framework for personal data protection in smart environments

Obligatory readings

- **These readings are the prerequisite for the understanding of the concept of the internet of things and its potential impact on privacy and data protection.**
 - WEBER, Rolf H. Cybersecurity in the Internet of Things: Legal aspects. *Computer Law & Security Review*. 2016, Vol. 2016, No. 32. Available (through university computers) at: <https://www.sciencedirect.com/science/article/pii/S0267364916301169>
 - COMMISSION STAFF WORKING DOCUMENT. *Advancing the Internet of Things in Europe*. SWD/2016/0110 final. 2016. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016SC0110>
 - JOHNSON, Graham. Privacy and the Internet of Things: Why Changing Expectations Demand Heightened Standards. *Washington University Jurisprudence Review*. 2018, 11. **Available through university computers) at Heinonline.org**

Voluntary readings

- **These readings provide additional insight into the challenges related to the various smart environments.**
 - SUN, Wencheng et al. Security and Privacy in the Medical Internet of Things: A Review. Security and Communication Networks. 2018 Available at: <https://www.hindawi.com/journals/scn/2018/5978636/abs/>
 - MINERVA, Roberto; BIRU, Abyi; ROTONDI, Domenico. *Towards a definition of the Internet of Things (IoT)*. IEEE. 2015. Available at: https://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf
 - EDWARDS, Lilian. Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective. *European Data Protection Law Review*. 2016, Vol. 2, No. 1. **Available through university computers) at Heinonline.org**
 - KASL, František. Cybersecurity of Small and Medium Enterprises in the Era of Internet of Things. *The Lawyer Quarterly*, Praha: Institute of State and Law of the Academy of Sciences of the Czech Republic, 2018, Vol. 8, No. 2, pp. 165-188. Available at: <https://tlq.ilaw.cas.cz/index.php/tlq/article/view/281/260>
 - SCHNEIER, Bruce. The Internet of Things That Talk About You Behind Your Back. Motherboard. 2016. Available at: https://www.schneier.com/essays/archives/2016/01/the_internet_of_thin_1.html

Additional readings

- **These readings provide broader context and up-to-date examples of situations, where privacy and personal data protection are being challenged by smart environments.**
 - DABBAGH, Mehjar; RAYES, Ammar. Internet of Things Security and Privacy. In: RAYES, Ammar; SALAM, Samer (eds.) . Internet of Things From Hype to Reality: The Road to Digitization. Springer International Publishing, 2019, 211–238. ISBN 978-3-319-99516-8.
 - SCHNEIER, Bruce. Click Here to Kill Everybody: Security and Survival in a Hyper-connected World. W. W. Norton & Company. 2018, 978-0393608885, 288 p.
 - BENEDIKT, Olesya. The Valuable Citizens of Smart Cities: The Case of Songdo City. *Graduate Journal of Social Science*. 2016, Vol. 12, No. 2. Available at: http://giss.org/sites/default/files/issues/chapters/papers/GJSS%20Vol%2012-2%201%20Benedikt_0.pdf
 - COSTA, Luiz. *Virtuality and Capabilities in a World of Ambient Intelligence: New Challenges to Privacy and Data Protection*. Law, Governance and Technology Series, Vol. 32, Springer International Publishing Switzerland, 2016, ISBN: 978-3-319-39197-7, 199 p. Available in the university library.



Smart home, still my home?

Super quick recap:

By this point in the course, you should know...

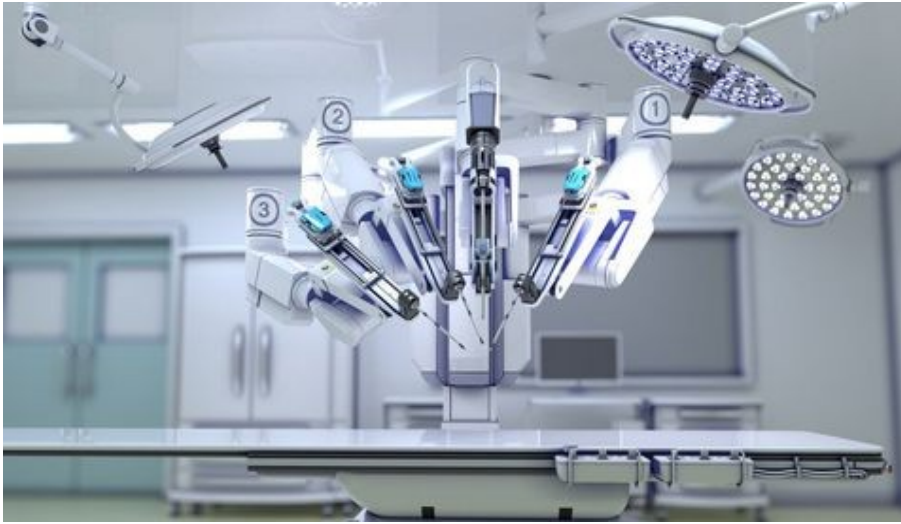
- What is privacy and why does it matter?
- What are personal data?
- What is surveillance?
- How do these concepts collide?
- What does technology bring to this mix?

Future is now

What is Internet of things?

- **Small environment with low complexity** scenario
 - network that connects uniquely identifiable things to the Internet
 - these things can sense and collect / perform activity based on program/profile
- **Large environment with high complexity** scenario
 - self-configuring, adaptive, complex network that interconnects things to the Internet
 - the things get unique „virtual identities“ and „profiles“
 - part of the environment = **ambient**
 - provide services tailored to the user = **personalized**
 - adapt and learn from available data = **intelligent**
 - available anywhere, anytime, and for anything = **ubiquitous**
- Examples
 - Interesting / Curious / Practical / Crazy / Scary / Weird / Unthinkable





Hidrate Spark 2.0 SMART WATER BOTTLE

Tracks water

Glow to remind

Syncs with Fitbit, Apple Watch,
MyFitnessPal, + more



Egg Minder THE SMART EGG TRAY

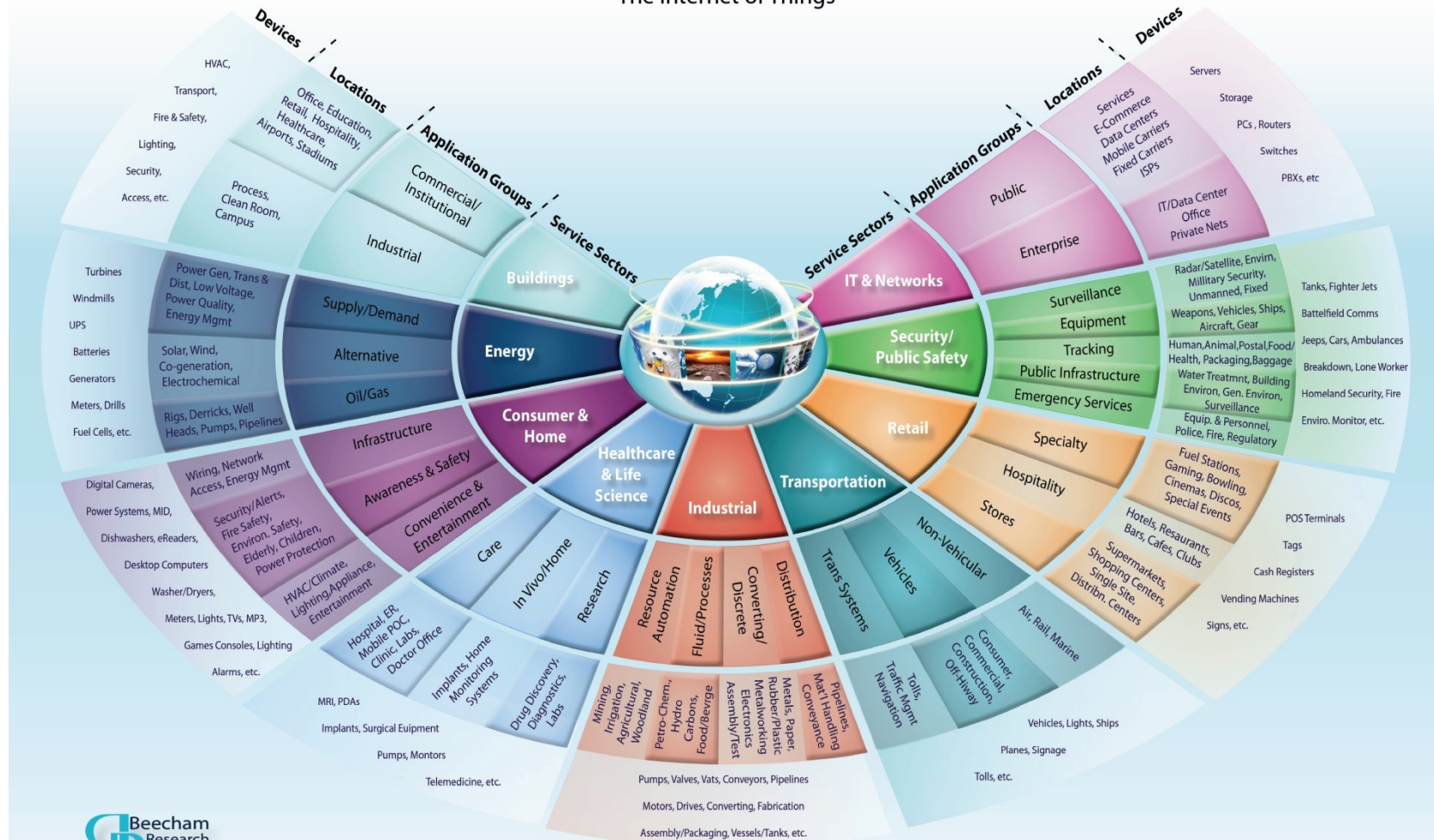


The world's first smart,
connected carry-on.



M2M World of Connected Services

The Internet of Things



Boston | London

info@beechamresearch.com

+44 (0)845 533 1758

www.beechamresearch.com

© 2009 Beecham Research Ltd.

Smart home

What should your house know about you?

- **Smart home**
 - IoT embedded in home environment
 - **optimisation, customisation, innovation**
 - new features for the user = **convenience**
 - new data for the provider = **profiling**
- **Limits of data collection**
 - protection of spatial privacy X consent?
 - protection of personal data X performance of contract?
 - human intimacy / special categories of personal data
 - legal X moral X philosophical X practical perspective

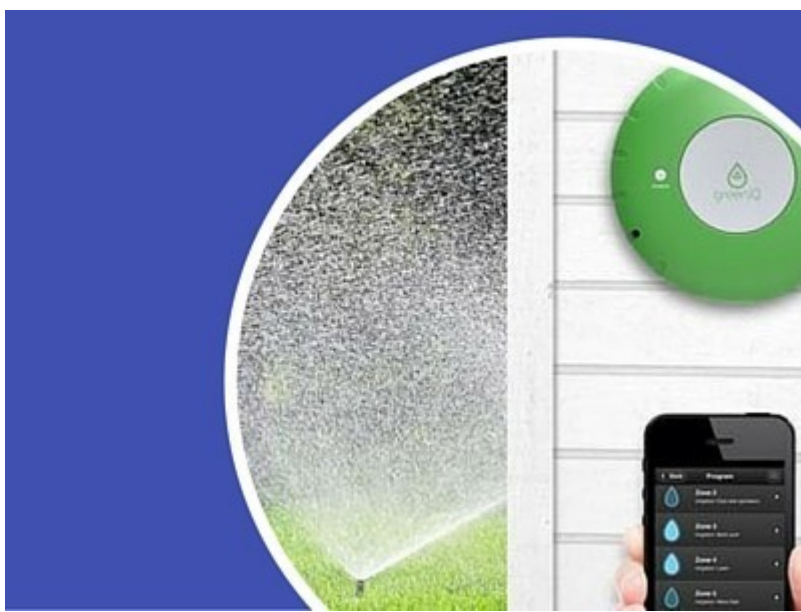


Smart Door Locks
Smart Home Retrofit



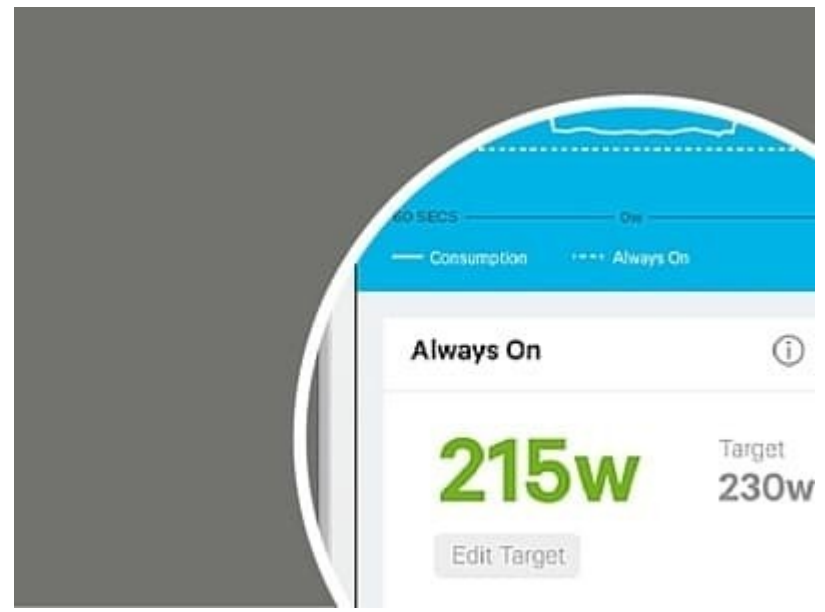
Smart Bluetooth Trackers
Smart Kitchen





Smart Irrigation Controllers

Wifi Lighting



Wireless Home Energy Monitors

IoT Cloud Platforms



Specific challenges brought by IoT environment

Is „smart“ always smart?

- Features: ubiquitous profiling, big data mining, machine learning, M2M communication, possible omnipresence, mesh connectivity...
- **Challenges**
- **A) higher likelihood, frequency and severity of cyber incidents**
 - increased data flow complexity
 - ‘weaponized IoT devices’ for DDoS attacks or other illicit activities
 - increased attack surface - variety creates in combination new vulnerabilities
 - limited security features and possibilities for advanced security countermeasures
- **B) new forms of data breaches, increased frequency, severity and volume**
 - data collected - omnipresence of IoT sensors => increased detail of all aspects of documented activities
 - new forms of data, metadata and derived data (by combination of the collected data)



ORWELL

Smart city for proper citizens
only?

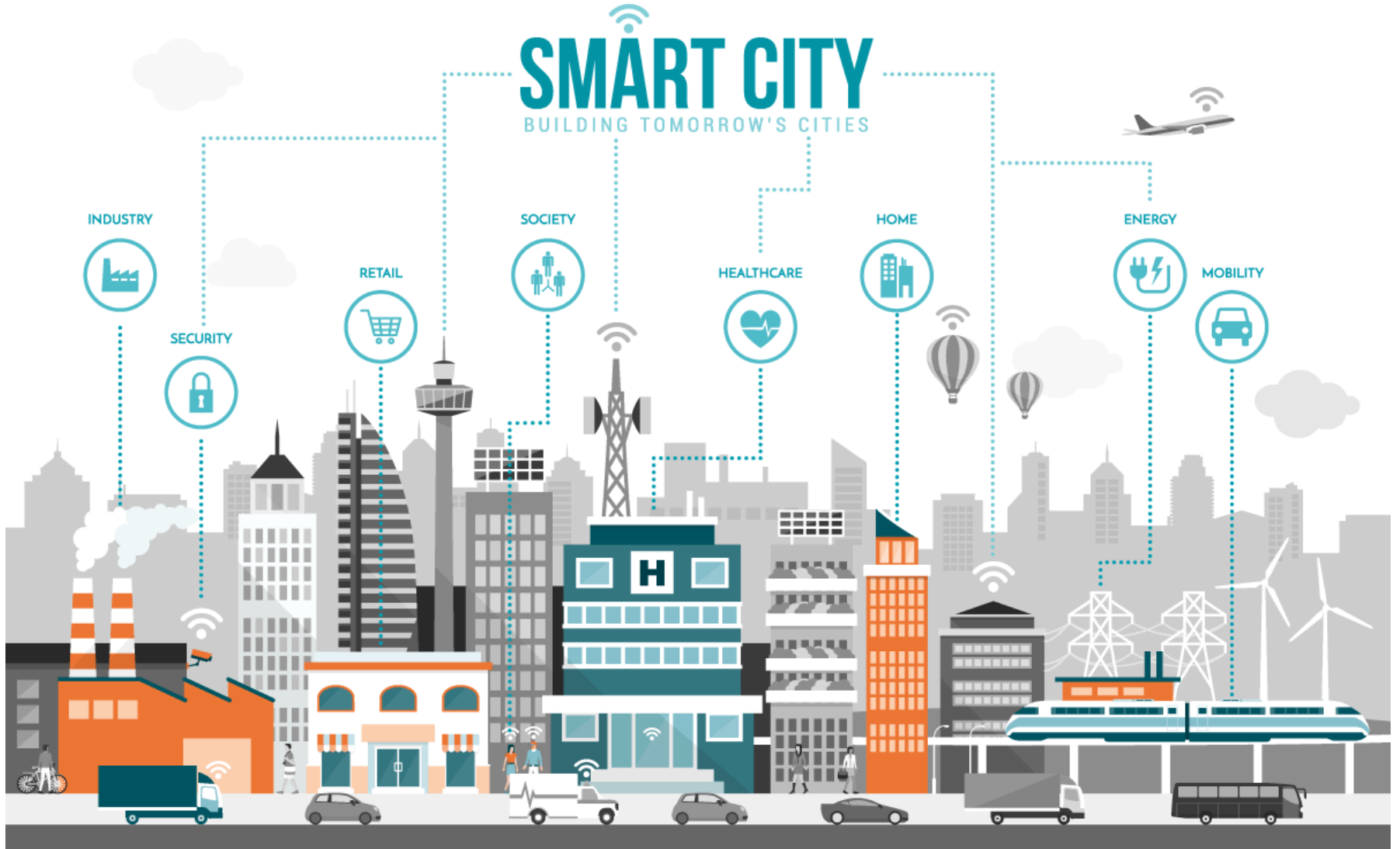
Smart city

What changes and challenges can we expect?

- synergy between Internet of Things, Big Data and Cloud
 - model of connected urban environment
 - => advanced sustainability
 - => improved resilience
 - => better urban living
- technology X social X political X economic factors
 - A) implementation of ICT solutions
 - B) multi-stakeholder socio-economic transformations of the urban ecosystem

SMART CITY

BUILDING TOMORROW'S CITIES



Road to a smart city

How does city become „smart“?

- A) **built fully anew** with integrated smart architecture
 - [Songdo](#) – Seoul – South Korea
 - [Makkah project](#) – Saudi Arabia
 - [Masdar City](#) – United Arab Emirates
- B) **transformation of existing neighbourhoods** by a series of projects incorporating smart modules
 - [Smart Cities Mission](#) – India – 100 cities
 - [London](#)
 - [Barcelona](#)
 - [New York City](#)

Every step you take

How to provide guarantees of privacy?

- smart street surveillance
 - X facial recognition + AI + state control ([..China..](#))
- smart traffic
 - optimisation + traffic jams X tracking + database
- smart devices for wifi access
 - X security / data traffic surveillance
- future hidden dangers?
 - [social credit system](#) – ranking of the citizens



Privacy by design in smart environments

EU legal toolbox for privacy

Nominal right X practical enforcement?

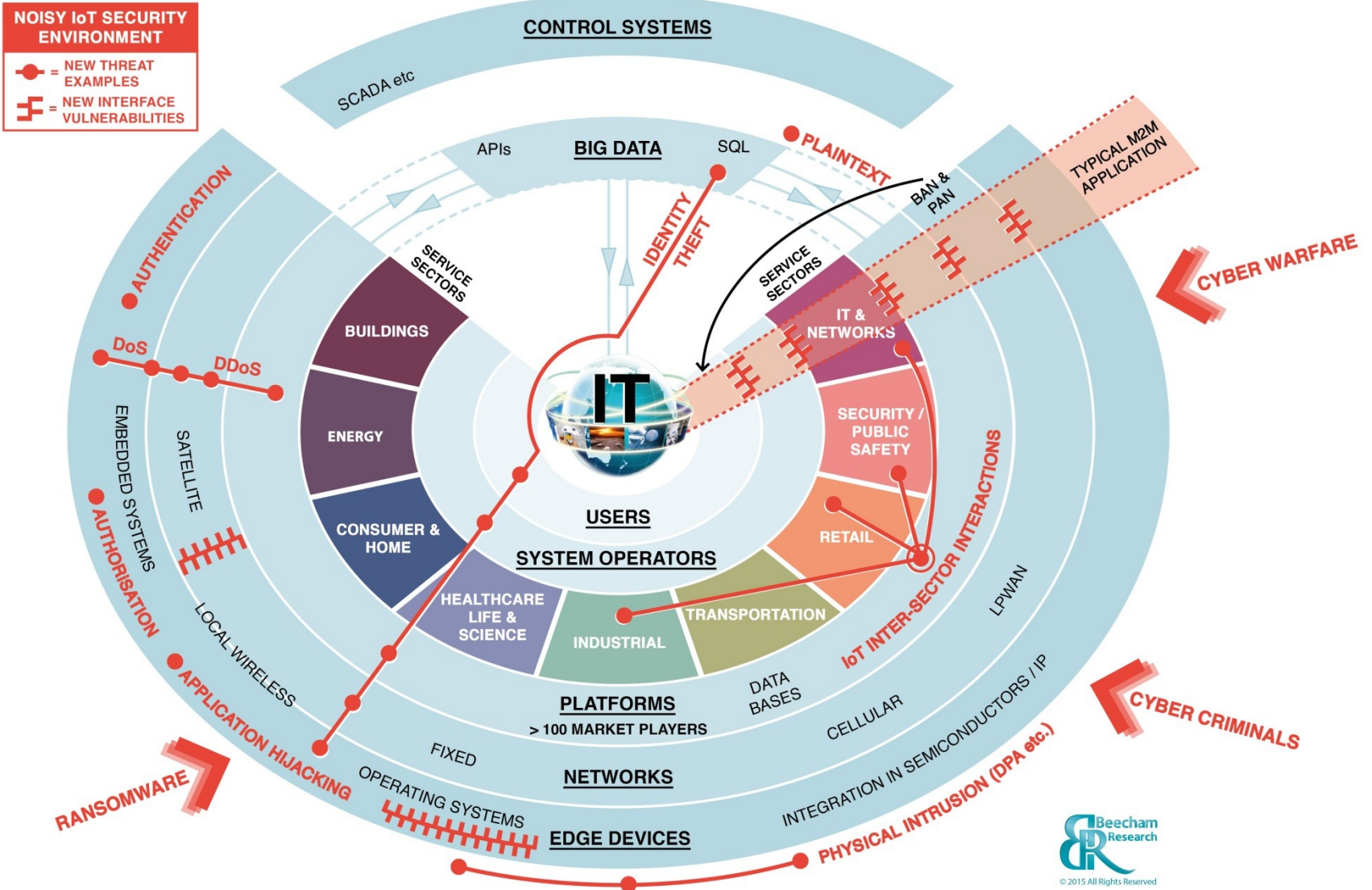
- **GDPR**
 - accountability + rights of the data subject + principles
 - data protection by design / by default
 - data breach notification obligation
- **ePrivacy directive / regulation**
 - new players – traditional telecom x new telecom (message apps)
 - communication content / metadata / cookies
- **Public procurement**
 - price X quality => security / data protection / integrity / data control
- **Cybersecurity**
 - critical infrastructure / CSIRT (Cyber Security Response Team)
- **Product standards and market access control**
 - CE marking / [product safety rules](#) / [IoT standards and protocols](#)
 - [Liability for emerging digital technologies](#)

Risk assessment in IoT data processing

New environment = new frame of mind?

- **new factors**
 - cyberphysical; indirect interconnection...
 - increased frequency, scope, variety
- **challenges for unified or comprehensive classification of risk**
 - ambiguous terms and fluctuant environment
 - risk-based approach missing adequate guidance in measures and indicators => need for flexible adaptation to IoT
- **need for**
 - automated reporting and monitoring
 - adjustment of risk scales
 - broad adoption of adequate methodology

IoT Security Threat Map





Thank you for your attention!

Questions?

Ideas?

Answers?

Looking forward to your essays!