



The European watch
on cybersecurity & privacy

The LSPs Programme: privacy and security in IoT

Dr. Pasquale Annicchino, Archimede Solutions SARL



CREATE-IoT

Funded by the European Commission
Horizon 2020 – Grant # 740129



The LSPs programme

- ◆ *Introduction to the LSPs programme*
- ◆ *The relevance of privacy and security*
- ◆ *Guidelines*
- ◆ *IoT challenges*

- ◆ *Q&A will follow*

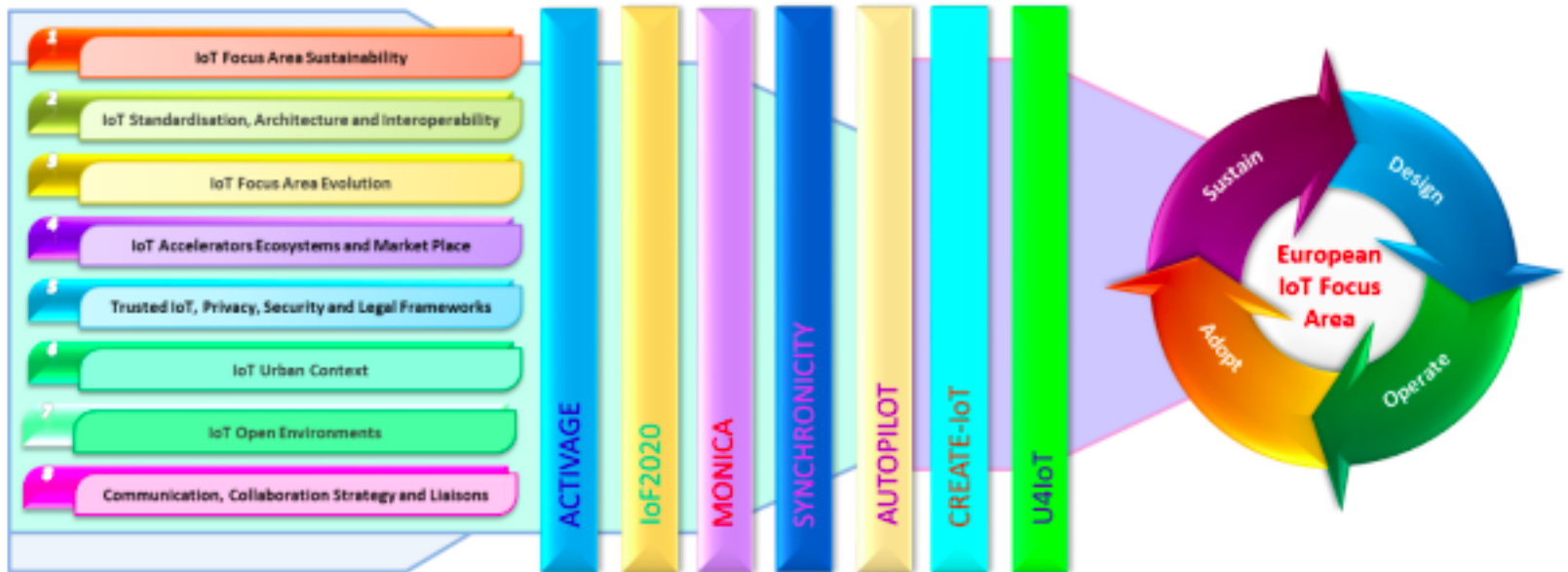
The LSPs programme

The IoT European LSP Projects

- ✓ Reference Zones in Cities
- ✓ Smart Living Environments for Aging Well
- ✓ Wearables for Smart Ecosystems
- ✓ Smart Farming and Food Security
- ✓ Autonomous Vehicles in a Connected Environment

The IoT European Large-Scale Pilots Programme includes the innovation consortia that are collaborating to foster the deployment of Internet of Things (IoT) solutions in Europe through integration of advanced IoT technologies across the value chain, demonstration of multiple IoT applications at scale and in a usage context, and as close as possible to operational conditions.

The LSPs programme



The relevance of privacy and security



Guidelines

IoT Legal Framework

LSPs Good Practices

Table of contents

1. Executive summary	4
2. Introduction	5
2.1 Purpose and target group	5
2.2 Contributions of partners	8
2.3 Relations to other activities in the project	9
3. Data control: An issue of horizontal relevance	11
3.1 Setting the scene	11
3.2 The regulatory challenges	12
3.3 Bridging the gaps	12
4. Data processing and Data protection	14
4.1 Informed consent requirements	14
4.2 Accountability measures: technical and organizational	15
4.3 Processing of special categories of data	16
5. Cybersecurity and resilience	17
5.1 The rationale of the Directive	17
5.2 Scope and definitions	17
5.3 The security and incident notification requirements	19
6. Consumers' safety	22
6.1 Outdated definitions of Product, Defect and Damage	22
6.2 The principle of strict liability	24
6.3 Paving the way forward	25
7. Customer data	27
7.1 The rationale of the Directive	27
7.2 Third party payment services	27
7.3 Strong customer authentication	30
8. Trade secrets	32
8.1 Trade secrets	32
8.2 Remedies	34
9. Upcoming regulation	35
9.1 The proposed Regulation on the free flow of data	35
9.2 The proposed Cybersecurity Act	36
9.3 The proposed ePrivacy Regulation	37
10. Conclusions	38
11. References	40

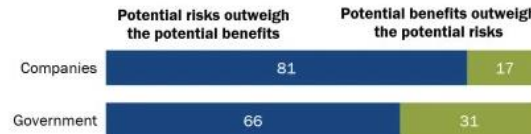
IoT Challenges

FBI recommends that you keep your IoT devices on a separate network

The FBI also recommends changing factory-set (default) passwords and not allowing an IoT device's accompanying mobile app to gain access to too many smartphone permissions.

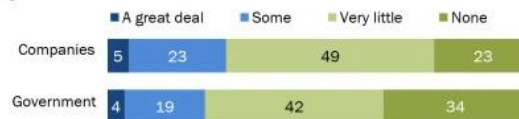
Majority of Americans think the potential risks of data collection outweigh the benefits

% of U.S. adults who say the ___ when it comes to data collection by ...



... and relatively few Americans say they personally benefit from the data that companies or the government collects about them

% of U.S. adults who say they benefit ___ from the data collected about them by ...



Note: Respondents were randomly assigned to answer a question about how much they feel they benefit from the data collected about them by "companies" or "the government." Respondents were also randomly assigned to answer a question about whether the potential risks outweigh the potential benefits of data collection, or vice versa, by "companies" or "the government." Those who did not give an answer are not shown. Source: Survey conducted June 3-17, 2019. "Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information"

Conclusion

- ◆ *Horizontal and vertical challenges*
- ◆ *Take data protection seriously: legal and financial risks;*
- ◆ *Continuous improvement process;*
- ◆ *Educate!*
- ◆ *Anticipate evolution and end-users' perceptions*