



Opportunity Report

“Towards Enhanced EU-US ICT Pre-competitive Collaboration”

Policy

Jonathan Cave,
Maarten Botterman

Department of Economics
The University of Warwick, UK

GNKS, IGF DC IoT, NLnet

With support by:

Steffen Watzek, Yaning Zou
Lucas Scheuvers, Gerhard Fettweis

Mobile Communications Systems
Faculty of Electrical and Computer Engineering
TU Dresden University, Germany

Vasilis Papanikolaou,
Nikos Sarris

iLAB
ATC SA, Greece

Christian Sonntag,
Sebastian Engell

Process Dynamics and Operations Group
Dept. of Biochemical and Chemical Engineering
TU Dortmund University, Germany

Revised version V1.1

Please send any feedback to: j.a.k.cave@warwick.ac.uk

ICT Policy, Research and Innovation
for a Smart Society

May 2018

www.picasso-project.eu



Executive Summary

Policy interacts with R&I, and the three PICASSO policy domains, in two main ways: policies that are intended to advance or support R&I; and R&I activities that lead to new policies or are enabling new ways to achieve policy objectives.

This report outlines specific policy challenges for collaboration between US and EU researchers. We found that there is very fertile ground for collaboration, and it will be important to develop this further to overcome the artificial barriers created by different use of terms (e.g. 5G according to 3GPPP in Europe and “Advanced Wireless” in USA) and to harness the associated productive differences in perspective. The same applies to the ‘natural experiment’ created by different legislative approaches (e.g. privacy as fundamental right, or as economic right that is tradable) and instantiations of community-related concepts.

We found that the differences between US and European values, approaches and available evidence are relevant and provide an opportunity to jointly develop ICT that may serve the global market and to transfer useful aspects of digital community formation between the US and the EU. ICT is associated with a range of global industry sectors and entities; the many layers in the value chain from the chip to national and global ICT services – and beyond into the application and regulatory layers - require innovation on the fundamental technical level, the level of innovative services and the organizational and business model levels as well.

By grounding policies in a solid understanding of acting in a global market, more opportunities will arise for collaboration amongst EU and US researchers.

The PICASSO Project

The aim of the 30-months PICASSO project is (1) to reinforce EU-US collaboration in ICT research and innovation focusing on the pre-competitive research in key enabling technologies related to societal challenges - 5G Networks, Big Data, Internet of Things and Cyber Physical Systems, and (2) to support the EU-US ICT policy dialogue by contributions related to e.g. privacy, security, internet governance, interoperability, ethics.

PICASSO is oriented to industrial needs, provides a forum for ICT communities and involves 24 EU and US prominent specialists in the three technology-oriented ICT Expert Groups - [5G](#), [Big Data](#), and [IoT/CPS](#) - and an ICT Policy Expert Group, working closely together to identify policy gaps in the technology domains and to take measures to stimulate the policy dialogue in these areas. A synergy between experts in ICT policies and in ICT technologies is a unique feature of PICASSO.

A number of analyses will be accomplished, as well as related publications, that will for a major part be made public and contribute to the project's outreach. Dedicated communication and dissemination material will be prepared that should support the operational work and widespread dissemination through different channels (website, social media, publications ...). The outreach campaign will also include 30+ events, success stories, factsheets, info sessions, and webinars.

PICASSO Project Coordination:

Svetlana Klessova, Project Coordinator

inno TSD, France

+33 4 92 38 84 26

s.klessova@inno-group.com



About the PICASSO Project:

PICASSO is co-funded by the European Commission under the Horizon 2020 programme.

Start Date: 1st January 2016







Duration: 30 months

Total budget: 1,160,031 €, including a contribution from the European Commission of 999,719 €

Project Website: <http://www.picasso-project.eu/>

PICASSO Consortium Members:

The logo for inno TSD, featuring a stylized 'i' and 'nno' with a blue triangle above the 'nno'.	inno TSD, France – one of Europe's leading innovation management consultancy firms, specialised in helping major private and public stakeholders design and implement R&D and innovation projects. https://www.inno-tds.fr/en
The logo for Technische Universität Dortmund, featuring the letters 'tu' in green and 'technische universität dortmund' in black.	TECHNISCHE UNIVERSITÄT DORTMUND, Germany – a leading German technically oriented research university with strong research groups in big data, communications, smart grids, e-mobility and cyber-physical systems. http://www.tu-dortmund.de
The logo for THINK Wireless Technologies Limited, featuring the word 'THINK' in blue and 'WIRELESS TECHNOLOGIES LTD' in smaller blue letters below it.	THINK WIRELESS TECHNOLOGIES LIMITED, United Kingdom - an ICT company founded in 2009 after more than a decade of research and development in wireless and energy harvesting technologies. http://www.think.com/
The logo for ATC Athens Technology Center, featuring the letters 'ATC' in blue and 'ATHENS TECHNOLOGY CENTER' in smaller blue letters below it.	ATC SA, Greece - an SME and Technology Centre in the field of ICT participating in 3 ICT European Technology Platforms: NESSI (Steering Committee member), NEM (member) and NETWORLD2020 (member), and founding member of European Big Data Value Association. http://www.atc.gr

	<p>AGENZIA PER LA PROMOZIONE DELLA RICERCA EUROPEA, Italy – a non-profit research organisation, grouping together more than 100 members, including public and private research centres, industries, industrial associations, chambers of commerce, science parks and more than 50 universities, with the main objective to promote the participation in national and European RTD programmes. http://www.apre.it/</p>
	<p>HONEYWELL INTERNATIONAL INC, United States – a multinational company and global leader that invents and manufactures technologies to address some of the world's toughest challenges initiated by revolutionary macrorends in science, technology and society. The company's products and solutions are focused on energy and the environment, safety and security, and efficiency and productivity. http://honeywell.com/</p>
	<p>GNKS CONSULT BV, Netherlands - conducting strategic and policy research and evaluation, building on excellence in understanding of the impact of the emerging Global Networked Knowledge Society http://www.gnksconsult.com/</p>
	<p>TECHNISCHE UNIVERSITÄT DRESDEN, Germany - a full-scale university with 14 faculties, covering a wide range of fields in science and engineering, humanities, social sciences and medicine. https://tu-dresden.de/</p>
	<p>FLORIDA INTERNATIONAL UNIVERSITY, United States - The Miami-Florida Jean Monnet Center of Excellence, (MFJMC), a member of the global network of EU-sponsored Jean Monnet centers, has the mission to promote teaching, research and outreach activities relating to the EU. http://www.fiu.edu/; https://miamieuc.fiu.edu/</p>
	<p>UNIVERSITY OF MINNESOTA, United States – The Technological Leadership Institute bridges the gap between business and engineering. TLI's mission is to develop local and global leaders for technology enterprises. https://tli.umn.edu/</p>

List of Figures

<i>Figure 1: Horizon 2020 ICT-related priority areas.</i>	<i>23</i>
<i>Figure 2: Policy-related working groups of the 5G Infrastructure Association.....</i>	<i>25</i>

List of Tables

<i>Table 1: Summary of policy collaboration opportunity topics and areas.</i>	<i>12</i>
--	-----------

List of Acronyms

3GPP	3rd Generation Partnership Program
4G	4 th Generation
5G	5 th Generation
AI	Artificial Intelligence
AIOTI	Alliance of IoT Innovation
AV	Autonomous Vehicle
AWS	Amazon Web Services
B2B	Business-to-business
B2C	Business-to-customer
BBi	Bio-based Industries
BD	Big Data
BDVA	Big Data Value Association
BDVPPP	Big Data Value Public Private Partnership
CEDR	Conference of European Directors of Roads
CERN	Conseil Européen pour la Recherche Nucléaire
CPS	Cyber-physical System
CPSoS	Cyber-physical System of Systems
CPS-VO	CPS Virtual Organization
CPU	Central Processing Unit
CS	Clean Sky
CSAAC	Cyber Situational Awareness Analytical Capabilities
D2D	Device-to-Device
DARPA	Defense Advanced Research Projects Agency
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DoC	Department of Commerce
DoD	Department of Defense
DoDIN	DoD Information Networks
DoE	Department of Energy
DoS	Department of State
DoT	Department of Transportation
DSL	Digital Subscriber Line
DSM	Digital Single Market
EC	European Commission
ECSEL	Electronic Components and Systems for European Leadership
EeB	Energy-efficient Buildings
EG	Expert Group
EPI	European Platform Initiative
ERA	European Research Area
EU	European Union
FBMC	Filter-Bank Multi-Carrier
FCC	Federal Communications Commission
FCH	Fuel Cells and Hydrogen
FET	Future and Emerging Technologies
FIRE	Future Internet Research & Experimentation
FoF	Factories of the Future
FP7	Framework Programme 7

FY	Financial Year
Gbps	Gigabit per second
GDP	Gross Domestic Product
GDPR	General Data Protection Regulation
GENI	Global Environment for Networking Innovations
GFDM	Generalized Frequency-Division Multiplexing
GHz	Gigahertz
H2020	Horizon 2020
H2M	Human-to-machine
HD	High-definition
HMI	Human Machine Interface
HPC	High Performance Computing
HPUE	High Performance User Equipment
IA	Industry Association
ICT	Information and Communication Technology
IEEE	Institute of Electrical and Electronics Engineers
IERC	IoT European Research Cluster
IIC	Industrial Internet Consortium
IIoT	Industrial Internet of Things
IM	Innovative Medicine
IMS	Intelligent Manufacturing Systems
INCOSE	International Council on Systems Engineering
IoT	Internet of Things
IP	Intellectual Property
IPR	Intellectual Property Rights
ISM	Industrial, Scientific, Medical
ITER	International Thermonuclear Experimental Reactor
ITS	Intelligent Traffic System
ITU	International Telecommunication Union
JTI	Joint Technology Initiative
JU	Joint Undertaking
LTE	Long Term Evolution
M2M	Machine-to-Machine
M&S	Modeling and Simulation
MEC	Mobile Edge Computing
MHz	Megahertz
MIMO	Multiple Input Multiple Output
MoU	Memorandum of Understanding
ms	Millisecond
NACFAM	National Coalition for Advanced Manufacturing
NB-IoT	Narrowband IoT
NCP	National Contact Point
NCURA	National Council of University Research Administrators
NFV	Network Function Virtualization
NGI	Next Generation Internet
NGMN	Next Generation Mobile Networks
NIH	National Institutes of Health
NIPRNet	Nonsecure Internet Protocol Router Network
NISD	Network and Information Security Directive

NIST	National Institute of Standards and Technology
NIT	Networking and Information Technology
NITRD	Networking and Information Technology Research and Development
NSF	National Science Foundation
NTIA	National Telecommunications and Information Administration
OCF	Open Connectivity Foundation
OFDM	Orthogonal Frequency Division Multiplexing
OMG	Object Management Group
PAWR	Platforms for Advanced Wireless Research
PCAST	President's Council of Advisors on Science and Technology
PPP	Public Private Partnership
PWG	Public Working Group
QoE	Quality of Experience
R&D	Research and Development
R&I	Research and Innovation
RAT	Radio Access Technology
RDI	Research, Development, Innovation
RFC	Request for Comments
SAE	Society of Automotive Engineers
SDAV	Scalable Data Management, Analysis and Visualization
SDN	Software Defined Networking
SEED	Standard Energy Efficiency Data
SIPRNet	Secret Internet Protocol Router Network
SME	Small and Medium-sized Enterprises
SMLC	Smart Manufacturing Leadership Coalition
SoS	System of Systems
SOTA	State of the Art
SPIRE	Sustainable Process Industry
SRA	Strategic Research Agenda
SSG	Senior Steering Group
Tbit	Terabit
Tbps	Terabit per Second
TRL	Technology Readiness Level
TTIP	Transatlantic Trade and Investment Partnership
TV	Television
UE	User Equipment
UHD	Ultra High Definition
URLLC	Ultra-reliable Low-latency Communications
US	United States
USGS	US Geological Survey
V2I	Vehicle-to-infrastructure
V2V	Vehicle-to-vehicle
V2X	Vehicle-to-everything
V5GTF	Verizon 5G Technology Forum
VDA	Verband Der Automobilindustrie
VPN	Virtual Private Network
ZT-OFDM	Zero-tail OFDM

Table of Contents

1. Introduction	10
2. Overview.....	12
2.1. A Summary of Challenges and Opportunities	12
2.2. Approaches to ICT Policy Issues in the EU and the US: Some Similarities and Differences	20
2.2.1. A Bit of History	20
2.2.2. The Difficulty of Meaningful Comparisons	20
2.3. Differences and Co-operation	21
3. Policy Priorities in the EU and the US.....	22
3.1. EU Priorities	22
3.1.1. Overarching Research Programme – Horizon 2020	22
3.1.2. Innovation Policy – IoT/CPS.....	25
3.2. US Priorities	26
3.3. Research-driven Policy in Two Technology Areas	26
3.3.1. Schema	26
3.3.2. EU Policy in the 5G Domain.....	27
3.3.3. EU Policy on the Internet of Things/CPS	28
4. Barriers to Policy-driven R&I Collaboration.....	30
5. Conclusions and Outlook	32
6. References	33

1. Introduction

This report concentrates on policy collaboration to support further ICT R&I collaboration between EU and US researchers on issues identified to be of common interest, specifically related to 5G networks (for US: Advanced Wireless Communications); Big Data: and Internet of Things (specifically: Cyber Physical Systems). The lessons learned feed back to these specific communities through our respective PICASSO expert groups, and in addition, the insights arising are shared across the Internet Governance communities where multiple stakeholders meet, including government officials, industry, users and researchers. As described in this report, policy interacts with R&I, and the three PICASSO policy domains, in two main ways:

- **Research-based policy** – policy intended to advance or support the conduct and exploitation of research, ranging over direct R&I support modalities, demand-side instruments, complementary regulation and other interventions intended both to accelerate the solution and societal benefits of specific R&I and to strengthen the ‘research base’ in terms of its effectiveness, economic strength, resilience and integration with other areas; and
- **Policy-based R&I** – R&I activities that target areas of policy relevance, and R&I activities designed to inform policy by helping both to identify and clarify policy issues and by (sometimes) providing (partial) solutions to policy problems.

In both cases, it is necessary to take into account:

- The historical interaction of the EU and the US in these domains;
- The different ways in which R&I (industry & academia) and policy interact;
- The balance of societal, commercial, scientific and technology policy in driving development (“multistakeholder” nature of driving R&I);
- The extent to which the R&I policy nexus in the EU and the US develops along lines parallel to the PICASSO technology domains (5G, IoT/CPS and Big Data), societal domains (Smart Production, Smart Cities, Smart Energy, Smart Transportation) and policy areas (privacy and data protection, security and cyber-security, standardisation, and spectrum); and
- The nature and track record of EU and US engagement with other nations in these areas.

This report does not attempt to analyse, or even summarise complex linkages between policy and R&I that relate to the PICASSO technology areas (5G, IoT/CPS and Big Data) or policy areas (privacy, security, spectrum and standardisation). The work is ongoing, and in most respects, compared to the technologies and their application, policy is changing almost as rapidly (and somewhat less predictably) even if development of legal measures still take as long as they used to. Also, we were not able to provide at this point a fully-parallel discussion of the policy landscape in the EU and the US; this forms the basis of the four policy-specific reports; the first – on privacy and data protection¹ – has been completed and the second – on security – is currently under preparation. Rather, we concentrate on those areas where – based on the work of the project to date - interviews with policy analysts and actors and participants in project webinars were conducted.

The rest of this report is structured as follows: Chapter 2 presents the primary identification of opportunities – these are given in abbreviated form for ease of review and engagement, but will be expanded in a subsequent stand-alone document – in the form of an overview, in tabular form, of policy-driven R&I and R&I-driven policy areas where joint EU-US collaboration might be fruitful. This is followed by a discussion (in sections 2.2 and 2.3) of the history and comparability of ICT-related policies in the EU and the US. Chapter 3 presents a partial picture

¹ <http://www.picasso-project.eu/wp-content/uploads/2016/12/20161130-PICASSO-Policy-Paper-1-Privacy-and-Data-Protection-Final3.pdf>

of the R&I priorities and frameworks of greatest policy relevance in the EU (section 3.1) and US (section 3.2). Section 3.3 discusses R&I-related policy from the EU perspective in two areas; (5G in section 3.3.2 and IoT/CPS in section 3.3.3). Potential barriers to collaboration on policy-driven R&I are further discussed in chapter 4, along with 'external' R&I-related policy initiatives.

2. Overview

2.1. A Summary of Challenges and Opportunities

The following table summarizes a set of policy-driven R&I and R&I-driven policy areas where joint EU-US collaboration might be fruitful. These will be more fully described after public discussion and consultation at the “Trans-Atlantic Symposium on ICT Technology and Policy” that is organized by PICASSO in June 2017 in Minneapolis².

Table 1: Summary of policy collaboration opportunity topics and areas.

Application domains:	Policy-driven R&I	R&I-driven policy
General, cross-area		
Policy areas		
Legal definitions	Need to develop common definitions or core vocabulary to be used in specifying policies and regulations.	
Removing “stovepipes” and work across sectors and domains	Research into information-sharing, joint control, etc. for safety, liability	Consistency of regulation and policy across domains.
cyber-security & privacy	<ul style="list-style-type: none"> Solutions³ to both concerns e.g. ‘enhanced access.’ Address SOTA (state of the art) paradox: most organisations believe they are compliant with the rules⁴ but lack: <ul style="list-style-type: none"> Concept of “state of the art”; Processes or metrics to measure alignment with SOTA; Periodic reviews. 	<ul style="list-style-type: none"> Reduce ‘false dichotomy’ that: <ul style="list-style-type: none"> security and privacy are inevitably opposed; and privacy is a global, fundamental concern but security is national. EU: Secondary rules under GDPR⁵ /NISD⁶ may produce effective and equitable policy linkage; US fragmented general⁷ and sector-specific⁸ initiatives may accurately reflect technology and practice, stimulate R&I, business evolution; EU and US can learn from each other to find a better synthesis⁹ than could be achieved by simply adjusting in isolation.

² <http://www.picasso-project.eu/newsevents/project-events/june-2017-symposium>

³ For different uses and domains or ‘up the stack’

⁴ In EU, GDPR + NISD.

⁵ General Data Protection Regulation, see http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC

⁶ Network and Information Security Directive, see http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

⁷ E.g. Securely Protect Yourself Against Cyber Trespass Act (phishing and spyware; 2005; dead); Cyber-security Act (2012; dead); Executive Order Improving Critical Infrastructure Cyber-security (2013; in force, but not ratified); National Strategy to Secure Cyberspace; Cyber Intelligence Sharing and Protection Act (CISPA; contested), etc.

⁸ i) Health Insurance Portability and Accountability Act (HIPAA, 1996), ii) Gramm-Leach-Bliley Financial Services Modernization Act (1999); and iii) Homeland Security Act, including the Federal Information Security Management Act (FISMA 2002). ISPs and computer companies are not covered. There are proposed extensions (e.g. the Consumer Data Security and Notification Act which would strengthen GLB to mandate breach disclosure, or proposals to extend GLB to all entities handling consumer financial information (e.g. payment services).

⁹ Taking into account both the impact of policy measures on future technology and the scientific, trade and policy links between the EU and the US.

Application domains:	Policy-driven R&I	R&I-driven policy
Roles of public, private and civil society domain entities and interests	<ul style="list-style-type: none"> Interface between regulation and criminal law on one side and contract and tort law (private harm-based lawsuits¹⁰) on the other; Which 'domain' has primacy? <ul style="list-style-type: none"> Privacy: protection from whom? IPR: Open vs proprietary Security: national, critical infrastructure, commercial types of security; security vs. cyber-security. Joint work to establish a consistent framework for balancing these competing perspectives Immunity or standing for inter-domain lawsuits 	
Demonstration at scale and replication of solutions	<ul style="list-style-type: none"> Joint demonstrations to build common demand; Pooled or shared solutions. 	<ul style="list-style-type: none"> Ease policy harmonisation through unified technical bases; Replicate, adapt or differentiate solutions, policy frameworks.
Trade and international application aspects of international rules	<ul style="list-style-type: none"> EU: GPRD and NISD <ul style="list-style-type: none"> Both require companies to 'take into account' and 'have regard to' <i>state of the art</i> for cyber-security; Neither specifies technologies; Coverage broader than US but still vague and technologically sensitive; May lead to over- or mal-investment. US: <ul style="list-style-type: none"> Few direct, no general¹¹ cyber-security rules; No specific cyber-security measures¹² (only "reasonable" levels of security); May lead to under-investment. Collaboration prospects: where direct economic impacts are viewed as asymmetric, collaboration is considered less attractive (<i>quid pro quo?</i>). 	
Anonymising data, encryption and processing in encrypted domains	<ul style="list-style-type: none"> End-to-end solutions; Secure 'enhanced access' with appropriate joint controls and automated consent; Solutions to ensure data integrity. 	<ul style="list-style-type: none"> Rules on international (esp. bulk) access, data analysis, equipment interference, etc.; Reciprocal access and suitable protections for non-citizens whose data may be compromised.
Regulation areas		
Data protection	<ul style="list-style-type: none"> Data structures; Data processing controls; Auditable algorithms; Extension to complex systems. 	<ul style="list-style-type: none"> Consistent regulations spanning data and processing; Regulation of (and by) algorithms.

¹⁰ Effectively, tort law governs implicit societal responsibilities that people have to one another, as opposed to those responsibilities laid out in contracts or defined in statute law.

¹¹ Sector-specific rules: Health Insurance Portability and Accountability Act (HIPAA, 1996); Gramm-Leach-Bliley Financial Services Modernization Act (1999); Homeland Security Act, including Federal Information Security Management Act (FISMA 2002). ISPs, computer companies are not covered. Proposed extensions (e.g. Consumer Data Security and Notification Act) would strengthen GLB to mandate breach disclosure, or extend GLB to all entities handling consumer financial information (e.g. payment service providers).

¹² Data Quality Act (2001) may let OMB impose CNII protections, but technical aspects remain open.

Application domains:	Policy-driven R&I	R&I-driven policy
Alternatives to regulation	<ul style="list-style-type: none">• Self and co-regulation with industry-based international lead;• Structured¹³ international standards;• Market-based alternatives (e.g. compliance trading);• Pool regulatory information to improve policy, reduce distorting differences;• Trade linkages (TTIP, Privacy Shield successor(s)); and• Multistakeholder agreements recognising and inciting global good practice¹⁴.	
Cyber-security and privacy	<ul style="list-style-type: none">• Specific technical loopholes and provisions in GDPR, etc.;• Technical feasibility of compliance in layered, self-organised, autonomous etc. systems;• Develop privacy and security sensitivity taxonomies for tools, applications and services;• Better ID and security solutions¹⁵.	<ul style="list-style-type: none">• Research to clarify provisions, impacts of NISD and its national approximation e.g.:<ul style="list-style-type: none">○ Regtech for Critical National Infrastructure operators¹⁶, designated services¹⁷ and related entities¹⁸) to report breaches and take other actions;○ Require “good behaviour” from ICT developers and users¹⁹
Safety certification of systems	R&I to ²⁰ : <ul style="list-style-type: none">• Determine types and limits of safety performance;• Measure and control stochastic behaviour;• Safety taxonomy.	<ul style="list-style-type: none">• Regulatory incentive and informational approaches;• Intermediaries, contract menus;• Third-party liabilities.
General regulatory areas transformed by Internet	Regtech solutions: <ul style="list-style-type: none">• Compliance reporting;• Automated adherence.	<ul style="list-style-type: none">• Consumer protection;• Personal data protection;• Intellectual property law.
Sharing good practice regulations ²¹	Develop policy-compliant solutions (both for ICT policy and for sectoral policies that relate to ICT) to attain critical mass and advance SOTA	
Harmonisation of regulations in specific areas		
Smart energy	General recommendation, not much technology specificity except for noting potential for economies of scale all along energy value chain: <ul style="list-style-type: none">• Allow stakeholders to make grid investments in EU and US.	

¹³ Encourage compliance by wide applicability, foreclose race to bottom; structure may mirror Trade Agreements.

¹⁴ See for instance the Good Practice Policies of the IGF Dynamic Coalition on the Internet of Things at <http://www.iot-dynamic-coalition.org/wp-content/uploads/sites/3/2016/07/loT%20Good%20Practice%20Paper%202016.pdf>

¹⁵ E.g. replace passwords, develop appropriate encryption and implement differential privacy.

¹⁶ Energy, transport, health and banking.

¹⁷ Online marketplaces, online search engines and cloud computing.

¹⁸ Cloud providers, internet exchanges, online marketplaces.

¹⁹ Based on definition that reflects current and new technologies, application areas and behaviour – an example is banning use of default passwords for IoT consumer devices.

²⁰ This does not refer to technological R&I per se (discussed elsewhere in this document) but to technological alternatives or complements to policy rules, standards and/or regulations.

²¹ E.g. for smart metering and tariffs to manage system load capacity.

Application domains:	Policy-driven R&I	R&I-driven policy
Smart transportation	A substantial amount of collaborative policy-driven R&I is already going on.	<ul style="list-style-type: none"> • Adoption of green technologies; • Improved efficiency of electric cars; • Align charging station policies²²; • Regulatory provision²³ for automatic train control systems; • Resolve autonomous vehicle (AV) regulatory issues²⁴; • Conduct/share AV pilot experiences at global level; • Resolve regulatory issues²⁵ to allow autonomous aircraft to operate safely in civil airspace.
Standardisation		
Interoperability standards and harmonisation for 'smart' domains (energy, production, transportation, cities, production)	R&I efforts to jointly comply with different national requirements, procurement processes, etc. providing input to RFC processes.	<p>Generic opportunities:</p> <ul style="list-style-type: none"> • Participate in standardisation; • Reflect standards in regulations.
Smart city functionality standards	<ul style="list-style-type: none"> • Collect and (bench)learn from practices; • Ethical and safe crowd management. 	<ul style="list-style-type: none"> • Legal status for Smart Cities and supporting entities; • New structures for (international) critical service providers and strategic technology partners.
Wireless standards for car infrastructures (V2V, V2I, ...)	<ul style="list-style-type: none"> • Common, localisable regulatory and administrative structure for AV network managers; • Standards-based rules for H2M and M2M communication; • Legal recognition for standardised smart contracts. 	
Standards for air traffic management	<p>EU-US link with regard to drones mainly reflects:</p> <ul style="list-style-type: none"> • Equipment market opening (hardware, services and information harvesting); • Interoperability with general Air Traffic Control systems; • Key policy issue is certification via standards or otherwise; • Rules for where and how drones can be used. 	
5G		
Promote collaboration between the 5G PPP in Europe and the Advanced Wireless Research Initiative in the US	Technology solutions for dealing with different spectrum requirements and limitations	<ul style="list-style-type: none"> • Funding; • Coordinate deployments/pilots; • Standardisation; • Spectrum allocation²⁶.

²² Subsidies, technological compatibility.

²³ Accepting international standards, suppliers, R&I and testing results.

²⁴ Safety, energy use, privacy, economic development, impacts on related sectors, insurance, etc.

²⁵ Training liability, operational regulation, guidelines and rules, ATC, privacy, noise, etc. policy.

²⁶ Esp. for managing global policy issues (competition, privacy, etc.).

Application domains:	Policy-driven R&I	R&I-driven policy
Global spectrum harmonisation	<ul style="list-style-type: none"> • Enable single devices to use many parts of the spectrum; • Dynamic band selection based on local spectrum use policy and on location, application combination. 	<ul style="list-style-type: none"> • Agree spectrum mapping for range of consumer and industry purposes; • Adapt spectrum licensing to fit new uses, power, interference etc.; • Modify spectrum allocation procedures (auction, trading) to serve 5G requirements.
Standardisation	<p>Market driven</p> <ul style="list-style-type: none"> • Reflect technological realities; • Stimulate R&I; • Remove or reduce market distortions; • Lower sectoral and use boundaries. 	<ul style="list-style-type: none"> • Ensure functioning of markets for ICT products and services; • Build on initiatives led by large companies²⁷ such as NGMN 5G²⁸; • Reflect standards in regulations and procurement.
Big Data		
There are very strong Big Data policy initiatives on both sides of the Atlantic	<ul style="list-style-type: none"> • Build privacy protection into data use (protect against personal data abuse); • Data quality, provenance checks; • Solutions and standards that allow auditing, monitoring and evaluation of data processing to verify privacy, confidentiality, integrity; • Technical and operational approaches to algorithm creation, use and linkage to ensure and/or demonstrate regulatory compliance. 	<ul style="list-style-type: none"> • Move privacy rules from protecting against <i>use</i> of personal data to protecting against abuse of persons by means of data processing; • Trade-compatible data mobility rules to address current technical, economic and policy issues, esp. <ul style="list-style-type: none"> ○ Data processing for science, government and commerce; ○ Extraterritoriality.
Regulation is a key enabler for global adoption of data-intensive services ²⁹	<ul style="list-style-type: none"> • Enable and facilitate control of data localisation or tracking; • Explore automating location-specific data processing. 	<ul style="list-style-type: none"> • Common legal (treaty) bases for national regulations (e.g. rights of the person, commercial activities); • Reciprocal legislation protecting the rights of the individual; • Negotiated harmonisation and subsidiarity structure for <ul style="list-style-type: none"> ○ Addressing current, future issues; ○ Balancing rights with regulatory and policy concerns.

²⁷ E.g. NTT Docomo, Samsung, Ericsson, T-Mobile and Verizon.

²⁸ See <https://www.ngmn.org/5g-white-paper.html>.

²⁹ This was recognised in e.g. Safe Harbour and Privacy Shield, though national differences and regulatory burden considerations have undermined this.

Application domains:	Policy-driven R&I	R&I-driven policy
Cloud computing implications ³⁰	Explore ability of technological, managerial and commercial solutions to: <ul style="list-style-type: none"> • Comply with letter/spirit of law; • Open path to better ways to attain general and specific policy objectives? 	<ul style="list-style-type: none"> • NISD covers e.g. cloud mining, other Big Data Analytics functions; • Need to reconsider legal structures - <ul style="list-style-type: none"> ○ ethereum and similar distributed computing platforms and services delivered over them; ○ Providers (ostensibly covered) who may not be local or attributable.
Blockchain implications ³¹	<ul style="list-style-type: none"> • Develop effective applications for specific purposes³²; • (Learning from practice). 	<p>Application-driven regulatory issues:</p> <ul style="list-style-type: none"> • Cryptocurrencies - anti-money laundering, terrorist financing and other financial regulations; • Smart contracts - contract law; • Token crowd sales - securities regulation.
IoT/CPS		
Policy		
Engineering trustable, reliable, evolvable and affordable cyber-physical systems requires huge efforts; joining forces will help to advance more quickly and thus meet societal challenges.		
Combining the CPS and IoT worlds.		<ul style="list-style-type: none"> • Consistent regulatory treatment; • Common rules for aggregating, decentralising and partitioning regulatory responsibilities and entitlements.
Guidance, good practice on implementing smart functionalities	<ul style="list-style-type: none"> • Establish global good practice framework; • Establish taxonomy for privacy/safety/security sensitivity. 	<ul style="list-style-type: none"> • Guidance-based: <ul style="list-style-type: none"> ○ Comply, demonstrate equivalent performance or explain; ○ Apply to identification, monitoring and enforcement of “good practice” ○ Where proportionate and justified – even cross-border; • Breach reporting legislation; • Consumer protection, Service Level Agreements.
Regulation		
Safety certification	<ul style="list-style-type: none"> • At device and/or system level: <ul style="list-style-type: none"> ○ Technical indicators; ○ Verification means; ○ Safety-by-design. 	<ul style="list-style-type: none"> • Legal standing of guidance; • Standards-based safety regulation; • <i>Ex ante</i> licensing and type approval; • Common or harmonised <i>ex post</i> (conduct or outcome) sanctions.

³⁰ NIS Directive definition: “digital service that enables access to a scalable and elastic pool of shareable computing resources.” Also: “cloud computing services span a *wide range of activities* that can be delivered according to *different models*.”

³¹ Big Data is (in large part) concerned with analysis of unstructured data, so the access structures and data quality certification aspects of Blockchain, the analytic applications of data mining and the data collection implications of distributed ledger technologies (selection effects in the record) make this a Big Data topic.

³² Applications for purposes refers to e.g. cryptocurrencies, distributed ledgers for banking records and interfirm coordination, smart contracts, regtech applications, and blockchain business models in retail, transport, manufacturing, etc.

Application domains:	Policy-driven R&I	R&I-driven policy
Privacy ³³ .	<ul style="list-style-type: none"> • At device and/or system level: <ul style="list-style-type: none"> ○ Technical indicators; ○ Verification means; ○ Privacy-by-design; • Privacy as service business models and processes; • Correct or route around design deficiencies to pre-empt or reduce requirements for coercive regulations³⁴; • Security standards and privacy protections matching information sensitivity³⁵; • Format consistency of security protections³⁶; • Technical implementation of data use, purpose, amount and time limits. 	<ul style="list-style-type: none"> • Foresight-based policy – take strategic account of data privacy and sharing regulatory impact on the development of CPS and IoT; • Harmonise regulation across technical, application, policy areas; • Industry-led³⁷ regulatory recommendations, guidelines; • Adjust consent rules to cope with lack of user interface on many IoT devices and intransparent automatic interaction among connected devices, which make it hard to meet legal requirements.

³³ Applications rely on collecting and utilising data from a myriad of sensors.

³⁴ E.g. lack of user interface/visibility/control; invisibility of most M2M interactions.

³⁵ This is a generic regulatory requirement (also embedding burden reduction mandates) that implies technological detection and response to changing or differentiated sensitivity.

³⁶ To protect private information against: loss; theft; corruption; and unauthorized access, disclosure, copying, use, or modification, *regardless of the format in which it is held*.

³⁷ E.g. BITAG ([http://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_\(IoT\)_Security_and_Privacy_Recommendations.pdf](http://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf))

Application domains:	Policy-driven R&I	R&I-driven policy
Security and cyber-security	<ul style="list-style-type: none"> At device and/or system level: <ul style="list-style-type: none"> Technical indicators; Verification means; Security-by-design; Security as a service business models and processes; Match security requirements to <ul style="list-style-type: none"> Information, functional sensitivity, Data amount, distribution, format and method of storage CPS architecture and control. Physical, organisational and/or technological controls; Shared, policy-focused research into attribution and incentives; Model (and simulate) potentially harmful interactions among devices, develop device- or system-level safeguard³⁸; Develop and implement monitoring and patching measures for devices in systems context. 	<ul style="list-style-type: none"> Innovation-friendly, coherent regulatory rules and procedures; Reward security-conscious products with certification; Promote adoption and legal standing of cyber insurance; Facilitate or accommodate industrial sharing of threat, incident information; Recognise voluntary good practice development, adoption; Agree and adopt responsibility³⁹ and accountability arrangements for data and functions moving across system, organisational, purpose, national etc. boundaries; Proportionate and conformant (common) monitoring, reporting and dispute resolution mechanisms esp. for cross-border issues; Develop legal framework⁴⁰ for class action lawsuits on privacy, data and security breaches; Address four linked rising challenges: <ul style="list-style-type: none"> Risk of harm; Sensitivity to privacy or performance problems; More – and more complex – vulnerabilities and difficulty of patching; Vulnerabilities created by third parties (knowingly or not).
Regulation to support market access	Blockchain ⁴¹ /tracking	<p>Policy research needed:</p> <ul style="list-style-type: none"> Markets hard to measure and analyse; market access regulation subject to many restrictions ranging from Trade Agreements to jurisdiction issues; Complex counterfactual.
Interoperability standards	<ul style="list-style-type: none"> Open standards; Intelligent matching/adaptability. 	Compliance with good practice standards

³⁸ For example, autonomous vehicle policy require this kind of R&I to establish what needs to be regulated and in what way this should be done. It requires collaboration because the value chain stretches from designers and manufacturers in one country to drivers in another.

³⁹ This includes DDOS and related issues – see e.g. https://www.schneier.com/blog/archives/2016/11/regulation_of_t.html.

⁴⁰ For example, it may not be practical for developers comprehensively to test all possible device interactions for compatibility issues. If an IoT device causes harm through decisions or actions made or coordinated with other devices, actual and efficient liability may be hard to determine. Establishing ‘fault’ for incorrect dosing from a medication pump is harder if the pump adjusts dosage after communicating with other connected devices to obtain health and environmental data – particularly if communication problems may have occurred. Fault for a traffic accident may be complicated by reactions of an AV to communications from other AVs, devices carried by pedestrians or networked sensors. Existing negligence, product liability and privacy laws provide some – but not complete guidance. In regulatory law, this is complicated by the differences between civil and common-law means of detecting and responding to change. In tort law, these uncertainties will encourage plaintiffs’ counsel to seek new ways to place liability for damages caused by IoT devices.

⁴¹ Operational (sensor and actuator) data in distributed interacting systems of things can usefully be placed in and processed via distributed ledgers.

2.2. Approaches to ICT Policy Issues in the EU and the US: Some Similarities and Differences

2.2.1. A Bit of History

The EU and the US have taken different approaches to ICT policy issues. One part of this concerns the underlying policy stance. At least until the implementation of the Digital Single Market Strategy (1), the EU sought to encourage the development of underlying infrastructures and the service and application markets created on top of them through demand-pull and removal of ‘bottleneck’ barriers to competition (though not the bottlenecks themselves). To do this, policy sought to drive down prices for DSL-based Internet services by forcing network providers to open their facilities at discounted prices to new entrants. But this had the (apparent) effect of limiting both maintenance and new technology investment incentives for providers, and restraining the growth of EU cable Internet, fibre-optic and high-speed mobile broadband networks. From the regulatory standpoint, this amounted to ‘utility-type’ control of large essential facility providers that tried, with varying degrees of success, to force competition in the ‘upper layers’ of the market.

The US pursued a similar strategy with respect to voice telephony, but intentionally exempted Internet services, in effect leaving fixed and mobile broadband Internet access markets to develop largely on their own. As a result, the US has seen much higher (nearly a trillion and a half dollars by 2015) private investment in cable, mobile, fibre, and next-generation copper/fibre hybrid services. This helped contribute to the development of innovative Internet-based businesses; 11 of the top 15 Internet businesses, most started in the last decade, are US-based, with the rest coming from China. None are from Europe. On the other hand, US markets remain largely foreclosed, with relatively little competition in broadband service provision, and consequent higher prices.

The DSM sought to reform the EU stance by embracing competition; critics of the US light-touch approach have urged the EU to ‘avoid the mistakes’ of US Policy (2). The new strategy led not only to considerable advances in many areas⁴² but also to a tighter linkage across different aspects of policy. However, progress towards ubiquitous availability, affordability, uptake and quality remains patchy; this uneven development is itself a drawback, since it leads to uneven playing fields for rural and urban enterprises, small and large enterprises, different services or technological approaches to service delivery (meaning that the market will not always go to the ‘best’ technology or firm) and to asymmetries among Member States. These types of digital divide can, as is well-known, harden into other divides. From the European perspective, this type of inefficient inequality is considered a serious policy problem.

In the US, the potential to limit competitors’ access over networks drove high levels of investment (3); the inevitable pushback led to a certain amount of net neutrality and other forms of open network regulation. The US also achieved fairly high availability and adoption of ‘regular’ broadband (though not of high-speed broadband) (4), but retains high levels of concentration (though some argue that potential competition in slower broadband and possible emergent competition in gigabit broadband may drive a degree of efficiency). As a further consequence, the US lags Europe in terms of affordability, especially for faster broadband (3).

2.2.2. The Difficulty of Meaningful Comparisons

But it should be stressed that there is little general agreement as to whether (or in which ways) the EU and the US are ‘doing better’; different metrics are associated with different ways of defining and stating overarching

⁴² See e.g. Digital Single market Scoreboard data (e.g. <https://ec.europa.eu/digital-single-market/digital-scoreboard>).

policy objectives. Available official statistics do not promote easy comparisons, and as a result, the scope and nature of policy interventions differ. This policy ‘status contest’ seems strongly to influence policy directions. To do this area justice would mean looking at the influence of industry on policy and the way R&I policy interacts with other ‘owners’ of the relevant policy space, but that goes beyond the scope of the current exercise. In what follows, we merely note that the EU and the US *tend* to attach different priority to such policy performance metrics as inequality (of opportunity or outcome), competition vs. profitability, co-operation vs. collusion, international openness vs. protectionism and the pace of innovation.

2.3. Differences and Co-operation

These differences both inhibit and create opportunities for mutually-beneficial co-operation. They inhibit them to the extent that

- EU and US public administrations see policy only in nationally (political or economic) competitive terms;
- Public administrations try to pick and support ‘national champions’ in global playing fields;
- ‘Not invented here’ parochialism on both sides of the Atlantic prevents conduct of R&I by teams representing the best minds, the fullest possible sharing and analysis of evidence or the best possible application of the fruits of R&I; or
- Differences in perspective lead to fragmentation and poor results arising from a lack of critical mass lead to the abandonment of promising areas for collaboration.

Differences of perspective can enhance cooperation if they:

- Suggest useful alternative ways of formulating or tackling problems;
- Allow the EU and the US collectively to influence policy on a global front or where collective R&I policy can influence technological or market development;
- Spark novel contacts such as partnerships among researchers, and between research, industry and government (the ‘strength of weak ties’ effect (5));
- Create a positive feedback competition leading to faster or better results by avoiding lock-in and minimising the chance of blind alleys; and
- Promote a diversity of disciplines, methods and perspectives leading to deeper understanding.

Note that the end result may be convergence to a common approach (in research or in application) or a complementarity (e.g. the development of use-specific standards as well as use-neutral ones, or the development of policies that reflect international differences or comparative advantage together with those that are harmonised in areas where the benefits outweigh the drawbacks. This arises directly from differentiated R&I collaboration, which allows us to distinguish those areas that require harmonisation from those that require differentiation in ways that reflect the ultimate ways in which technologies will be developed rather than the mechanisms of interoperability on the purely technological plane.

3. Policy Priorities in the EU and the US

Associated with each of the identified technologies are a range of policy areas; these go beyond the overarching areas identified in PICASSO, but are worth identifying because policy initiatives are on one hand not technology-specific while technological advances can not only address multiple policy issues but also change the trade-offs to be considered by policy-makers and the degree to which policy may be shaped by R&I (and thus, given the greater ease with which technology crosses national boundaries (compared to policy) the potential alignment of policies.

For 5G, the two main policy areas are:

- Spectrum - a priority for policymakers to set the stage for 5G is allocation of high-band millimeter wave spectrum. Here the US FCC has set a strong precedent: in 2015 the Commission proposed rules as to how best to put high-band spectrum to use and has proposed an order to open up a significant amount of high-band spectrum⁴³. For its part, the EU has made spectrum an explicit part of both the 5G Action Plan and the Proposed Electronic Communications Code.
- Infrastructure - high-band spectrum, or any small-cell densification will require significant investment in infrastructure—both for siting the antenna equipment and for backhaul. The US again is relying on industry, while the EU foresees substantial co-funding.
- It should be noted that 5G in the 3GPP sense, not to be confused with various marketing claims and proprietary 5G-like schemes currently being deployed in the United States. The work on “Advanced Wireless” currently done in the US comes closest, and goes beyond the 3GPP 5G in some aspects.

For IoT/CPS, the priorities are more diffuse, but include such elements as:

- Governance of complex and diverse masses of connected devices;
- Secure and accurate identification of devices and their systemic compatibility;
- Privacy, trust, security and performance of complex systems of interacting devices and subsystems;
- Algorithmic regulation in the context of cyberphysical systems; and
- Legal and regulatory issues and policies arising from these phenomena.

We do not cover Big Data in the same way, in part because industry and academia are well in advance of government in this area and in part because the linkage to policy domains beyond the scope of this project is stronger for that area.

3.1. EU Priorities

3.1.1. Overarching Research Programme – Horizon 2020

The Horizon 2020 programme has identified a number of strategic priorities tied closely to the technology, societal and policy application areas identified by PICASSO. They are not divided exactly along the same lines, but the linkages are clear. The overall programme is structured around three priority areas: excellent science; industrial leadership; and societal challenges. These in turn define three ‘pillars’ of the overall programme. This is shown in graphical form in Figure 1.

⁴³ 3.85 gigahertz of licensed, flexible use spectrum and 7 gigahertz of unlicensed spectrum. Six hundred megahertz will be reserved for experimental spectrum-sharing models.

More specifically, the Excellent Science pillar is linked to science, R&I and education policy; the Industrial leadership priority is linked to industrial policy (investment in key technology areas and measures to increase private sector investment), SME support measures and (to a lesser extent) policies to improve competition and remove market distortions in technology-based sectors. The societal challenges priority area is linked to climate, environment, energy, transport and similar policy areas, to multidisciplinary approaches (including those that strengthen links between science and policy) and to improving the evidence base for these policies by tests, demonstrators and scale-up activities.

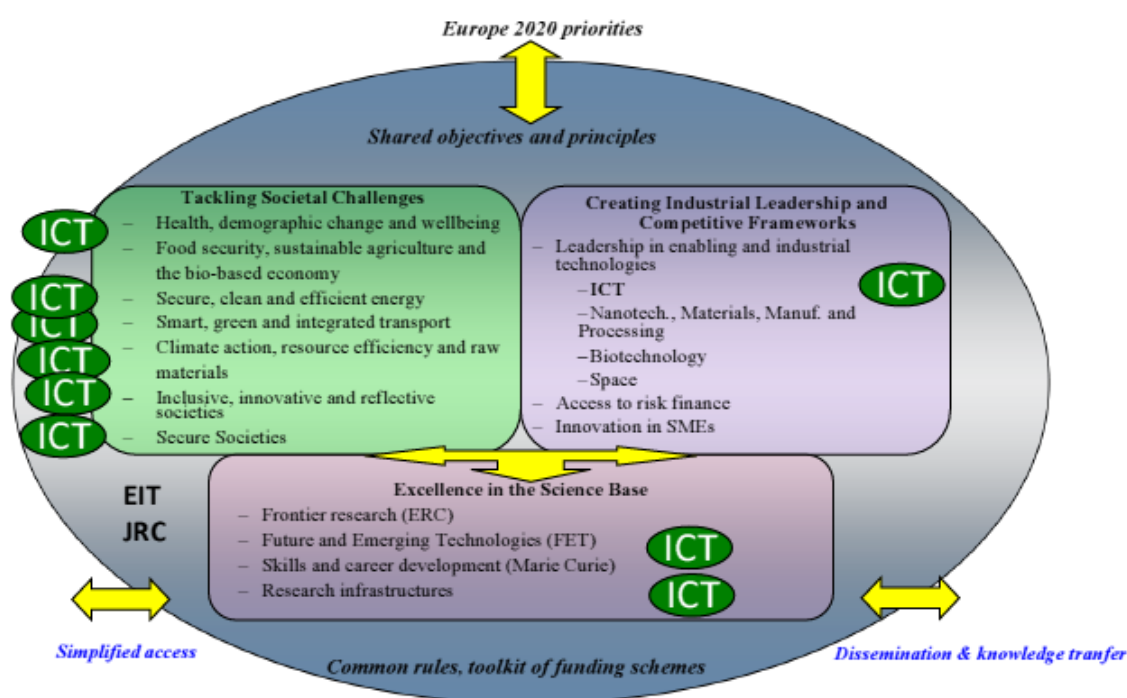


Figure 1: Horizon 2020 ICT-related priority areas⁴⁴.

Progress is not limited to direct project funding, but includes a range of partnerships:

- Public private partnerships, through Joint Technology Initiatives or other formal structures (Art. 187) and through contractual agreements that provide inputs to work programmes (on the basis of clear commitments from private partners).
 - The Joint Technology Initiatives (usually institutional PPPs run as Joint Undertakings between industry and the EU) involve a range of different structures and funding mixes. The first batch of JTIs included several of relevance particularly in the IoT/CPS area – ARTEMIS (Embedded Systems), ENIAC (Nanoelectronics) and EpoSS (Smart Systems Integration) – which have been merged into the ECSEL Joint Undertaking (Electronic Components and Systems for European Leadership). Each JTI implements a common Strategic Research Agenda (SRA) and defines its own Work Programme, and runs its own support arrangements (Calls, project selection, negotiation of Grant Agreements, reporting etc.). The current crop includes:

⁴⁴ European Commission (2016) “A Guide to ICT-related activities in WP2016-7” at: <https://ec.europa.eu/programmes/horizon2020/sites/horizon2020/files/Guide%20to%20ICT-related%20activities%20in%20WP2016-17%20A4%20v8.pdf>.

- [Innovative Medicine 2 \(IMI\)](#) to develop next generation vaccines, medicines and treatments, such as new antibiotics;
 - [Clean Sky 2 \(CS2\)](#) to develop cleaner, quieter aircraft with significantly less CO₂ emissions;
 - [Fuel Cells and Hydrogen 2 \(FCH\)](#) to develop and demonstrate clean and efficient fuel cell and hydrogen technologies for stationary and mobile applications;
 - [Biobased Industries \(BBI\)](#) to use renewable natural resources and innovative technologies for greener everyday products;
 - [Electronic Components and Systems for European Leadership \(ECSEL\)](#) to boost Europe's electronics manufacturing capabilities. ECSEL combines the Joint Technology Initiatives (JTI) ARTEMIS - Embedded Systems, ENIAC - Nanoelectronics and EposS;
 - [Shift2Rail \(S2R\)](#) to develop better trains and railway infrastructure; and
 - [SESAR](#) to develop the new generation European air traffic management system.
- The funding for contractual PPPs comes equally from the private and public sectors, and is awarded through open H2020 Calls administered by the EU. Include (those of most relevance in bold):
- [Factories of the Future \(FoF\)](#) to strengthen European manufacturing industry's international competitiveness, increasing the small and medium-sized enterprise base by development and integration of innovative technologies;
 - [Energy-efficient Buildings \(EeB\)](#) to support the European construction sector by exploring innovative methods and technologies to drastically cut energy consumption and CO₂ emissions of buildings via energy-efficient systems and materials for new buildings and refurbishment and retrofitting of existing buildings;
 - [Green Vehicle](#) to promote R&I in technologies for renewable and sustainable use and safety and transport planning;
 - [Sustainable Process Industry \(SPIRE\)](#) to foster a sustainable process industry by enhancing manufacturing resource and energy efficiency;
 - [Photonics](#) to realise the potential of photonics to contribute across sectors and products;
 - [Robotics](#) to enhance industrial competitiveness and tackle such societal challenges as demographic change, health and welfare, food, mobility, safety and security;
 - **5G Infrastructure to support development, deployment and use of 5G networks for the Internet of the future to provide advanced ICT services for all sectors and users;**
 - [High Performance Computing \(HPC\)](#) to underpin European economic growth European science; and
 - **Big Data to combine public and private research in order to develop pioneering concepts in the fields of energy, manufacturing and health.**
 - [A prior PPP on [Future Internet](#)] was discontinued last year.

Many of these initiatives are linked to PICASSO priorities. For example, the 5G priorities explicitly incorporate:

- Technological challenges such as the traffic increases expected from IoT and other M2M communications and objectives like capacity/efficiency improvements, increased service/content

centricity, virtualisation & cloud transition, AI (cognitive and context-aware processing), improved manageability (including via complexity-related channels like self-organisation and –optimisation), cross-layer optimisation, increased flexibility, smart environments, sensor and sensor-actuator networks and M2M; and

- Societal and policy impetus from ‘Smart’ systems (Cities, Transportation, Energy and Grids) to meet challenges of (*inter alia*) urbanisation, urban sprawl, changes in population density, mobility and diversity (age, income education, ethnicity, etc.), increased information supply, demand and processing power, evolving and increasingly plastic social networks, increased (cause for) concern about privacy, security, environmental impact, energy efficiency, food security, healthcare and education (*inter alia*).

The 5G public-private partnership (launched in 2014 with starting EU funding of €700 million and founder members drawn from the largest European corporate players in the area – Ericsson, Orange, NSN, SES and Alcatel-Lucent. The current membership⁴⁵ stands at 27 industrial members, 13 research partners and 10 SME members and 15 Associate Members, including e.g. standards organisations. This PPP is very active in the global 5G Infrastructure Association, which has a range of policy-orientated Working Groups aligned with the H2020 Pillars and EU policy:

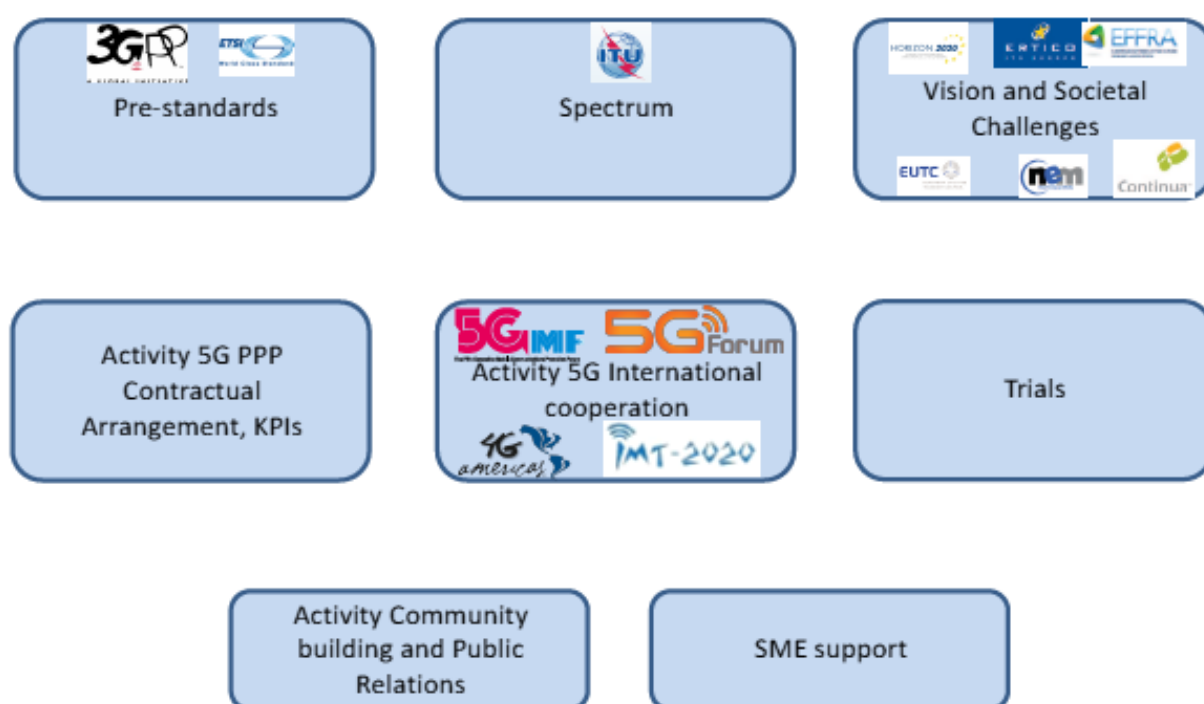


Figure 2: Policy-related working groups of the 5G Infrastructure Association.

3.1.2. Innovation Policy – IoT/CPS

The EU is seeking to support innovation in the IoT domain by using public funding to adjust the balance of research in the direction of open and easy accessible IoT platforms. One concrete expression of this is the recently-launched “IoT European Platform Initiative (IoT-EPI)⁴⁶” which is aimed at building “a vibrant and sustainable IoT ecosystem in Europe.” This platform will be linked to the inter-industry Alliance for Internet of

⁴⁵ A full listing can be found at: <https://5g-ppp.eu/our-members/>.

⁴⁶ <http://iot-epi.eu/>

Things innovation (AIOTI) (see Section 3.3.3), which in turn builds on the work of the IoT European Research Cluster (IERC)⁴⁷ – a grouping of FP7 and national IoT projects and initiatives.

The European Union also participates in international research and policy discussions in order to advance the technology. International calls for joint proposals are foreseen under the Horizon 2020 programme.

International public-private collaboration is also progressing via the Industrial Internet Coalition⁴⁸, which is “a global, member-supported, organization that promotes the accelerated growth of the Industrial Internet of Things by coordinating ecosystem initiatives to securely connect, control and integrate assets and systems of assets with people, processes and data using common architectures, interoperability and open standards to deliver transformational business and societal outcomes across industries and public infrastructure.”

3.2. US Priorities

The US is keen to preserve its position in relation to 4G, relying on a permissive and industry-led approach⁴⁹.

3.3. Research-driven Policy in Two Technology Areas

3.3.1. Schema

In this section, we survey some aspects of policy-relevant research that provide fruitful scope for collaboration in two specific areas; 5G and IoT/CPS. This discussion should be seen as supplementing the suggestions and opportunities identified in Table 1. They can be divided roughly according to whether:

- Policy is directed at technological, economic or societal levels (objectives and instruments);
- The two regions have parallel (but largely separated) policy mechanisms and issues – for instance, telecommunications is largely localised and regulated primarily at Member State (MS) or EU level in the EU (though increasingly harmonised), but is nationally more uniform and primarily regulated at Federal level in the US. This can be further subdivided according to whether conduct is regulated at EU or US Federal level or at MS/state level;
- The two areas have overlapping policy issues (e.g. privacy and security, which are shared because the systems to which they are connected and the flows of data and interactions are global in scope); and
- The policy issues are linked to (or sharper in) specific application areas that are shared (e.g. finance) or complementary, e.g. health, where delivery is local but inputs (e.g. pharmaceuticals) are increasingly global.

Where the policy issues in the two regions can be separated, they may be

- Convergent – e.g. where dominant technologies or approaches will prevail in both areas;
- Divergent – where solutions and institutional arrangements follow different equilibrium paths (including regulation and other policies)

⁴⁷ <http://www.internet-of-things-research.eu/>

⁴⁸ <http://www.iiconsortium.org/index.htm>

⁴⁹ See e.g. the remarks of Michael O’Rielly, FCC Commissioner, to Hogan Lovells’ Technology Forum: “The 5G Triangle” at: https://apps.fcc.gov/edocs_public/attachmatch/DOC-339558A1.pdf.

- Localised – where differences in development reflect ‘environmental’ or settled differences in local conditions
- Complementary – where the interactions between the two regions on the policy or technology planes reflect comparative advantages (e.g. in hard or soft innovation)

3.3.2. EU Policy in the 5G Domain

Overall, it appears (at the moment) that the EU and the US both recognise the importance of 5G and are eager to encourage both infrastructure and exploitation, though in very different ways (as, indeed, was the case with 4G). While policy remains fluid, some broad outlines can be seen.

As regards 5G, the EU has concrete plans and initiatives (both via the 5G PPP described above and other actions foreseen in the 5G Action Plan⁵⁰ and the closely-associated industry-developed 5G Manifesto⁵¹), that extend and builds on the R&I underpinnings established by the 5G PPP, especially in the direction of a European market for 5G. This includes in particular

- The proposed Directive for a European Electronic Communications Code⁵², which seeks to support the deployment and take-up of 5G networks, notably as regards assignment of radio spectrum, investment incentives and favourable framework conditions;
- Recently adopted open Internet rules that provide legal certainty to the deployment of 5G applications.
- Aligning roadmaps, timetables and priorities for coordinated 5G deployment across all EU Member States, with i) a timetable involving preliminary trials, national deployment roadmaps, at least one major "5Genabled" city per country by the end of 2020 and uninterrupted 5G coverage in all urban areas and major terrestrial transport paths by 2025 and ii) 5G national roadmaps that coordinate fibre and cell deployment;
- Making provisional spectrum bands available for 5G ahead of the 2019 World Radio Communication Conference (WRC-19), to be complemented by additional bands as quickly as possible, and work towards a recommended approach for the authorisation of the specific 5G spectrum bands above 6 GHz;
- Promoting early deployment in major urban areas and along major transport paths and pan-European multi-stakeholder trials to accelerate progress from technological innovation into full business solutions.
- Implementation of an industry-led venture fund in support of 5G-based innovation including plans for key technological experiments and demonstrations starting in 2017 and detailed roadmaps for advanced pre-commercial trials in 2018 in key sectors; and
- Collective action to develop and promote global standards.

⁵⁰ See: <https://ec.europa.eu/digital-single-market/en/5g-europe-action-plan>.

⁵¹ “5G Manifesto for timely deployment of 5G in Europe” at: <http://telecoms.com/wp-content/blogs.dir/1/files/2016/07/5GManifestofortimelydeploymentof5GinEurope.pdf>.

⁵² See <https://ec.europa.eu/digital-single-market/en/news/proposed-directive-establishing-european-electronic-communications-code>, both for the proposed Directive and for the detailed Impact Assessment, which identifies and assesses problems connected with 5G, IoT/CPS and Big Data, and seeks to assess the impacts of specific elements of the Code, especially in relation to the specific objectives of ubiquitous very high capacity connectivity (in the Single Market), competition and wide user choice and simplification and harmonisation of the regulatory environment.

- This is to be backed up by demand-side measures (Member States are supposed to consider using the 5G infrastructure to deliver communications for public safety and security) a targeted public-private venture capital financing initiative (combining EU funds and governance with EIB and industry).

By contrast, the US approach appears to be more laissez-faire, relying on making available large blocks of spectrum for experimentation and supporting industry-led standards and deployment initiatives⁵³.

However, there are as yet few concrete steps to harmonise policy involving the US and the EU; at the moment, the global picture appears somewhat fragmented⁵⁴.

3.3.3. EU Policy on the Internet of Things/CPS

Starting in 2015, the EU has launched a series of policy measures to accelerate IoT development and take-up.

In March 2015, a dedicated association, the Alliance for Internet of Things Innovation⁵⁵ (AIOTI) was launched by the European Commission support EC-industry joint action to establish a competitive European IoT market and foster the creation of new business models. Today AIOTI is the largest European IoT Association.

The May 2015 adoption of the Digital Single Market (DSM) Strategy⁵⁶ contained specific objectives for the Internet of Things; in particular to avoid fragmentation and to foster interoperability. This was further clarified in an April 2016 staff working document "Advancing the Internet of Things in Europe"⁵⁷. This document is part of the "Digitising European Industry (DEI)" initiative⁵⁸; it outlines the EU's IoT vision based on three pillars:

- a thriving IoT ecosystem;
- A human-centred IoT approach; and
- A single market for IoT.

Potential obstacles that could be addressed by collaborative R&I include the growing need for e.g.:

- Capacity to handle large diversity and volumes of connected devices;
- Secure identification⁵⁹ the ability to discover devices that can be plugged into IoT systems;
- Acceptable and effective ways to tackle privacy, trust, security and performance issues surrounding complex systems of separate (but interacting) things;
- Understanding of the functions, interactions and impacts of algorithms used to process data and to take actions within the context of cyberphysical systems;
- Methods for regulating the systemic behaviour of networks of algorithms (as well as devices); and

⁵³ See e.g. <http://www.5gtf.org/>.

⁵⁴ See e.g. the presentation by Werner Mohr (Chair of the Board of 5GPPP) at the Global 5G Event, Rome, Italy, November 9, 2016: https://5g-ppp.eu/wp-content/uploads/2016/11/Opening-2_Werner-Mohr.pdf.

⁵⁵ <https://ec.europa.eu/digital-single-market/en/alliance-internet-things-innovation-aioti>.

⁵⁶ <http://ec.europa.eu/priorities/digital-single-market/>.

⁵⁷ Staff Working Document: "Advancing the Internet of Things in Europe", accompanying the document "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Digitising European Industry - Reaping the full benefits of a Digital Single Market COM(2016) 180" available at: <http://eur-lex.europa.eu/legal-content/TXT/?uri=CELEX:52016SC0110>.

⁵⁸ This initiative emphasises cyber-physical systems to a greater degree and also deals with cloud computing, big data and data analytics, robotics and 3D printing – see <https://ec.europa.eu/digital-single-market/en/digitising-european-industry>.

⁵⁹ Numbering and identification issues were partially being addressed in conjunction with the 2016 Review of the EU telecommunications rules and is being further developed as part of the measures proposed under the rubric of "Connectivity for a European Gigabit Society" (<https://ec.europa.eu/digital-single-market/en/connectivity-european-gigabit-society>), the European Data Economy initiative (<https://ec.europa.eu/digital-single-market/en/building-european-data-economy>)

- Ways to handle legal, regulatory and policy issues arising from these R&I-based developments.

4. Barriers to Policy-driven R&I Collaboration

In principle, the policy relevance of R&I activity does not create any extra barriers to international collaboration, provided the policy issues themselves are sufficiently broad or shared. This is just as well; existing barriers are steep enough already in joint undertaking of publicly-funded R&I. Purely private-sector or third-sector activities are generally less sensitive to the extent that the participating entities are already international in scope or partnerships; existing barriers are less bound up with considerations of national interest than with more easily-definable commercial or career interests (e.g. IP formation, ownership and exploitation, market access and power, etc.). These can be priced and contracted for, providing framework conditions (e.g. relating to patents) can be aligned.

Within specific domains, however, policy considerations can create more direct barriers; as noted in the Policy Thematic Papers, privacy and data protection are approached in very different ways and existing attempts to harmonise the legal requirements in order to address privacy and data protection concerns in relation to international flows of data have stalled and may be in danger of reversal⁶⁰. It may be that this uncertainty militates against shared R&I activity, leads to a situation where technological solutions are required to reconcile the different approaches in different countries, or fragments research in the two regions. In particular, as regards Big Data and IoT/CPS initiatives, it may be appropriate to develop solutions that provide some of the benefits of data flows without attendant risks.

Similar considerations apply to security and cyber-security, with potential additional classification complications, not exclusively focused on “securing” access and data, but including security measures intended to facilitate surveillance and (police) investigations.

Other issues are related to “terms of art”, such as 5G. In Europe, this is taken in the 3GPPP sense, broadly, whereas the term is in use in the USA as marketing concept by telecom companies in the narrower sense. EU work on 5G compares more to US work on “Advanced Wireless” – and here, collaboration remains attractive.

In terms of funding, there are explicit arrangements under Horizon 2020 for international collaboration (e.g. by launching parallel projects, or through having US entities participate in EU projects using US funding), but these do not fully cover US-EU R&I collaboration. More precisely, Horizon 2020 is open to participation from across the world, provided European researchers include international partners when preparing proposals. Therefore US researchers, enterprises and institutions can join with European partners jointly to develop knowledge and data and to participate in or even to lead scientific teams and networks.

Of course, participation and funding are different matters. The EU will fund the participation of partners from developing countries⁶¹, it does not automatically fund the partners from industrialised countries such as USA. US researchers should bring their own funding – either from the participating institutions or US funding agencies.

⁶⁰ The Art 29 WP has expressed its doubts about the US-EU Privacy Shield (see http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/20160726_wp29_wp_statement_eu_us_privacy_shield_en.pdf) and the recent US Executive Order on “Enhancing Public Safety in the Interior of the United States” includes the statement that “Agencies shall, to the extent consistent with applicable law, ensure that their privacy policies exclude persons who are not United States citizens or lawful permanent residents from the protections of the Privacy Act regarding personally identifiable information.” The picture is complicated by the EU-US “Umbrella Agreement” which seeks to protect personal data transferred for law enforcement purposes between the EU and U.S. under existing international agreements involving the EU and U.S. The Agreement’s privacy protections apply to many earlier agreements such as the Passenger Name Records Agreement, various Mutual Legal Assistance Treaties (“MLATs”), and the now defunct Safe Harbour framework. Redress was ensured by US passage of the Judicial Redress Act in February 2016; on January 17 2017, the US Attorney General made clear that the protection included citizens of all EU Member States other than Denmark and the United Kingdom (which were expected to be included in the definition soon). It is not wholly clear whether this is nullified by the Executive Order, or whether the EU remains protected by Section 14 of the Executive Order which requires agencies to act in a manner “consistent with applicable law.” If this situation changes, the EU may withdraw its assent to the Privacy Shield, or decline to extend it beyond the current ‘probationary’ period.

⁶¹ Specifically, the EU will fund researchers (and institutions) from 16 *associated countries* (Iceland, Norway, Albania, Bosnia and Herzegovina, the Former Yugoslav Republic of Macedonia, Montenegro, Serbia, Turkey, Israel, Moldova, Switzerland, Faroe Islands,

However, there is currently no jointly agreed mechanism is currently in place for co-funding Horizon 2020 research and innovation projects, although US participants in projects under the Horizon 2020 Health, Demographic Change and Wellbeing Societal Challenge are automatically eligible for funding and European researchers are also eligible for funding in US NIH projects. It is conceivable that similar reciprocity arrangements could be negotiated with respect to other pillars of the H2020 programme and US counterpart programmes or agencies⁶².

Ukraine, Tunisia, Georgia and Armenia) and 130 *developing countries*. Additionally, researchers from anywhere in the world can be funded to work in Europe through the European Research Council or the Marie Skłodowska-Curie actions.

⁶² See e.g. European Commission (2012) "Enhancing and focusing EU international cooperation in research and innovation: A strategic approach" Communication COM(2012) 497 final at:

https://ec.europa.eu/research/iscp/pdf/policy/com_2012_497_communication_from_commission_to_inst_en.pdf.

5. Conclusions and Outlook

This report outlines specific policy challenges for collaboration between US and EU researchers. We found that there is very fertile ground for collaboration, and it will be important to develop this further to overcome the artificial barriers created by different use of terms (e.g. 5G according to 3GPPP in Europe and “Advanced Wireless” in USA) and to harness the associated productive differences in perspective. The same applies to the ‘natural experiment’ created by different legislative approaches (e.g. privacy as fundamental right, or as economic right that is tradable) and instantiations of community-related concepts.

We found that the differences between US and European values, approaches and available evidence are relevant and provide an opportunity to jointly develop ICT that may serve the global market and to transfer useful aspects of digital community formation between the US and the EU. ICT is associated with a range of global industry sectors and entities; the many layers in the value chain from the chip to national and global ICT services – and beyond into the application and regulatory layers - require innovation on the fundamental technical level, the level of innovative services and the organizational and business model levels as well.

By grounding policies in a solid understanding of acting in a global market, more opportunities will arise for collaboration amongst EU and US researchers.

6. References

1. *How to Understand the EU-U.S. Digital Divide*. **Downes, L.** 2015, Harvard Business Review. <https://hbr.org/2015/10/how-to-understand-the-eu-u-s-digital-divide>.
2. **Crawford, S. und Stott, B.** *Be Careful What You Wish For: Why Europe Should Avoid the Mistakes of US Internet Access Policy*. s.l.: Stiftung neue Verantwortung, 2015. Policy Brief. http://www.stiftung-nv.de/sites/default/files/broadband.eu_.usa__0.pdf.
3. **Yoo, C.S.** *U.S. vs. European Broadband Deployment: What Do the Data Say?* s.l. : UPenn, 2014. Research Paper No. 14-35. <https://ssrn.com/abstract=2510854>.
4. **Marcus, S., et al.** *Entertainment x. 0 to boost broadband deployment*. 2013. European Parliament, ITRE Committee. <http://www.europarl.europa.eu/document/activities/cont/201309/20130926ATT71942/20130926ATT71942EN.pdf>.
5. **Granovetter, M.S.** The strength of weak ties. *American Journal of Sociology*. 1973, Bd. 78, 6, S. 1360-1380.