Policy issues affecting EU/US ICT development collaboration

PICASSO Policy White Paper

White Paper with a focus on recommendations for specific high potential ICT policy initiatives in the EU-US Dialogue

Authors: Maarten Botterman, Jonathan Cave, *GNKS Consult BV – The Netherlands*

ICT Policy, Research and Innovation for a Smart Society

May 2018

www.picasso-project.eu

PICASSO has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement N° 687874.

Thanks

Thanks go out to all who participated in the debate at the 2017 PICASSO workshop on 19 and 20 June 2017 and the various PICASSO Webinars. Special thanks go out to the PICASSO colleagues from the 5G networks, Big Data and IoT/CPS Expert Groups who contributed from the specific perspective of their expertise.

Disclaimer

PICASSO has been financed with support from the European Commission.

Foreword

On January 1st, 2016, the project PICASSO was launched with two aims: (1) to reinforce EU-US collaboration in ICT research and innovation focusing on pre-competitive research in key enabling technologies related to societal challenges - 5G Networks, Big Data and the Internet of Things/Cyber Physical Systems; and (2) to support EU-US ICT policy dialogue related to these domains with contributions related to e.g. privacy, security, internet governance, interoperability and ethics.

PICASSO is oriented to industrial perspectives and provides a forum for ICT communities. It is built around a group of 24 EU and US specialists, organised into the three technology-oriented ICT Expert Groups and an ICT Policy Expert Group and working closely together to identify policy gaps in or related to the technology domains and to recommend measures to stimulate policy dialogue. This synergy among experts in ICT policies and in the three ICT technology areas is a unique feature of PICASSO.

This paper brings together insights relating to the reciprocal relation between policy and the further development, and thus R&I collaboration on development, of 5G networks; Big Data; and IoT/CPS. Overall, it is no longer contentious or even necessary to point out that ICTs have already assumed both enabling and shaping roles in society. Digital services are rapidly becoming the norm; many of these services are already being taken for granted (except when they fail)– ranging from traffic lights that react to real time traffic flows, to indoor climate systems that note our presence and patterns of use of the space. It is also clear that developments are increasingly driven by Communities, which are not always confined within borders, let alone jurisdictions *per se*. Because we have now reached a threshold where the importance of international collaboration, and the sensitivities of people to issues arising in or transformed by these disruptive technologies, and because significant regulatory and policy measures are in prospect or in effect, it seemed appropriate to take a forward look from the policy perspective. It is in that understanding we developed a modest set of strategic proposals.

Our thanks go out to all those who contributed by their active participation in our meetings to our understanding of the policy issues in the EU and the USA especially as they relate to the three PICASSO domains. We could not have done this without them.

Please feel free to share your thoughts via email to maarten@gnksconsult.com.
Looking forward to engaging with you all,

Best regards

Maarten Botterman
Chairman Policy Expert Group
PICASSO project

Dave Farber
Co-Chair Policy Expert Group
PICASSO project

Content list

Executive Summary

This paper brings together insights relating to the reciprocal relation between policy and the further development, and thus R&I collaboration on development, of 5G networks; Big Data; and IoT/CPS. Overall, it is no longer contentious or even necessary to point out that ICTs have already assumed both enabling and shaping roles in society. Digital services are rapidly becoming the norm; many of these services are already being taken for granted (except when they fail)– ranging from traffic lights that react to real time traffic flows, to indoor climate systems that note our presence and patterns of use of the space. It is also clear that developments are increasingly driven by Communities, which are not always confined within borders, let alone jurisdictions *per se*. Because we have now reached a threshold where the importance of international collaboration, and the sensitivities of people to issues arising in or transformed by these disruptive technologies, and because significant regulatory and policy measures are in prospect or in effect, it seemed appropriate to take a forward look from the policy perspective. It is in that understanding we developed a modest set of strategic proposals.

These are:

1. *Privacy*: Solutions need to be found to allow services to develop that respect (European and US) privacy and data protection frameworks and – where appropriate – challenge their provisions. This will require policy collaboration that is looking forward to joint and sustainable solutions aimed at ensuring an even higher level goal than preserving privacy: that of preserving "human dignity" in a digital age, ensuring that we can still live as humans in our digital environment
2. *Security*: Recognising basic security is key to whatever we want to ensure: set up joint EU/US research collaboration to develop biologically inspired security. With IoT and underlying interconnections, there's a significant risk with IoT devices providing a back door to enterprise systems and data. Using biological constructs (in particular those relating to immune responses and contagion), we may be able identify attacks before they become widespread and respond in a proportionate and dynamic fashion by directing resources to the appropriate area.
3. *Standards*: Stimulate participation of sponsored research and innovation in global (IETF, ITU, IEEE etc.) rather than focus on regional standardisation platforms alone, for EU/US collaboration.
4. *Spectrum*: Set up joint EU/US research collaboration on developing agility in spectrum allocation and management to ensure that ubiquitous connectivity enabling digital services to work becomes possible, not being held back by (slow and ineffective) spectrum allocation negotiations.
5. *Communities*: Support exchange of good practice experience between Communities in EU and US; many societal challenges are common to both regions and different types of communities and the potential of many solutions that have already been devised for adaptation elsewhere and optimisation *in situ* remain under-explored.

1. Introduction

This paper, and the PICASSO project more generally, focusses on opportunities for ICT Research and Innovation (R&I) collaboration between the EU and the US, particularly as they relate to the development of 5G networks, Big Data, and Internet of Things (Cyber-Physical Systems, further: IoT/CPS). Much of this is driven by and concerns purely scientific and technological issues – either in themselves or as they affect technology applications. However, an important horizontal complement arises from the interactions between R&I and policy; many important policy issues relate to societal challenges and are affected by technology developments, which is in turn influenced by policy concerns and the constraints arising from e.g. regulation. Much has been written about the generalities of policy-technology interactions; in the abstract, in the EU and US contexts and globally. Our focus is narrower. The opportunities for collaboration arise from a number of factors.

Case for collaboration

The primary drive comes from EU-US differences in the environment within which technologies are developed and applied. These are visible in:

- legal frameworks and instruments;
- regulatory contexts, corpus of regulations and regulatory authorities;
- structure, modalities and orientation of R&I support and other scientific and economic policies;
- the ways common or overlapping policy concerns are understood;
- maturity and sectoral structures an conduct and performance of commercial development; and
- the interests, instruments and capabilities of financial systems.

These differences create opportunities for fruitful collaboration in several ways. First, variation creates 'natural experiments'. If properly mapped and used to structure a comparative analysis, it becomes possible to:

- Compare the outcomes of different approaches in similar contexts and *vice versa* in order to assess the generalisability of findings or identify otherwise-hidden prerequisites for success or sources of risk;
- Link the form that specific developments take to antecedent developments (history) and the broader economic, policy, cultural and scientific environment; and
- Measure and analyse features of the R&I system itself such as the form, structure and performance of collaborations within and among the scientific, engineering, commercial and public sectors, the flows and modularity of knowledge, the types of data that are collected and how they are processed and used, the services provided by and to the R&I community, the form, extent and quality of intellectual property rights (and the protected IP itself), etc.

These natural experiments allow us to identify common lessons, a second collaborative benefit arises from the potential for realigning the differences directly (through policy) or by the creation of mechanisms to allow a greater degree of self-selection or sorting. In other words, instead of a future in which technological approaches and their economic and policy reflections converge, collaborative R&I can lead to a future in which the EU and the US remain different, but with a greater degree of complementarity to realise comparative advantages. Such differences are not necessarily good or bad – they may serve all or specific domain, sector, role-based or geographic interests. They may even be inefficient, with the wrong kind of specialisation. This applies as well to the cross-linking of policy and technology. For example,

- Ostensibly technology-neutral privacy policies may be shaped by differences of interpretation linked to specific technologies (e.g. Big Data) and leading to avoidable conflicts between EU and US legal requirements applying to their shared information space;
- Security policies applied to a specific technology (say 5G) may distort its development relative to other technologies;
- Standards developed 'above the technology layer' – e.g. data interchange standards or ontologies – may not fully take account of the potential of technology to provide alternative means of interoperability or even to dispense with the need for levels of data interchange that raise privacy or security concerns (for instance, low-cost, simple exchange of sensor data in IoT networks); and
- Spectrum allocated to meet the needs of high-priority *technologies* may starve others of resources they need to develop high-priority *capabilities* where most needed (therefore, while a wide range of resources may be available in the more densely populated areas, this may not be the case in less dense communities that are less dense – see also the history of spread of broadband).

Beyond these specifics, mutual awareness of issues and approaches can create incentives for greater and deeper policy evaluation and change; this awareness is a perturbations that exposes deeper connections and structures.

Of course, these arguments for international collaboration are not limited to ICT R&I. But the potentially global nature of technology and the mixture of public, higher education and commercial players involved do create a special connection as regards ICT R&I and policy. Due in part to different histories of public participation in science and technology, there are institutionalised differences in R&I policies, especially as regards the amounts, modalities and governance of science and technology funding. There are also highly-visible difference in the linkages among administration, business and civil society (ABC) institutions in supporting R&I, setting its agenda, carrying out its activities and developing and using solutions based on its outputs. Behind these differences lie complex variations in the balance of power between different drivers of R&I collaboration e.g. policy objectives, market forces, curiosity and societal problems.

These all culminate in differences between the EU and the US as regards framework conditions for:

- the appliance of science - including levels of commitment to better regulation[1] and evidence-based policy and the extent to which market competition is based on features, novelty or performance; and
- multistakeholder collaboration among disciplines and among ABC institutions via which they exchange e.g. money, information[2], models, network access, policymaking, marketing activities.

Most-relevant issues

The following Table lists policy-relevant considerations from the PICASSO policy briefs.

	5G	*Big Data*	*IoT/CPS*
Privacy	Tracking everything	Data/algorithm ethics	Ownership and control
Security	Scale, multi-domain	Complexity, known unknowns	Virtual/physical
Standards	Improve existing	Data types, processing	Interoperability
Spectrum	Access, coexistence	Latency spectrum, management	Low volume ubiquity
Digital communities	Ensuring access	Benefit community, protect individual	Enabling communities to adopt IoT where useful
General policy	++	+++	++++
R&I collaboration	++	++++	+++

The following chapter discusses the privacy, security, standards and spectrum domains; main issues, policy context and links with PICASSO technology areas. Chapter 3 focuses on future trends that we regard as particularly significant, especially the security area. As communities are becoming increasingly "digital" and driving change, we adopt "digital communities" perspectives where relevant. The final chapter builds on the conclusions of each of the policy area discussions that lead to recognition of common themes, overall conclusions and proposals for strategic initiatives.

2. Policy challenges for ICT R&I collaboration

Whereas the focus of PICASSO is on ICT R&I, it is recognised that R&I is guided by policy, as in terms of what is desired, from a policy perspective, and what not. The primary policy areas that we focus on, in relation to R&I collaboration in the fields of 5G networks (or, at the US side: Advanced Wireless Communications); Big Data; and Internet of Things (focus on Cyberphysical systems) are discussed below:

- Privacy & data protection
- ICT security
- ICT standards
- Spectrum

Privacy & Data protection

Solutions need to be found to allow services to develop that respect (European and US) privacy and data protection frameworks and – where appropriate – challenge their provisions. This will require policy collaboration that is looking forward to joint and sustainable solutions aimed at ensuring an even higher level goal than preserving privacy: that of preserving "human dignity" in a digital age, ensuring that we can still live as humans in our digital environment

Context

The 'headline developments' in the policy context are connected to important laws in the EU (e.g. General Data Privacy Regulation and the e-Privacy Directive) and the US (Clarifying Lawful Use of Overseas Data (CLOUD) and the proposed email Privacy Acts). While it is too soon to analyse their consequences, these initiatives have the potential profoundly to change the environment within which personal data are collected, processed and shared across borders and between government, industry and research entities[3].

Briefly, CLOUD allows the US Government to form agreements with qualifying foreign governments that would in effect give access to data held by companies regardless of where the data are stored. This potentially weakens some existing protections[4] and concepts of territoriality. On 17/04/2018, CLOUD was mirrored by a European Commission proposal[5] to give EU Member State law enforcement and judicial authorities access, directly from services providers, to electronic evidence held inside or outside of the European Union.

On the other side, GDPR gives people wide-reaching powers to control their data and threatens data controllers who fail to respect these powers with steep fines (up to €20 million or 4% of global turnover). In principle, those who use US-based cloud services to provide end-user services could be liable for such fines if they (or their providers) surrender customers' data in this way, even though they may not know about the request. The basis of the GDPR protections can be linked to the data processing principles laid out in Article 5:

GDPR Principles:

- Fair and lawful - personal data must be processed lawfully, fairly and transparently
- Purpose limitation - personal data must be collected for specific explicit and legitimate purposes
- Data minimisation - personal data must be adequate, relevant and limited to what is necessary
- Accuracy - personal data must be accurate and kept up to date
- Storage limitation - personal data must be kept in a form that permits identification of data subjects for no longer than necessary
- Integrity and confidentiality - personal data must be processed in ways that ensure appropriate security
- Accountability – the personal data controller is responsible for compliance with these principles

The potential consequences for PICASSO may be political (mutual access requests from other countries), technical (protections aimed at preventing access or facilitating query-based interrogation of databases of personal data) or structural (changing data processing practices or business models of those who deal in data and potentially influencing the quality, price and functionality of data-intensive services and applications).

To put this into context and to draw out its implications, this section briefly reviews major transatlantic privacy differences relevant to the PICASSO domains and some headline implications for R&I collaboration.

Differences in legal status of privacy

Much stimulus for collaborative R&I comes from variations in the legal status of privacy between and within the US and Europe and between privacy and data protection. EU law treats data privacy as a *fundamental right*[6]. The Council of Europe's privacy and data protection Convention[7] articulates protections enshrined in article 8 of the European Convention on Human Rights. This is the only international legally binding instrument dealing with data protection and privacy is seen by international organisations and nations as the quintessential legal provision on the subject. By contrast, the US favours an *economic* right derived explicitly from the Constitution.

EU protections apply to *broad classes* of data processing; the US protects *specific types* of data. GDPR includes a *general Right of Erasure*[8] which data subjects must request; the US *mandates erasure of specific data*[9].

The EU primarily protects citizens against *data privacy* invasion by *private sector actors*; the US Constitution protects citizens against "unreasonable search and seizure" *by government* and recognises 'unenumerated' privacy rights *beyond data protection*. US law *prohibits* certain government actions; the EU *requires government actively to protect rights* against infringements by other actors.

As a result, commercial exploitation of data has flourished in the US. Its negotiators have tended to treat privacy as a trade issue while their EU counterparts see view it much more broadly. Even mutual recognition does not guarantee a starting point for agreement, as indicated by the current CLOUD/GDPR tension.

There are opportunities as well to understand latent preferences for ways to protect data subjects while enabling economic use of their data and to create a "privacy sensitivity taxonomy" showing areas where differences in approach do not inhibit EU-US ICT collaboration.

ICT development impacts

Technology and policy influence each other, especially for PICASSO; its technologies and applications are global, but policies remain primarily local. This creates tensions because:

- Data processing increasingly crosses geographic, legal, organisational and technical borders;
- It is hard to separate data claimed by multiple individuals, firms, governments, etc. as private or secure from those belonging to others or the public;

- It has proven difficult to define, choose, implement and monitor appropriate access and processing by humans, responsible entities or automated systems;
- Privacy in 'unusual' environments (IoT/CPS, 5G networks, clouds) may be seen as new phenomena or not;
- The status of data storage and processing facilities used in cloud computing is internationally contested; and
- The commercial and legal implications for data analytics and encryption have yet to be clarified.

These and similar aspects are bound up with the three PICASSO ICT collaboration areas.

5G networks

5G networks facilitate low-energy and ultra-reliable connections among masses of mobile and fixed sensors and actuators. Eventually, it will be possible to keep tabs on almost any physical object or function, producing masses of data that may be related to natural persons directly or through artificial intelligence, raising privacy concerns beyond anything we have seen today – and thus beyond current policies. New ways of analysing real and imagined concerns are required, leading to new governance approaches and technology-enabled alternatives to existing regulations. These may remain in government hands or evolve towards self-regulation, international law, standards or 'regtech'.

A specific EU/US collaboration opportunity is to ensure that systems reveal to participants the location and flows of data and the available options, linked to existing development of interoperable "data ethics" codes.

Big Data

Big Data raises distinct privacy concerns and collaboration opportunities. 5G changes the operational constraints and granularity of systems that produce and exploit data; Big Data is more horizontally concerned with how such data are processed. The implications go well beyond system-level functions; analytics allows conclusions about peoples' states of mind, preferences, vulnerabilities, etc. Some of the data used would not be considered private or sensitive on their own, but must be re-evaluated when combined with other data; queries and algorithms may allow identification or inferences about sensitive matters (e.g. health). On a practical level, acting on some characteristics visible to Big Data may be prohibited by anti-discrimination rules for decisions affecting individual welfare and freedoms. But if such decisions are based on data that are publicly available or have both legitimate and proscribed uses, it is not obvious that the data privacy can be 'patched' to protect against abuse without blocking desired benefits. Some balance of new forms of consent, *ex post* sanction against abusive behaviour and *ex ante* specification (e.g. of algorithms) is needed; it should be as (technologically) neutral as possible, but not more so. Exploring the potential of technology to create and solve such challenges requires active collaboration, as do new services that do not violate EU and US legal and ethical restrictions.

Ultimately, the R&I and policy challenge is to create a trusted, transparent and portable technology, service and regulatory ecosystem that respects US and EU norms and the national laws that express them and balances the interests of commerce, citizens and the State in a way that is robust to continuing change.

Global adoption of such an ecosystem would expand access to worldwide markets and protect domestic markets from globalisation's adverse privacy impacts that already obstruct trade, law enforcement and other policies.

Uncertainty about privacy and data protection regulatory frameworks can reduce investment in potentially privacy sensitive projects. Former European Data Protection Supervisor (EDPS) Peter Hustinx's advice[10] "If Big Data operators want to be successful, they should … invest in good privacy and data protection, preferably at the design stages of their projects" stresses the importance of soft law[11] and privacy and data protection as a precursor and subject for technology innovation and raises the possibility that privacy protection may be a pre-condition for European (co-)sponsored research (e.g. via Privacy Impact Assessments).

This applies in particular to Big Data; the provenance, processing and use of data may be unknown to those who may bear legal liabilities. An overly 'precautionary' approach can inhibit technology and its positive impacts -

including technical solutions to privacy problems, if it seems safer and cheaper not to tackle privacy issues at all. This potential 'liability overhang' is not limited to regulation; data ethics are receiving increasing attention[12] and the market consequences of ethical failure can be more severe and irreversible than breaking data laws.

The 'make do and mend' approach to privacy challenges gives data subjects responsibility for and control of 'their' data (until it escapes into the open), but this may infeasible or disproportionate; it is not possible to keep up with information "leaked" by applications and websites, created by normal life in smart and shared environments or produced by recombinant processing of multiple data sources. The current rush to comply with GDPR consent requirements provides a case in point; the requests are intrusive and their simultaneity ensures that most will not carefully consider them. Perhaps rights and entitlements should be redrawn, or protection and scrutiny should be assigned to automated artificially intelligent systems. What is clear is that a new system of *ex post* and *ex ante* protections, rights and constraints will require interdisciplinary research combining theoretical, technological, empirical and experimental methods and evidence.

The Internet of Things and Cyberphysical Systems

In PICASSO, the IoT/CPS focus is on large-scale systems and industrial closed-loop systems connected to physical actuators or involving embedded intelligence. Many of these systems are critical to safety, security and other functions that are generally considered distinct from privacy. Of course, not every use of personal data threatens privacy interests; a 'smart' vehicle may monitor occupants' health and contact and automatically rendezvous with paramedics in an emergency, overriding existing instructions. Consent may not be possible, so 'ethically complete contracts' must be devised. Such examples indicate the gulf between privacy interests and data protection. Although GDPR expresses a human right to data protection, it is not easy to translate to IoT/CPS systems, because data cannot possess human rights or be owned by individuals. Indeed, data may be collected without human awareness, scrutiny or effective control and may also simultaneously pertain to groups. It thus appears that rules protecting human rights by giving individuals control over their personal data cannot fully address the challenge. Applying such rules may distort development, and fail adequately to protect personal data or to respect fundamental human privacy rights. Again, the urgently needed research spans technological, commercial, social scientific, legal and ethical domains and must be internationally collaborative, because the US and EU environments embed different conceptions of privacy.

Privacy and data protection conclusions

A framework for ICT collaboration (whether privacy-specific or not) needs fully to reflect our shared democratic and individual rights-based values, expressed globally in Universal Declaration of Human Rights, in Europe by the European Convention on Human Rights, the Lisbon Treaty and the Charter of Fundamental Rights and in the U.S. by the Constitution. To do this, such a framework also needs to reflect the differences that enrich our interaction. These conclusions and recommendations are based on desk research and the project's consultative activities.

Solutions need to be found to allow services to develop that respect (European and US) privacy and data protection frameworks and – where appropriate – challenge their provisions. EU-US cooperation on privacy-relevant matters is complicated and enriched by: the fundamental-economic right divide; the data protection-privacy distinction; and interference between commercial and crime/security objectives.

These themes are developed in more detail in chapter 4.

Security

Recognising basic security is key to whatever we want to ensure: set up joint EU/US research collaboration to develop biologically inspired security. With IoT and underlying interconnections, there's a significant risk with IoT devices providing a back door to enterprise systems and data. Using biological constructs (in particular those relating to immune responses and contagion), we may be able identify attacks before they become widespread and respond in a proportionate and dynamic fashion by directing resources to the appropriate area.

Context

This section considers ICT security issues[13] in relation to EU/US ICT-orientated R&I collaborations in technologies used for future services and international policy affecting security. Of course, such collaboration is complicated by different meanings of "sensitive" or "secure" and national security interests – but it is frivolous to expect any policy that does not provide a measure of security to be followed.

There is no magic cure for the security issues associated with the infrastructures and services on which we increasingly rely. Adverse and highly-publicised events compromise real and imagined security. The increasing complexity of hardware and software[14] offers many opportunities for mischief and sophisticated (but temporary and limited) protection. Even if new systems are 'fixed', older systems will be in use for many years to come.

The Internet provides critical infrastructures for most ICT and data related services; its limitations severely affect security because its decentralisation prevents security measures from being widely applied. The original Internet design was intended to deal with similar issues (not least as a result of its semi-military origins) but these capabilities withered or failed to adapt through underuse. An effective response cannot be limited to tweaks and patches, but should address architecture, design and praxis and the less controllable forces of evolution and disruptive change. Fortunately, many solutions already exist in corners of the Internet or technical publications[15].

Often, the causes and parties responsible for security failures cannot be identified due to legal constraints and a 'security mindset'. Some of this stems from lack of international agreements on issues ranging from ICT-enabled criminality to the use and supply of poorly protected or tested software and hardware. Limits on encryption are one example where legal provisions have not kept pace with the development of the Internet, and where privacy bumps up against divergent national and corporate security objectives.

Whether EU/US collaboration leads to solutions will depend on *competition* (across markets, labs and legislatures) and *conflict* as much as *cooperation*. R&I collaboration must face these realities if it is to work.

Although PICASSO could not address fully all stakeholder concerns, it explored ways to support US/EU R&I collaboration in this area where EU and US interests are somewhat more aligned than in the privacy domain.

The technical situation

The power and importance of computing have increased dramatically; so has its vulnerability, due to increasingly distributed control and access[16] and reliance on unseen, autonomous functions of the infrastructure, and:

- Operating system monocultures and application ecosystems, whose scale and range of users create attractive targets and possibilities for unintended failure[17];
- The complex interdependence and age-range of Internet components, which creates additional systemic, intersystem and intergenerational problems[18];
- Remote (often unscrutinised) software maintenance/upgrades and new forms (e.g. apps[19]) that create an environment favouring widespread, rapid and undetected distribution and triggering of malware; and
- Proliferating IoT devices that lack human attention, respond to remote signals, include old and/or defective software and lack security to prevent vast, coordinated attacks on critical infrastructures and system nodes.

In response, significant research into e.g. processor architectures, Software Defined Networking [20] and Information Centric Networking (ICNs)[21] has helped alleviate the problems, but as yet there has been little integrated work on distributed infrastructures that can guarantee reasonable security in important critical areas such as power, water, financial systems etc. A useful anchor on the policy side is the EU's Network Information Security (NIS) Directive[22] principles, which define a set of top-level outcomes that collectively describe good cyber security for operators of essential services.

The threat is not easing. Consumer-centric products drive behaviours that further compromise security. Such products emphasise speed to market, maximal 'features' and minimal cost. Low entry barriers and market forces discourage security provisions that might slow development, limit feature sets and/or increase cost. Together with limited time-scales for support upgrades, this results in a welter of systems with unsupported, unpatched, compromised or obsolete components. These forgotten (but active) elements are the very definition of "technology debt"[23] and progressively complicate system design and assessment. Unfit components and systems do not always die and potentially superior alternatives may not attract a critical mass of users before their virtues can be demonstrated and captured.

We understand that technological diversity *can* increase security (in an evolutionary way[24]). However, security is emergent and increasingly virtual, human and commercial users are adaptable and "appropriate insecurity" at the micro and meso level is needed to foster greater security at the macro level.

Most past efforts failed in the market; industry, consumers and governments were unwilling to pay for security or unable to understand how to deliver or obtain it. Perhaps past research should be reconsidered in light of the demonstrated urgency of improving critical infrastructure security and reliability. Many solutions have already been invented, but are forgotten or not widely deployed. State-of-the-art Open Standards would help, but incentives are deficient, since greater threats make closed standards and Walled Garden solutions more profitable. Where necessary, new solutions may need to be found, but we also need a better shared understanding of useful security and the assignment and transfer of information and responsibilities. Then a perpetual security arms race can be avoided.

The policy situation

National and regional policy[25] and legal differences stand in the way of optimal[26] ICT security mechanism design. This is closely linked to trust; it is not always useful to seek to minimise risk or to maximise trust.

Policy engages with cyber-security in several ways. Cyber-security policy often results from stakeholder demands for action or seeks to head off corporate actions[27] with other, adverse impacts. In addition, other important policy domains are affected by cyber-security-related concerns, including some critical to EU-US relations.

To frame a useful discussion, it is useful to distinguish: *personal* (privacy and non-commercial aspects of security); *commercial* (protecting proprietary information, system function, reputation and IPR); and *public* (societal, critical infrastructure and essential public service[28]) security.

The conceptual context adopted by the project can be summed up in three principles[29]:

- Cyber-security cannot be minimised – it involves too many interests and components, probability and severity must be balanced and appropriate incentives to discover and manage risk must be ensured;
- Trust cannot be maximised – trust is different for people, machines, systems or information and trust creates vulnerability, so we should seek to distribute trust efficiently and increase it where needed; and
- Trust and security are both real and imagined – some consequences only flow from real risks or failures; others (equally concrete) are due to fear, hence real improvements and greater understanding are needed.

Perhaps the greatest security risk is the attractiveness of easy answers to hard questions. Many of the thorniest cyber-security policy problems stem from inherited ways of thinking inappropriate to the scale, complexity, speed and scope of information exchanges. Their 'solutions' should enable people to identify and fix problems,

but all too often rest on inappropriate assumptions. The following presents examples of how this conflates distinct things, separates issues with important common elements or locks down systems that should evolve.

An annex to this document provides additional perspective on the background to our recommendations, relating to the conceptual underpinnings of security and cybersecurity and the links between security and laws relating to cyber-crime and encryption. This annex also tries to flesh out the 'layered' relationship between technology and policy in the security area by means of a stylised dialogue between technology and policy perspectives. A much more detailed discussion can be found in the Security Policy Brief, in particular as relates to the connection of data security to data processing and integrity.

Underpinning many of the recommendations is a growing recognition that it may be desirable to reconsider the usefulness of liability as a governance mechanism. This reconsideration takes a different form in relation to each of the three PICASSO technological domains.

- For 5G networks, traffic data (including geographical position and links) and data traffic must be protected from tampering and unauthorised access. This is designed in, encouraged by breach notification laws.
- Big Data emphasises secondary use of data; breach notification laws are difficult to apply. If anything, abuse of data (e.g. for malicious, unlawful purposes) may be more subject to protection than access to data itself.
- IoT/CPS devices are often linked in one environment; CPS security relates to the weakest link. An important consideration is responsibility for failing/poorly secured parts; can a "CPS provider" be expected to double-check the quality of individual devices beyond "certification" by the device producer?

Identification primarily enables *personal* liability; it is less effective against security failures due to corporate carelessness or criminality. Gaps in identification system coverage could in theory be filled by a global online universal ID system, but most governments would resist strenuously[30]. Even with such a system, linking a security threat to a person in another jurisdiction is unlikely to lead to effective sanction. We also note that: people are often identified online by numbers; other means of identification (esp. passwords) are becoming unwieldy and insecure; and multiple enrolment can defeat even strong identification systems.

Data and processing integrity and quality

From a technical standpoint, the truth and accuracy of data relate to the connection between data (or processed conclusions) and objective reality. This is not an idle philosophical conundrum; real – and deeply serious - outcomes may result from wholly mistaken beliefs, while partial (but true) information may produce results that serve no-one's interest. Thus, we may need to rethink data 'quality' for a post-truth era.

Solution 1: validation and laws

The benefits of evidence-based policy rest on validated data integrity[31]. Traditionally, this means *de facto* data ownership e.g. authentic sources, certification or liability. Nuanced technical alternatives are being developed (distributed ledgers and smart contracts), but quality assurance may be challenging because validation is localised and contingent rather than absolute. Proper enforcement of data minimisation (amount, time and purpose) could take care of much of this, but may be frustrated by:

- State interests in retaining records for forensic and security purposes; and
- Commercial datavore interests in retaining data in pseudonymised form[32].

The knowledge and ability needed to counter these abuses using legal powers are not evenly spread, making the 'protection' of laws, regulations, treaties etc. unjustifiably and unethically unequal.

Solution 2: rights-based approaches

These range over the trusted and trustless ends of a continuum measuring the power of people to ensure the accuracy of parts of the collective body of data and knowledge. For purely personal data, this is the dominant regulatory model. But even there it is not wholly satisfactory; it may be disproportionately burdensome to find and assess information about rights-holders. This can undermine two important principles:

- Data agency –trusting organisations to hold and use information about a subject in combination with other information that the subject cannot hold in order to further the subject's interests; and
- Data responsibility - giving subjects access and powers of correction[33].

Rights-based approaches for personal or proprietary data often do not scale in amount, types, speed or global reach or complexity[34] and are difficult to multiple subjects or autonomous non-human systems[35].

Solution 3: the 'data home'

Asymmetries of scale and knowledge can be tackled directly to restore data agency and responsibility. Health systems use a 'medical home' – a person with a professional/fiduciary duty to represent patients by collecting and managing information, helping them to understand and contribute to this information and supporting their decision-making. eGovernment systems use an 'authoritative source' - a repository of reliable records that provides a *single* point of visibility, control and correction. It need not literally be a monolithic 'data double' of the real-world person or entity; it could be a federated or networked structure of decentralised but unique data elements, identifying e.g. their location, provenance, permitted uses and security- or privacy-related characteristics. This unambiguous point of control would facilitate impact assessment and could replace fixed and potentially manipulable assignments of rights by explicitly changing processing structures rather than by designing security policies to operate independently of those structures.

The advantages seem powerful. Without a 'data home' it may be impossible to curate 'online identities' or see security failures. Rights to correct or erase cannot insure against informational incoherence, substantially misleading interpretations or abuses by data subjects and those who process their data for fun, policy or profit.

ICT development impacts

Security policies on both sides of the Atlantic affect and are affected by the PICASSO technology areas (as well as new/complementary technologies like biometrics, encryption or Blockchain approaches to security).

Businesses are looking for guidance on "what good practice looks like" and how policy will change. Continuous (and accelerating) changes linked to security complicate the picture and highlight the opportunities for EU-US ICT collaboration. Examples of challenges that this brings include:

- Uncertainty about the bedding in of EU, US and joint legal measures[36];
- Specific challenges related to data location and mobility and thus "applicable jurisdiction";
- Challenges to funding of collaborative research
    - on topics of high near-term commercial importance[37],
    - EU and US tend to fund their own companies and research institutes (though US is more open[38]); and
    - bureaucratic processes, timescales and requirements complicate project 'extension' across the Atlantic.

EU-US collaboration will always be a complement or exception, to local funding. In this:

- Collaboration will be easiest on issues of current, but non-strategic, interest in both the US and the EU;
- The existence of potential (funded) partners may make it easier to fund collaborative than separate research, as evaluators will be able to take additionality into account; and
- Issues of (research and application) security and intellectual property rights will need to be resolved.

Below we consider some specifics relating to the three PICASSO ICT collaboration areas.

5G networks

5G networks will provide differentiated support to vertical industries such as automotive, transportation, industry automation and eHealth. This provides both opportunities and challenges, especially as regards security.

2G to 4G mobile networks were considered relatively safe, providing basic connectivity between a user and up to two operators (home and roaming). Each user's equipment is uniquely identified with a subscriber identification module (SIM) card. This security model will need to change to fit 5G cross-domain networks.

An unprecedented number of devices will be connected to the network; their security capabilities and the consequences of insecurity will vary widely (e.g. IoT devices need much less security than high-speed mobile services). If they are connected to the same network without standards disproportionate to some devices, mandated interoperability and/or additional security at the network level, low cost and security-light devices could be used to compromise the whole network.

Network level architectures and security mechanisms must therefore meet the connectivity and application requirements of different uses and verticals. For example, remote surgery robotics require extremely low-latency and high-reliability connections while factory automation emphasises protecting wireless transmissions from interference. These represent a challenge specific to 5G security design and are unlikely to converge to a one-size-fits all design. In addition, many new services will most likely be provided by multiple operators in one or more domains[39], which creates further security requirements. The security required for some applications (e.g. power grids and traffic control) are too expensive (in cost or performance) for others.

To reduce cost and speed up 5G network deployment and optimisation, hardware and software are increasingly decoupled in network/equipment design[40]. Security shifts from dedicated hardware to software, which is complicated by multiple operators and application providers working on the same hardware (and *vice versa*).

A heterogeneous identity and privacy management mechanism might be needed to serve diverse applications and industries. At the same time, basic connection services and verticals will seek to define the ownership, governance and uses of 5G data flows; this involves personal and proprietary data security[41].

Finally, because 5G is intended to address future demands and business contexts network security design is constrained by cost- and energy-efficiency.

Currently, designers view network slicing (allowing multiple logical networks to be created on top of a shared physical infrastructure) as an important technical component to address these design challenges. It allows differentiated and flexible security as a service, while isolating logical networks for improved security.

In general, the challenge of transforming single-domain into multi-domain networks requires a better understanding of security-sensitivity of systems and the right kind of top-down technical and policy approaches.

Big Data

Big Data, machine learning/artificial intelligence and algorithmic/automated decisions have specific security challenges, but scalability dominates them all. Critical data flow volumes are expected to double every two years. Within the IoT realm alone, these flows are likely to grow into the brontobyte range—10^{27} byes. At the same time, network management will go beyond distributed data centres to million-node networks.

- *Distributed data centre management* involves the 'small worlds' security challenges of any complex system.
- In *million-plus node network management*, most nodes are sensors or actuators doing relatively limited processing or mobile devices, where the complications are exposure to multiple network neighbourhoods, limited observability of critical events and limited control of individual nodes in an oceanic environment.

As networks grow, it is not feasible or appropriate to scale up the network management, security, etc. practices used on smaller networks. Instead, it is likely that we will have to adopt a mix of

- Only managing 'local' interactions;
- Risk-based approaches, which accept higher-than-zero odds of different failure modes;
- Variable geometry, where governance, security information, etc. change with circumstances; and
- Security approaches for strongly emergent[42] problems that use approximate and/or structure-based methods to deal with issues that cannot be anticipated without using infeasibly large quantities of data.

This – in effect –moves security away from system design and closer to real-time uses. It should focus on *efficient*[43] *risk management and allocation* rather than static risk-minimising structures and responsibilities.

Secondary emphasis should be placed on understanding and managing trade-offs between the *probability and severity* of security failures, where data reside and their valuation in terms of business outcomes.

A third objective, is a *learning* approach, balancing management of 'known known' security challenges and clarification of 'known unknowns' – new challenges or opportunities not considered when security policies were designed and implemented. This is not trivial; security protocols can mask unexpected failure signatures.

Security must ensure that data retain their integrity and are secure from unauthorised access and available for authorised use. The Internet does not provide this by design, as spoofing, sniffing and hacking prove every day. This signals a paradigm shift from security as a system property to service level subjective, relational security.

Beyond these data security issues are Big Data specifics; ensuring that analytics are not spoofed, processing retains its integrity and fidelity to the 'real world' and algorithms do not embed bias. These technical matters are at the heart of current data science development.

The Internet of Things and Cyber Physical Systems

Many closed-loop, real-time IoT-enabled cyber-physical systems operate in a business-to-business context but vulnerabilities can arise from anywhere. In such systems, access to information provided by IoT-connected sensors is much simpler and more flexible than in traditional technical systems; IoT connectivity will enable cyber-physical systems of systems, closing the loops from sensors to system operation and user demands and thus improved monitoring, management, resource efficiency, service quality, and safe and reliable operation.

Information security and privacy are made significantly more complex and fragile by connected devices, service orientations and converged IT and operational technology[44]. Cyber-security, privacy and trust are increasingly dominant topics for IoT/CPS (esp. in the US compared to the EU).

The convergence of connectedness and dependence on information allows attacks and accidents to produce undesirable and even catastrophic effects on the physical environment. It's not just a question of securing devices belonging to an organisation or allowed to connect to its networks. Devices that are designed insecurely or lack (secure) mechanisms for detecting and patching insecurities can provide a pool of malware capable of attacking other systems. Moreover cyber-attacks can mask or exacerbate physical attacks and *vice versa*. Thus IoT security is concern for the entire Internet community[45]. The large-scale, closed-loop nature of these systems implies numerous points of vulnerability, dramatically increased by sensors, communication networks, data repositories, analytics engines, actuation devices and human-in-the-loop interfaces.

IoT/CPS provides fruitful grounds and justifies support for collaborative R&I. Many systems cross national boundaries; this creates policy issues and ups the ante in favour of policy alignment. The involvement of different companies, suppliers, operators, etc. in a single IoT-enabled CPS raises issues of data separation, liability, ownership, trust and trustworthiness in technical systems viewed as crucial challenges in the EU and the US.

Security conclusions

Security of ICT devices, data and services is broadly seen as a top priority that needs to be addressed. Without appropriate security, trust in ICT-linked products erodes; this reduces the benefits. A framework for EU/US ICT collaboration needs fully to reflect and integrate: security; privacy; and awareness.

As the security landscape continues to evolve, so will the challenges. Currently, highly capable threat actors are capitalising on prolific black markets for capabilities and information. They will grow as additional devices, services and data sources come online. The growing volumes and flows of data require new technologies and associated procedures and business models to protect user devices, data and systems. Particular attention will

need to be given to adaptive, self-defending, autonomous capabilities. This may require a fairly fundamental rethinking of the meaning of security and the ethos of security policy to more risk-based and evolutionary alternatives. The answer is unlikely to be either an overly-cautious precautionary set of design specifics and prohibitions or an overly-optimistic *laissez-faire* approach. Finding the balance requires international, interdisciplinary and collaborative efforts and an evolving mix of policy, technology and market experiments.

Standards

Stimulate participation of sponsored research and innovation in global (IETF, ITU, IEEE etc.) rather than regional standardisation platforms for EU/US collaboration.

Context

The use of standards in industry and commerce grew in importance with the onset of the Industrial Revolution and its requirements for high-precision machine tools and interchangeable parts. Originally such standards were set within specific sectors; in many ways, this focus continues. However, flows of information cross (or obliterate) sector boundaries. This creates tension between standards highly optimised for specific uses vs. broader application. As a result, three overarching issues stand out:

- The impact of growing ICT-dependence on the complex web of standards in use;
- The significance and importance of standardisation processes; and
- Broader implications e.g. the emergence of horizontal service intermediaries serving many vertical sectors and shared technical, economic and societal spaces using common or complementary standards.

How ICT dynamics affect standards

ICT penetration is often viewed as a *convergence*; if "general purpose" ICTs can be used across sectors, existing standards may need substantial revision or replacement by broad-based or flexible standards. But the implications for standards and their implementations are not simple and the extent of convergence should not be over-emphasised.

Implications of convergence

ICT-driven convergence threatens existing standards because it spans sector boundaries (e.g. aviation, logistics, health care, etc.), societal roles (commerce, science, civil society, administration) and subject domains (e.g. merging transmission protocol and encryption standard-setting). These "crossovers" argue for a networked (as opposed to a federated or hierarchical) structure of standardisation. For concreteness, the following discussion uses as an example ICT convergence across industrial, financial and healthcare sectors.

Standards cannot always be "broadened" to span sectors without changing their essential nature. For instance, *security* concepts behind standards for information exchange in industrial systems may be inappropriate to financial service or healthcare settings. A standard intended to work for all of them may:

- Descend to a minimum level with fragmentation from context-specific supplemental standards and/or technological implementations;
- Be "gold-plated" to a needlessly cumbersome or expensive maximum level, which weakens the perceived advantages of compliance and possibly distorts or limits uptake; or
- Have no clear ranking from least to most restrictive, which may mean that standardisation is abandoned or set to serve the interests of the most powerful businesses, sectors or perspectives affected.

Why should this matter? On the negative side, technological standards to address functional or application level needs may respond to the spread of general–purpose applications by fragmenting in ways that limit further technological convergence. Continuing the above example, incompatible standards for data sharing in industrial, financial and healthcare settings may block deployment of common data storage and analytic solutions and thus inhibit advanced services using all three types of data, as well as global personal data privacy or security solutions.

On the positive side, the challenge of technological convergence could stimulate a shift to functional as opposed to technological standards, defined at the application or service level (e.g. business process standards) to be compatible with basic technological standards for, e.g., security or data exchange. The same challenge may also enhance privacy by inhibiting the merging of data sets into common big data collections open to intrusive, hard-to-audit artificial intelligence-based inference mechanisms. In the same example, this could lead to standards that provide appropriate and negotiable levels of protection for different kinds and uses of data in place of "privacy and security by design" approaches carried out by multidisciplinary teams not used to working together and/or overly prone to seeing purely technological solutions to logical, human or societal problems.

Convergence is not inevitable

Convergence should not be taken for granted. Adding functions to common devices (e.g. smartphones) has not prevented the uptake of other devices with overlapping capabilities. This proliferation of supposedly converged devices and services within user groups (e.g. people who routinely use multiple smartphones) leads to a patchwork of devices linked by their users and users linked by their devices. The "right kind" of standardisation should reflect this inevitable tendency towards overlapping devices, functions and cultures of use.

We therefore need new collaborations to understand the interplay among standards, technologies and applications. Because technologies and markets cross EU-US boundaries even more readily than cultures of use, transatlantic research collaboration seems essential and useful. Working together, EU and US technology and standards development can retain a strong presence in world markets, further stimulate interoperable technologies, services and things and ensure that these developments embed shared values – meaning that law and regulation will not be left to patch up the ethical and societal risks associated with ICT adoption.

Standardisation as a collaborative and competitive activity

Standard-setting and standard development are valuable activities regardless of the standards produced. Killing off old standards (or bodies) may be as valuable as making new ones; as with laws, dense thickets of obsolete or misleading precedents are not helpful.

Standardisation can limit the monopoly power of dominant systems providers[46] or lock in upstream and downstream users (e.g. mobile phone chargers). Standards can also allow regulated hardware/systems providers to stimulate competition in their supply chains, driving down input prices without requiring them to invest in equipment or fall foul of competition regulations.

ICT technologies and services used around the world and across borders are subject to multiple jurisdictions and national standards (such as the layout of power networks, or safety and privacy regulations). Hard and soft innovation continue to accelerate, bringing new technologies, services, business models and service as the result of world-wide R&D, deployment and competition.

Even ICT standards are increasingly global. Telecom wired and wireless networks are geographically limited, so associated standards were originally locally-developed, spreading as service and equipment providers and markets expanded. Internet standards have also been developed in one country in support of national standards and/or legislation, and used later on a global basis, though they are increasingly developed for a global market.

The architecture[47] of standards-making organisations in the telecommunication and IT industry fields has fundamentally changed since the 1980s. The original simple and clear structure where standards development organisations (SDOs) with explicit geographic and subject matter jurisdictions followed slow and well-regulated

processes has evolved into today's loose network of new bodies[48] with diverse and overlapping constituencies and boundaries, which compete in more-or-less commercial global standards markets[49].

In industries without a dominant hardware or OS provider[50] interoperability. In non-information industries objects only need to interoperate in well-defined ways. The Internet requires flexible interoperability, continuity of connection and non-interference with other traffic, which must be enforced through costly regulation if not provided by standardisation or voluntary action.

Re-usable and flexible standards will allow 5G networks, Big Data and IoT/CPS to realise their full beneficial contributions to societal digitisation. Standardisation is needed because their growing speed and scope will exempt an ever-widening range of activities from human intervention, while increasing our dependence. We cannot – and cannot afford to - prevent this evolution from happening. The only way to ensure that these developments meet existing challenges without creating new risks is by understanding the way these systems evolve and using this to establish appropriate architectural principles and design and operational standards.

Standards can be set early or late in the technology life-cycle; why now?

1. *Standards are of critical economic importance*; they help to create compatible products leading to a vast connected "virtual marketplace" within which every product or service forms part of a coherent ecosystem.

This allows more effective and efficient satisfaction of needs and value creation. Markets elicit, aggregate and "price" information through trade interactions; *property rights* give people things to trade. Markets also mix competitive and cooperative interactions. Classically this involves horizontal competition (within a market segment's supply or demand layers) and vertical cooperation (within supply chains and other contractual arrangements) using individually-owned and transferrable property rights.

Markets are transformed by data-intensity; they need far richer architectures of cooperation and competition to identify and implement efficient outcomes while preserving investment and innovation incentives. One aspect is a need for property rights that are neither exclusive nor individually owned. In the information space, this can be seen in "open" alternatives to copyright[51] and in the Open Data, Software, Innovation and Information movements. Standards are perhaps the most concrete expression of this, representing as they do, a collective or shared form of intellectual property right (spread out along the spectrum from closed/proprietary to fully open). They also provide a "language" through which products communicate, extending the power of markets.

2. *Standards enhance competition*, especially within markets.

If markets are to function efficiently, customers need standards to avoid being locked in to vendors. Standards can make it easier to switch suppliers (without having to change other products), enabling competition that drives improvements in quality, price and other important attributes (e.g. privacy, security). Open standards facilitate bottom-up innovation of new composite products and services. Moreover, in two-sided (platform-based) markets standards enhance the joint mobility of buyers and sellers helping to eliminate inefficient lock-in at the platform level. Standards can also enhance competition by allowing developers to focus on value-adding features instead of reinventing basic functionality. Standards often allow products to interoperate while offering superior performance, security or other functionality for competitive advantage.

3. *Standard setting and development processes pull in more reviewers* and facilitate non-market cooperation.

Reviews and collaboration help correct errors, identify and manage security issues and deal with problems arising between as well as within systems, which might not be corrected by competition. The relative stability of interoperable markets can reduce risks of stranded investment in technologies that will not succeed, reducing risks associated with investments in infrastructures and innovation and limiting the excessive inertia and volatility common in markets with strong network effects[52].

4. *Standardisation can help to overcome "frog-boiling"* - emergent problems that are not recognised and dealt with until they have become irreversible.

This reflects the collaborative and multiparty nature of open standardisation and its advantages in dealing with problems that arise in one area or level, affect another and can be efficiently dealt with at a third.

The remainder of this chapter summarises current standards setting and development, its implications for EU and US ICT developers' collaboration and opportunities to stimulate sustainable collaborations.

Standards development in practice

Standardisation at a global level embraces three key principles: openness, consensus and transparency. Specific discussion of current arrangements is provided in the Standards Policy Brief.

- Openness - participation by all interested parties affected by the technical specifications and that standards be available for implementation without significant expense or IP requirements. That is, the process and the standards need to be open to avoid a closed market.
- Consensus - a collaborative decision-making process that does not favour any single stakeholder.
- Transparency - information about technical discussions and decisions is available, archived and identified; information on new standardisation activities is publicly and widely announced; and participation of all relevant categories of interested party is sought

Permissionless innovation

Permissionless innovation allows anyone to create new things on top of existing constructs. Most new Internet applications come from grass-roots innovation, start-ups and research labs, without permits, new network construction or commercial negotiation with other parties. The easier we make innovation, the faster it finds its way to users and the market. In fact, "open development" may need to become a standard in itself for R&I.

There are trade-offs between the advantages of permissioned and permissionless innovation.

- Timing – the value of innovation may rest on 'legacy IP.' This can encourage innovation, depending on whether use of legacy IP is sought before or after innovations are developed. If permission must be sought in advance the returns to 'fundamental' innovation may be protected[53]. If IP options are used (negotiated after innovations), exploitation and development rights may be more equitably and efficiently assigned.
- Market vs public value - if *exclusive* rights to innovations can be acquired by legacy rights-holders, public value may be reduced if incumbents are willing and able to pay more than new entrants for such rights because they: may already have established market positions; can internalise externalities of negotiating rights to new and existing IP; and stand to gain more because such rights increase market power and hence profit compared to more competitive outcomes. On the other hand, this greater benefit might encourage them to invest more in innovation than rivals might and may increase value not captured in market revenues.
- Other externalities – permissionless innovators may have different sensitivities to and ability to influence privacy, security and other non-market impacts, especially if the entity granting permission is a) the one responsible for those impacts or b) a regulator willing and able to enforce mitigation.

Open Standards

The same considerations of open (e.g. permissionless) vs closed (e.g. permissioned) models apply to standards, when considered as shared (rather than exclusive) IP. Open standards encourage efficiency-enhancing competition within markets and in developing new markets and standards[54]; they lead to more societal return, but less commercial return. This Prisoners' Dilemma for industry has led to self-regulation to promote open standards, e.g. as reflected in the five principles of the OpenStand paradigm:

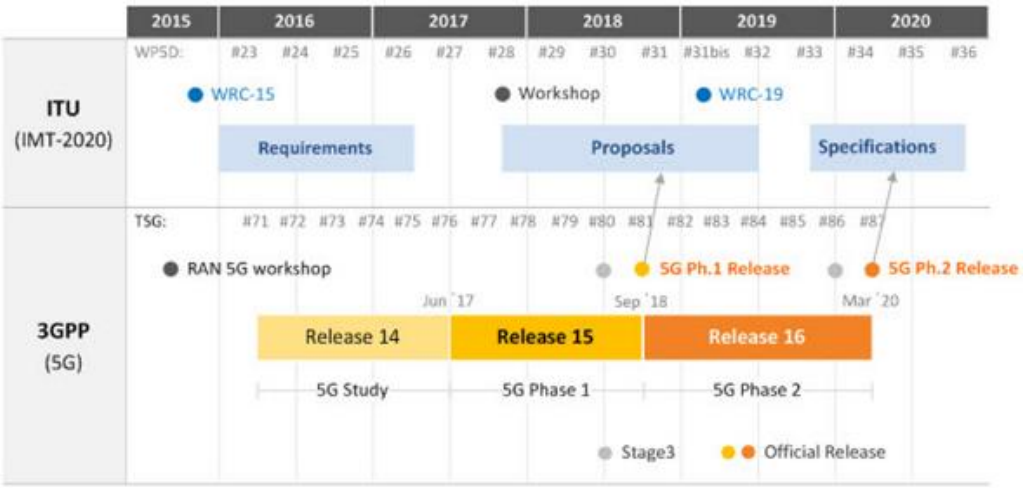
- co-operation (respecting different organisations' roles)
- collective empowerment[55]
- availability[56]
- adherence to fundamental principles[57]
- voluntary adoption

ICT development impacts

5G networks

ITU's Radio Communication Sector established the roadmap for the development of 5G mobile and the term that will apply to it: "IMT - 2020" on October 26 - 30, 2015. All the submitted proposals will be evaluated by independent external evaluation groups. The definition of the new radio interfaces to be included in "IMT - 2020" will take place from 2018 - 2020.

3GPP set its roadmap and timeline of 5G standardisation in 2015. The target is to submit initial technology submission to ITU-R WP5D meeting #32, June 2019 and detailed specification submission to ITU-R WP5D meeting #36, October 2020. From the second half of 2017 to September 2018, 3GPP will start to work on "phase 1" 5G specification under release 15. The target is to address a more urgent subset of the commercial needs. It will focus on deploying lower frequency bands, as the higher frequency bands need to be approved in WRC-19. From September 2018 to March 2020, 3GPP will work on "phase 2" 5G specification under release 16. It aims for the IMT 2020 submission and to address all identified use cases & requirements.



Source: IEEE

The IEEE established a 5G initiative on December 2016. Currently it is working on its roadmap that it will announce in the autumn of 2018. On an architectural level, the requirements are to virtualise the entire Radio Access Network (RAN) and Core Network (CN) infrastructure so that they can be as easy to deploy and scale as the data centres and other cloud infrastructure that have revolutionised the IT industry in the last few years. The main difference is that existing IT infrastructure concentrates on storage and compute virtualisation.

IETF will extend this to also support network virtualisation, which has not been previously done in the IT industry, as only IETF has the mandate to change the IP protocols to support network virtualisation. An example of the standardisation efforts starting in IETF related to virtualisation is the specification of the Service Function Chaining (SFC). SFC will allow dynamically linking of all the virtualised components of the 5G architecture, such as the base station, serving gateway and packet data gateway into one path. This is required because unlike previous generations, 5G processing components—called Virtual Network Functions (VNFs)—will be dynamically created in a cloud-like environment and so need to be dynamically linked together. The timeline for development and deployment is not clear.

In most cases it is expected that 5G applications will run over the HTTP protocol as nearly all applications that connect to the internet in a secure manner do today, or better yet on the emerging secure HTTPS protocol. Here again, important work needs to be done in improving the HTTPS protocol so it runs efficiently, easily and more securely in mobile environments.

Big Data

Big data promises to change the way we do business, management and science. It entails the scalable processing of huge amounts of data to draw conclusions and inferences on physical and technical phenomena, systems and human behaviours. A variety of data volumes, sources and types could qualify as big data for different intended applications. For example, 1 TB of data would be considered small for gene sequencing (about 10 genomes), but huge when collecting sensor measurements in a field. Additionally, there are many data types, data storage models, data query languages, data access methods (accessing stored data offline or in streaming mode before they are stored), data analysis and visualisation methods. In addition, many of the most promising applications involve combining many types of data and/or analysing essentially unstructured assemblages.

In view of this, there is broad consensus that, if we are to obtain the full potential from big data, outside of the realm of scientific research (where data intensive processing has been performed since many decades), the time has come for standardisation. Standardisation in big data aims to provide a common terminology, recommendations and requirements for data collection, visualisation, analysis and storage. From several viewpoints standardisation is already happening: definition of large objects (LOBs); data storage models (XML, JSON, BSON); distributed query and analysis (e.g. map-reduce algorithms); big data compression (Anamorphic Stretch Transform); data query languages (SQL, SPARQL, XQuery); and data analysis and visualisation languages (R). Indeed, each of the components of big data processing can be standardised processes as needed.

There remain significant challenges viewing the Big Data ecosystem as a whole or in specific applications.

As regards the general picture, many Big Data solutions claim to improve data processing and analysis capacities in all respects, but there is no unified evaluation standard or benchmark to balance the computing efficiency of Big Data with rigorous mathematical methods. A recent survey[58] urges development of evaluation systems and standards for data quality and data computing efficiency.

In addition, individual domains require their own standards; for example, Herbert et al.[59] proposed a framework called BIOAJAX to standardise biological data to facilitate further computation and improve search quality.

Standardisation bodies include the Cloud Security Alliance Big Data working group, the NIST public working group on Big Data and ISO/IEC (International Organisation for Standardisation and International Electrotechnical Commission). A small survey[60] on standardisation in Big Data has been performed and in 2015 NIST issued a seven-volume Big Data Interoperability Framework, which includes a Standards Roadmap. ISO/IEC began standardisation work in 2016 and produced a range of standards[61].

In 2013 the ITU (International Telecommunication Union) first issued ITU-T Technology Watch Report “Big Data: Big Today, Normal Tomorrow” and in 2015 the first recommendation “ITU-T Y.3600 Big Data – Cloud Computing Based Requirements and Capabilities”. This standard details the requirements, capabilities and uses of cloud-based Big Data, with an eye toward ensuring that its benefits can be achieved on a global scale. It also outlines how cloud computing systems can be leveraged to provide Big Data services. The IEEE is also involved in standardisation via the IEEE Big Data Initiative, which aims to advance technologies that support, make sense of and preserve the security of the growing mountains of data.

The BDVA (Big Data Value Association[62]) is involved in initiatives to produce value from data that recognise the role of standards. It is the private counterpart to European Commission's Big Data Value Public-Private Partnership, which seeks to create a functional Data Market and Data Economy in Europe to give Europe a leading role in the global Big Data market.

Recently investigations have begun on the use of artificial intelligence techniques in Big Data visualisation, interpretation and use. The combined efforts in Big Data and in Artificial Intelligence have come to the attention of policy fora and can be expected to be the subject of future standardisation or regulation policies.

These examples demonstrate the growing availability of initiatives related to Big Data standardisation. However, a joint EU-US standardisation coordination effort working on this subject could fill an existing large gap and bring

both regions to the technological forefront, particularly where such standardisation may facilitate or conflict with other elements of policy e.g. privacy, IPR and security.

Internet of Things/Cyber Physical Systems

Interoperability is the preeminent challenge to IoT/CPS in all of the application domains that we've analysed. While interoperability is often regarded as a technological challenge, standardisation is an important building block. This is reinforced by the facts that a lack of interoperability is seen as a barrier for future IoT/CPS systems.

Production systems consist of thousands of (often proprietary) hardware and cyber components by a large number of manufacturers that should be integrated with each other and with legacy systems. This makes interoperability a key prerequisite for novel ICT technologies that will require global real-time access to all devices at the field and for automation levels.

Challenges such as plug-and-play reconfiguration, zero-configuration integration of automation systems, real-time analytics and optimisation, monitoring and diagnostics and remote update depend on the interoperability of technical systems. Companies must move away from proprietary solutions towards more open and standardised interfaces and platforms.

The production of Industry 4.0 compatible automation products is seen as an opportunity for harmonisation within the industry; the expectation is that the cloud and the IoT will be used to connect smart components.

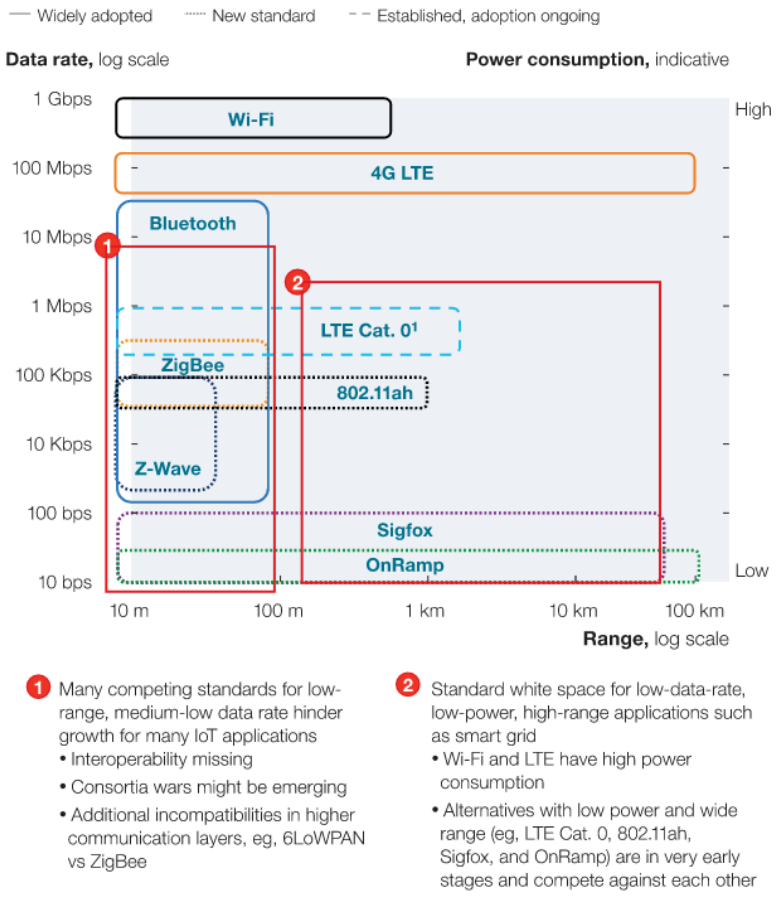


Figure 1: IoT standardisation[63]

Joint work on international standards and interoperability may be more feasible than close-to-market collaboration since it requires companies to release less sensitive IPR. The PICASSO Opportunity Report (D2.2) used interviews and review of recently released strategic documents to conclude that (industry-driven) standardisation activities will gain importance in the near future (especially in the quickly evolving IoT landscape)

and that international collaboration will be essential to ensure interoperability and successful integration of future large-scale infrastructures. Collaborative actions might focus on pre-competitive R&I with a low-TRL (Technology Readiness Level) or other efforts that do not require access to sensitive company-internal IP.

Many organisations are involved, in diverse ways and standards and activities are "cross-informed" as there is a big drive towards making things work together – more on some platforms (like the AIOTI in Europe) than others.[64]

Standards Conclusions

Standardisation processes have changed dramatically, but struggle to keep pace with the evolution of both collaborative R&I and the application of its fruits. Convergence onto platforms, devices, protocols, etc. is not so strong as to enable us to hope for a similarly-converged single set of standards or standardisation processes, but interconnectedness (beneficially and intentionally or otherwise) is sufficiently pervasive and important that we cannot hope to create a unified and federated standardisation alternative. Even traditional 'stovepipes' (e.g. technology domains or economic sectors) will not contain this growth. The messy mix of standards at different levels (e.g. data, logical, service, hardware) and for different purposes will continue, which is precisely why: joint research on the nature of standardisation is required (since it is not simply a design or control problem) and the standardisation implications of technological R&I must be better understood when it is being conducted, which requires interdisciplinary and international collaboration. Globalisation also plays a role; nationally oriented standardisation is only useful when aligned with international developments, and secular interests can threaten the coherence of standardisation and technology development.

Possible ways forward towards better collaboration would include on a general level:

- Relinquishing the hope that national policies will provide "competitiveness by exclusion";
- Better use of IP for society and economy to benefit from new insights; and
- Specifically for EU/US collaboration, considering both EU and US values in order to trade effectively and to become relevant to multiple regions of the world.

5G developments are already well-advanced and diverse across the world. Specifically much 5G development is considered "commercial" in the US, but public support for collaborative R&I is still available in Europe. [This may be partially down to different definitions; there is a big overlap between US research on Advanced Wireless Broadband and EU supported research on "5G"].

Big data goes global and needs to have global solutions, as well as adaptations to local laws. GDPR is an important driver in the generation of standards towards ensuring privacy of individuals, but ethical challenges remains, especially with regard to AI.

IoT devices are used all over the world and data are exchanged between objects and aggregates in big data sets – sometimes by purpose-built IoT ecosystems, at other times through big data techniques.

At this point our conclusion is that also for EU/US collaboration it mostly makes sense to stimulate participation of sponsored research and innovation in global standardisation platforms, such as IETF, ITU, IEEE etc., rather than at regional level.

Our second conclusion is that standards should aim at setting a minimal responsible level, and not less than that. This is because every application of standards will also need to adapt to the specific requirements of that application.

Spectrum

Set up joint EU/US research collaboration on developing agility in spectrum allocation and management to ensure that ubiquitous connectivity enabling digital services to work becomes possible, not being held back by (slow and ineffective) spectrum allocation negotiations.

Context

The PICASSO technological domains[65] rely on connectivity, increasingly via wireless means. Users are growing accustomed to similar services on the move and in fixed environments (ubiquitous connectivity). In much of today's fixed location connectivity, physical infrastructures (e.g. copper, cable) are supplemented or replaced by radio connections, which may easier and cheaper to install, maintain, extend and update. PICASSO-relevant developments (including) all rely on connectivity that depends on various forms of radio and fixed communications based on new and innovative forms of wireless communication.

Part of the resulting demand for spectrum can be met by using higher frequencies. The rest must be accommodated by more efficient use of current spectral bands. TV white space[66] is one spectral domain that can be more efficiently exploited by Dynamic Spectrum Access (DSA) techniques. These facilitate flexible and controlled spectrum use by giving individual users, uses and devices just the connectivity they need, when and where they need it, giving the impression of almost infinitely wide channels; when one use ends, the spectrum is available for another. Particular frequencies may be used for IoT, M2M, voice etc. over a short space of time.

Until now, most areas have relied on exclusive spectrum access rights, obtaining flexibility by allowing trade or recontracting. This approach is already becoming less prevalent, but DSA may not take over as a new dominant model; while its use is expected to grow steadily over the next few years, it is unrealistic to expect all spectrum governance to convert to DSA in a single step – or for DSA to provide the best long-term solution in all cases. DSA and conventional spectrum allocation methods will coexist for the foreseeable future, and DSA itself may operate in several modes. In some cases, entirely unregulated access to portions of the spectrum may be more efficient, facilitating experimentation and uses where the costs of DSA exceed the efficiency gains. The range of DSA approaches is indicated in the following Figure, adapted from Zhao and Sadler 2006.

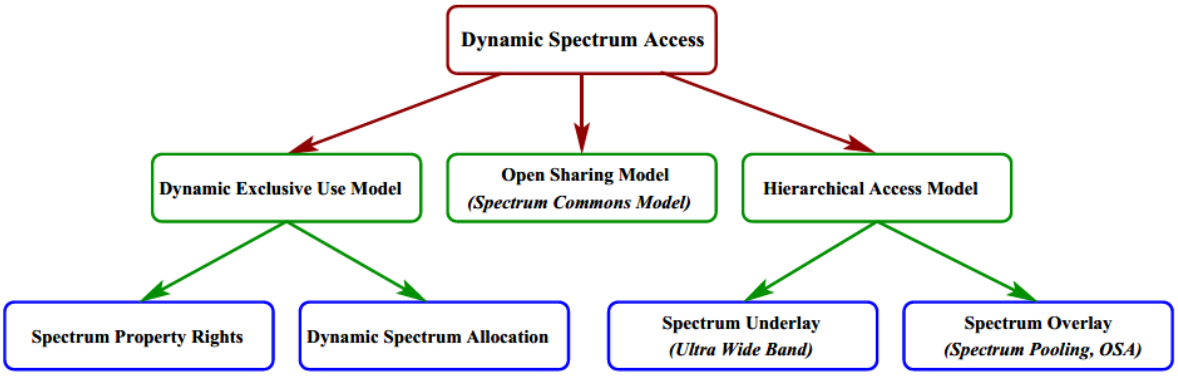


Figure 2: varieties of DSA approaches

We foresee three main overlaps between spectrum policy and R&I with a transatlantic footprint, from the needs:

- To adjust spectrum allocation and management polices to cope with technological development. Many of these policies are – and will remain - internationally coordinated[67];
- To anticipate and coordinate changes to research programs and outputs arising from spectrum policy, which implicitly influences[68] the eventual 'winners' and 'losers' of R&I. These outcomes have national and international importance; nationally-based policies should not unduly inhibit technology R&I; and

- To ensure, through policy and other means, availability of spectral resources for scientific purposes, which is both a general objective and one specific to collaborative R&I in PICASSO domains.

We briefly discuss each of these before considering specific elements relating to the three PICASSO domains.

Challenges to existing spectrum policies

Interactions among spectrum policy and technology development challenge existing spectrum management rules (esp. on licensing and access) and require research to rebalance 3 styles of spectrum access control:

- *Prohibition* – banning or excluding[69] access to or use of specific spectral resources by designated users, uses or technologies, with the default being to allow access or use under common framework conditions[70];
- *Permission* – allowing access or use with the default being not to permit such access;
- *Trade* – creating a system of tradeable spectrum access or use rights[71]; and
- *Negotiation* between spectrum creators, owners or managers and those who need access or usage rights.

The impacts of such arrangements change over time. The immediate effects are to enable or inhibit the identification and implementation of efficient use of spectral resources and thus to service production and distribution. In the longer term, they create incentives to develop and deploy new technologies, services and business models along any value chain that runs in part over the electromagnetic spectrum.

Implications for radio technology and service R&I

The potential availability and price of spectrum access determines whether technologies are developed, deployed, licensed, etc. The PICASSO technologies require adjustments to conventional spectrum allocation and management policies to cope with new features, each of which poses its own research challenges.

- *User demands* – users of capabilities and services associated with PICASSO technologies need different service continuity, quality, privacy, security etc. These are likely also to vary among e.g. mobile users, Autonomous Vehicles and IoT devices and smart systems.
- *Uses* – spectrum use across these domains involves different (and fixed, varying or agile): access and management technologies; time-patterns[72]; frequencies; bandwidth; access; location etc.
- *Property rights and (re)assignment mechanisms* – the system of rights must conform to the contending needs of different spectrum users and uses and to business models and could involve licensed, unlicensed and overlay/underlay spectrum, and requirements to monitor and make available unused spectrum.
- *Physical infrastructure* – users may require (or have) different dedicated physical infrastructures and links to wireline/fibre networks. Issues include: femtocell planning, permissions, ownership and operation; train/road/subway/plane provision; and creating, operating and maintaining networks of 4G/5G repeaters.

The linkage between technology and allocation is illustrated[73] by the following example[74].

Example: 2.6 GHz spectrum auction

2.6 GHz spectral band(s) are available in the EU for wireless broadband based on technology neutral use. They are suitable for use by symmetric/paired (e.g. LTE) and asymmetric/single-band (e.g. WiMAX) technologies. It was not obvious *a priori* how much spectrum should be used for each technology, but it was clear that the allocation would determine the useful bandwidth; adjacent licenses using the same technology would not interfere, while adjacent licenses using different technologies require 'guard bands.' Moreover, bidders likely to deploy paired or unpaired technologies were drawn from different populations. LTE bidders were typically MNOs (mobile network operators); WiMAX bidders were almost exclusively fixed-line broadband providers or ISPs. The 3-stage auction mechanism used by the UK to allocate this spectrum was designed to determine the optimal division of the licenses between the two classes of technology; the impact assessments recognised that spectrum allocation and pricing would directly influence technology development, and that secondary trading (resale) of licenses would change the technological and commercial landscape and regulatory requirements.

Spectrum availability for research purposes

A closely related issue is the need for policy to ensure availability of spectrum for research and innovation purposes. Coordinated 'scientific spectrum' policy can facilitate transatlantic research cooperation and the development of interoperable and globally-compatible technologies. Associated issues include direct availability of 'research spectrum'; its integration into general spectrum; and the mobilisation of spectrum policies to extend the reach and utility of shared scientific infrastructures such as the European Open Science Cloud.

ICT development impacts

5G networks

5G will probably provide the first major use of DSA approaches, exclusively or mixed with other spectrum allocation methods. Although 5G is a single system concept, it combines many elements, each of which will be equivalent to a single service[75]. This involves convergence of engineering concepts in constructing 5G and convergence of business models to allow them to interoperate harmoniously. The glue that holds this together is spectrum allocation for 5G use. Spectrum must serve current and forthcoming technological possibilities while allowing currently quite diverse business models to evolve new 5G ways of working. It must also serve needs ranging from M2M services that only need a few kilobytes of data on an occasional basis to real-time video experiences enhanced by demanding graphics. DSA *in principle* can deal with these profoundly diverse spectrum needs and provide the best use of the spectrum for each. In practice, this needs a 5G infrastructure and thus an evolution of ideas, design, finance and building from now until rollout.

The GSMA position paper includes the following conclusions, which represent a 5G perspective on spectrum and illustrate the momentum that a technological domain can accumulate.

- Significant new and widely harmonised mobile spectrum is needed to allow 5G services to meet future expectations and deliver the full range of potential capabilities.
- Spectrum is needed in three key frequency ranges (Sub-1 GHz, 1-6 GHz and above 6 GHz) to deliver widespread coverage and support all use cases[76].
- Licensed spectrum should remain the core 5G spectrum management, complemented by unlicensed bands.
- 5G and other wireless services can coexist in higher frequency bands above 24 GHz.
- Technology neutral spectrum licences are essential to allow existing mobile bands to be easily refarmed for 5G thus ensuring spectrum is used most efficiently.

- Governments and regulators should
  - support 5G needs in international spectrum discussions due to the lengthy timeframes involved in making new mobile spectrum available and
  - adopt national policy measures to encourage long-term heavy investments in 5G networks.

Specific issues

The following list collects potential areas for EU-US R&I collaboration relating to spectrum policy and 5G.

- Access methods – what access methods are specifically needed for 5G and how can they be reconciled with other uses of dedicated, shared or adjacent spectrum? Are there promising hybrid or general-purpose access methods? What is needed to meet the connectivity needs of vertical sectors?
- What technical and other research is needed for innovative agile spectrum access and management? How should this be reflected in spectrum policy-making to ensure effective 5G deployment[77]?
- What licensing mechanisms are needed for 5G access to high frequency bands (26, 40 and 60-70 GHz)[78]?
- How can co-existence with existing uses (e.g. fixed links and satellite services) be managed?
- What is the scope for licensed vs rule-based spectrum use controls? Possibilities include

Exclusive licences	Tiered authorisation e.g. CBRS[79]
Licensed shared use	Dynamic Spectrum Allocation[80] for inter-tier coordination
Light-touch licensing[81]	Splitting bands into exclusive, light/concurrent use blocks

- Transition to denser networks, targeted small cells, virtualisation and equipment considerations – scalability, cost, ease of deployment.
- Assessment of the amount of spectrum available, esp. in the 26 GHz band:
  - Setting and negotiating band boundaries and locations;
  - Defining spectrum blocks - contiguous/non-contiguous, sizes, configuration; and
  - Earth to space and inter-satellite links and protecting passive use (e.g. below 24 GHz)[82].
- Adapting analysis and policy frameworks for spectrum use conditions and pricing with new technologies: 5G is complicated by the range of options and lack of precedent; dispute resolution must cover e.g. priority demands by technology domains and incumbent/entrant disputes over licence length; and licences could work different levels (national, etc.) and stipulate coverage, sharing, etc.

These issues can be explored in different use cases which might form fruitful bases for R&I collaboration, including mobile broadband, 5G FWA[83], ultra-reliable networks, IoT and media uses. These use cases cover corresponding motives for seeking spectrum which in turn can be served by different approaches.

- 5G mm-wave awards should attract providers of converged fixed + mobile services[84].
- Verticals[85] seeking to use 5G in specific environments[86] or intra-vertical combined or converged services will want localised licences or local shared access.
- Neutral host small cell providers need reliable access to serve a wide range of localised uses.
- mm-wave small cells that are privately owned and/or deployed by users require exclusivity, negotiation and/or real-time access sharing.
- Integrated service providers or affiliates may need dual use (access services + backhaul) spectrum.

Not all of these allocation issues require '0-based' definition and implementation of efficient and differentiated access rights. But many existing mechanisms (e.g. auction designs) assume bidder symmetry and cannot easily deal with the fact that some users (e.g. MNOs) already have 'high spectrum' licenses and start with an advantage or only need 'complementary' access[87]. The following figure shows some of the issues that must be resolved in respect of the different access models before a choice among them can usefully be made.

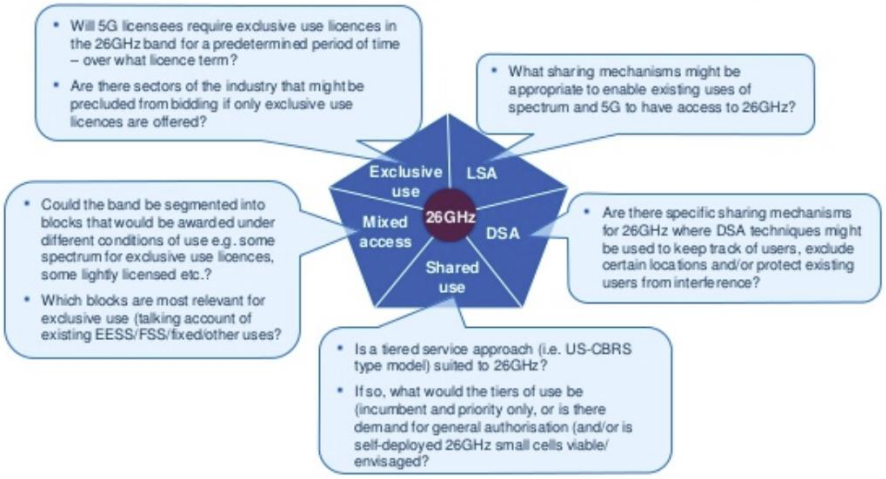


Figure 3: issues for various (5G) spectrum access arrangements.

This diagram outlines but does not resolve the main questions; for example, exclusive use conditions can only be evaluated after allocating spectrum to 5G use or modelling mechanisms for determining the 5G 'slice' or implementing adaptable or 'technology neutral' allocation schemes. But the questions provide a useful framework for a more general consideration of the main items on the agenda of any coherent programme of EU-US collaboration (once extended beyond the purely 5G focus of the diagram).

Big Data

Data analytics interacts with spectrum policy in two indirect ways; spectrum as an infrastructure to support Big Data applications and data analytics-intensive systems and the application of Big Data to spectrum management.

Big Data traffic flows over the electromagnetic spectrum

Big Data communications demands are likely to grow in size and complexity; inevitably, much of this will be wireless, giving rise to a set of related policy and research issues:

- Scaling
- Handling the 3+ Vs
- Data latency spectrum
- Mobile data access restrictions (privacy and security)

As sensor nets spread and deepen, the *scale* will expand to a wireless exaflood involving many different degrees of sensitivity and required Quality of Experience. Conventional ways of establishing (or refusing to establish, in the name of net neutrality) priorities and access may not scale and research[88] as well as policy experimentation[89] will be needed to handle the challenge. Dealing with this will also require new techniques e.g. using bursty transmission to move data in and out of cloud or fog environments without 'big data moves'.

At a systemic level, real-time data analytics approaches are sensitive to communication performance (and thus spectrum policy) and need to adapt to data *volume, velocity, variety and complexity of information*[90].

Part of the solution involves stratifying data flows by collection, processing and use time-scales. Within organisations, this *data latency spectrum* should optimally inform a protocol for prioritising data flows (dealing quickly with the most urgent) even if the protocol is complex and highly dynamic. Between organisations sharing networks and/or spectral resources, the problem is much harder (constrained by spectrum policy, global operations and hardware markets) but needs to be better understood to design spectrum policy, standards, etc.

A final and related issue concerns *mobile privacy*, especially in relation to Big Data approaches to delivering societal objectives, improving health outcomes, environmental management, opportunities for learning and

consumer goods and services. This also applies to commercial uses of Big Data in mobile environments esp. under GDPR, where *access restrictions* are of particular importance in e.g. automated data exchange among firms.

Use of data analytics to allocate rights and manage spectrum use

Big Data approaches can improve the agility and efficiency of spectrum management as it does in other systemic contexts such as Smart Grid or Smart Transport networks or the micro approaches associated with active supply management and active demand management.

Contributions to spectrum management range from data visualisation, technical calculations and control monitoring systems (generally for specific entities and devices) to flexible, adaptive and 'open' sensing and control methods including Machine Learning (ML) techniques to detect new patterns in unstructured data and manage DSA systems where management and users respond to each other via interventions and experiments[91].

Such systems are already under active development from Shanghai to Canada. For example, the Canadian Research Council has developed a prototype spectrum monitoring system using a sensor network and big data visualisation of the spectrum environment that spectrum managers can query in near real-time[92].

Internet of Things/Cyber Physical Systems

The growth in the number[93] of devices wirelessly connected to the internet will depend critically on Machine-to-Machine (M2M) communication, which allows complex 'things' (utility meters, vending machines, cars) to interact even when the primary purpose of the device does not require connectivity. M2M is a fundamental enabler for the Internet of Things (IoT), at least in initial phases that involve adding connectivity to passive objects[94], deploying connected sensors[95] and transmitting instructions to dependent or (semi-)autonomous actuators. The IoT requires these data to be readily and widely accessible[96]. As the CPS-enabled society gains complexity, objects that can sense their environment and communicate with each other will become necessary tools for understanding this complexity and responding to it swiftly and effectively[97]. This decentralisation of communication and control has huge potential for enhancing efficiency – and equity. For instance, information from many parts of a Smart City can be used to alter other parts dynamically to produce collective benefits.

Such physical information systems are already being developed. Pill-shaped sensors in the human body can already send images or other data to locate sources of illness; they will soon be able to deliver localised drug or radiation therapies or conduct micro-surgical interventions. Such communications must use spectral resources.

Remote satellites and ground sensors send data wirelessly back to precision irrigation, agrichemical etc. equipment to improve farming efficiency. Many areas are remote and sparsely populated, which argue strongly for use of wireless communications, especially those not requiring extensive local hardware.

Billboards and 'smart devices' in the home instantly assess consumer behaviour and adapt advertisements, change functions or alert helpers accordingly. Retrofitting costs to support wired communications would make many such implementations prohibitively costly, but WLAN communications used by most existing Smart Home Hub devices may not support all the security, privacy and Quality of Service needed by potential uses.

Some IoT/CPS devices will be physically mobile while others will be stationary. Although both kinds could use mobile data service networks, stationary devices can also use wired or fixed wireless (including short range) communications depending on practicability, performance and cost. Spectrum policy will thus need to reflect the technological and organisational specifics of communications infrastructures.

From the spectrum management perspective, IoT/CPS per-connection data volumes are likely to be low compared to other mobile broadband uses, but devices may be further from conventional mobile coverage. Such applications would particularly benefit from a low capacity but ubiquitous coverage layer – and are more likely to be developed and supported where it exists. In addition, they may have different service requirements, such as the absolute need to prioritise robustness of the communications link for safety critical uses[98].

Widespread adoption will take time, but underlying technologies are improving rapidly. Existing IoT/CPS R&I seeks to connect the widest possible range of devices anytime, anywhere and for (almost) any purpose. There remain questions over the extent to which policy – and R&I for policy - should continue this 'agnostic' approach or become more specific. But the diversity and criticality of IoT/CPS uses will force spectrum policy to adapt in order to ensure that priority uses, devices, functions and users are identified and connected in appropriate ways.

Any IoT object can be a data source, conventional ownership concepts are becoming blurred. This obviously applies to ownership of devices, the data they exchange and the functions they (collectively) perform and spectrum use, suggesting that neither exclusive licences nor an unregulated commons will prove sustainable.

This rich research agenda must be tackled across many boundaries, including oceans. Specific elements include:

- General requirements applying to IoT/CPS traffic;
- Device-specific needs of Machine-to-Machine communications such as smart metering[99];
- Use case-specific needs such as Smart Cities or intelligent/additive manufacturing.

Beyond this, the main policy concern is less how much/ which spectrum is allocated to IoT/CPS uses than about the nature and stability of allocation mechanisms (including shared access). This is further discussed in Annex A.

Spectrum Conclusions

Spectrum use has changed dramatically over the last decades, and is bound to change even more. Primarily, these changes will bring activity in from the extremes towards a more varied and dynamic centre ground:

- The modalities of spectrum management will shift away from static, long-term licensing to a mixture with dynamic and uncontrolled regimes, within broad limits on interference;
- Spectrum allocation will become less likely to be restricted to specific uses or to all uses by specific single 'owners' of a particular band;
- Spectrum use will become far more agile in time, with today's long-term exclusive licences superseded by short-term, local, transferrable and 'recombinant' alternatives; and
- The intersection of spectrum policy and regulation will no longer be the exclusive domain of telecommunications regulators, but will increasingly involve other public entities (e.g. competition, privacy, financial, health etc. regulators) and a mix of industry and civil society stakeholders, in order to reflect the increasing diversity of uses and impacts of spectrum choices. Therefore, spectrum policy will be part of a more integrated set of digital policies.

These are developed in slightly more detail in the discussion beginning on page 46.

3. Future Outlook

In this chapter, we collect some of the pending developments that are most likely to shape opportunities for EU-US collaborative R&I. We begin with a general discussion, and then consider a specific context within which the different technologies and policy domains come together; digital communities.

General trends

This section does not attempt to give a comprehensive scenario of future developments; the scope is too vast and the world too uncertain for this to be a fruitful exercise.

The following overall trends seem inevitable, however:

- Increasing spread, density and capability of communications networks and the flows of information through them;
- Collection and processing of growing amounts of data for a widening set of purposes;
- Increasing levels of automation and machine intelligence in data processing and implementing decisions made in response to such processing;
- Decreasing ability of human beings to understand or control the automated systems created by new technologies and their deployment.
- Growing tension among technology deployments seen as privacy-enhancing or privacy-invasive (or both at once) and market, civil society and government attempts to control them;
- A growing debate over the adequacy of controls on privacy-relevant elements (data protection, algorithmic regulation, consent mechanisms) to keep pace with and respect evolving notions of personal privacy and their value (or otherwise) in relation to development;
- More?

Overarching developments

A number of new developments foreshadow the contribution of standards to development of the ICT 'space'. The following developments are expected to be particularly important. They are discussed in more detail in Annex D.

- Sharing economy – "an economic system in which assets or services are shared between private individuals, either free or for a fee, typically by means of the Internet."[100] Its growth requires *user convenience*. Interoperability related standards will be market driven, while for safety and quality for quality and safety there is regulation in place, such as consumer protection regulation etc. The level of sharing goes beyond the well-worked bounds of formal contracts and transactions with or among legally defined corporations raises new challenges in all of the domains listed above.
- Technologies become invisible - ambient intelligence brings computational capacity to everyday environments and makes them responsive to people. It requires *seamless* interoperability and connectivity.
- Blockchain – it is not clear whether this facilitates secure interoperability, or indeed how people can rely on such unsecured structures. Transactions recorded in distributed ledgers are globally published, generally in unencrypted form.
- Artificial intelligence – Machine learning and artificial general intelligence will eventually be part of how our systems will help us manage complexity and increasingly pervasive and salient interactions. It may also arise 'by accident' through the interaction of multiple 'smart' systems (sometimes called artificial general intelligence) Since it cannot practically be audited, controlled or even understood in real-time, it cannot be left unsupervised, but the feasibility, means and even objectives of supervision remain unclear.

These and other developments firmly indicate what we can learn from the past: the future, 10 years from now, will contain elements and characteristics that are currently beyond coherent imagination. 10 years ago, few thought data would be as abundant as they are, mobile services would pose so much challenge to fixed-line networks, and the Internet of Things and AI would be as far out of the starting blocks as they are.

The evolving security landscape

ICT security is likely to be a particularly fruitful area for collaborative policy-relevant R&I; it is closely linked to national regulatory and enforcement structures that are regarded as essentially sovereign concerns which (thanks to interdependence of national interests in globalised networks) drives policy harmonisation, but not tight coordination. Moreover, its failures are closely linked to vital public services and to powerful commercial interests. For this reason, we discuss it separately.

We are entering an era when of dramatically increased network speeds especially in many backbone and interconnection networks. Criminals are smart and seemingly one step ahead of security measures. With the changing landscape of technology and applications in the connected world, threat actors and attack vectors are expected to change even more. In the beginning, threat actors were motivated by fame, focused on the newly interesting, novel technology – this 'innocent' troublemaking will resurface with each major new paradigm as they compete to showcase their hacking expertise and expose vulnerabilities. But as technologies mature and become more critically embedded, attacks will increasingly be based on the attacker's (or the affected parties') monetary, ideological, commercial or idealistic objectives. Since real-time interactions are key to ICT communications, actors may use jamming and interference with communications, misrouting of information, impersonation, or flooding and draining of resources, which could cause Denial of Service or at least confusion.

Beyond such 'malicious' attacks are the accidental or unintended security failures due to systems scale, speed, complexity and fragmentation. The probability distributions of such failures and the extent to which they can be managed by security policies are very different from those associated with attack-based security failures. Research across domain and national boundaries is needed to expose and understand these differences.

We have also not finished working through challenges from prior disruptions. The increase of geographically distributed and interconnected potentially real-time cloud computing requires increased bandwidth with high availability and security. This will eventually require us to re-evaluate many of the assumptions and mechanisms, built into Internet protocol designs. In many ways, the current Internet is more and more becoming the backplane of a massive distributed computer system.

Basically, there are three ways forward:

- *Make do and mend* - making the most of what we have today and increase the security of our ICT and communications infrastructures by better implementation, patching new vulnerabilities and ensuring that stakeholders do their part by raising awareness on good practice and enforcing responsible behaviour by all stakeholders in the value chain;
- *Clean sheet* - redesign the ICT and communications infrastructure to remove key vulnerabilities remaining from the Internet's youth as a collaborative research environment rather than the world-wide system for accessing and sharing information and communication;
- *Bootstrapping* – Define and build in security by design at appropriate levels for new systems and catch up/patch up vulnerabilities from the past/to new threats in existing systems where feasible and necessary, where this does not involve wasted effort by being too localised (treating specific rather than systemic vulnerabilities) or inhibiting true progress.

1- Awareness raising of vulnerability issues, patching, and ensuring stakeholders take their responsibilities.

Much of what is needed to reduce vulnerability of our ICT environment to acceptable levels is already known, and ICT security would be much higher if all stakeholders in the value chain of ICT services apply "good security practices" to their work. As was identified before, most stakeholders today feel very little economic or legal incentive to ensure application of good security practices, as there is no common view on this. Possible measures here may be a review of existing measures to improve security and development of new tools and services where possible; establishing a bottom line of "expected good practices" thus to ensure companies and individuals can be made responsible for failing living up to good practice; ensuring industry self-regulation through public commitments to "good behaviour" with regards to securing tools, systems and services; and awareness raising towards policy makers, law enforcement and end users as to ensure people know what to live up to.

With this "solution", the system will become less vulnerable, but we will not be able to take out some of the intrinsic vulnerabilities in our ICT and communication systems, in particular those that guarantee origin of communications and integrity of information packages.

2- System-wide redesign of computing and communication systems we increasingly depend on

At the same time the mechanisms that software uses to protect and secure inter and intra computer communications strongly suggests that we reconsider (for the 4th or 5th time) the use of capability architectures to identify and protect information as it is moved from system to system and that that be done by hardware enabled methods. Mechanisms such as that would provide a way of identifying forged software and fake information (email etc.). It is beyond this paper to detail the design but we strongly suggest that it is time to create an integrated international research to design this next generation computing infrastructure (Internet).

A way forward may be to jointly engage in what the USA National Science Foundation calls a *"grand challenge"* and create an operational test bed where the goal is to architect the next generation of network protocols/hardware, securable processor, and the software necessary to operate an integrated secure Internet as well as to be able to attach non-secure environments to the network and still protect the world against their bad behaviour. Basically, the effort would be to gather all the past and current understanding of how to create secure systems and to produce a test bed that can lead the path toward as secure a distributed cloud based system as we can. The test bed would, by its nature need to partner both the academic world and the industrial world of at least the EU-USA. It would be best if the initial test bed demonstrated the technology in one of the critical areas – power, aspects of the financial systems etc.

This requires political will and economic buy-in from both governments and industry, and this may require either visionary leadership across the continents, or an increased awareness of the need as major disasters result from the inherent vulnerabilities in our communication networks today on which all ICT and data services are build.

The role of Communities

Support exchange of good practice experience between Communities in EU and US; many societal challenges are common to both regions and different types of communities and the potential of many solutions that have already been devised for adaptation elsewhere and optimisation in situ remain under-explored.

Communities drive change, and are driven by change. This is in particular true for "digitisation". They play an important role in determining how we work and live together, the role of technology and of course in policy ("all politics is local"). Increasingly, communities become "Digital". We define Digital Communities as:

"Digital Communities are where people come together to learn, share and collaborate to build digital solutions to common problems and challenges".

Digital communities may be distinguished along a number of dimensions. Of greatest relevance for current purposes are the colour of the field and the measure of proximity.

- 'Brown-field' digital communities are existing communities in which "digital" becomes an increasing part of the fabric of Community life;
- 'Green field' digital communities are new communities that emerge because of the spreading use of digital technologies[101]
- 'Spatial' communities are based in a particular physical locale
- 'Non-spatial communities' involve people linked by shared interests, technologies, and other 'non-local' characteristics
- Hybrid communities are complex communities of one sort are linked by connections of the other – e.g. a network of 'Smart Cities' (non-spatial linking of spatial communities) or a city-based 'games cluster' (spatial linking of complementary functional communities of game developers, venture capital, etc.).

We see Digital Communities as a place where the range of policies considered in Chapter 2 (and the detailed Policy Briefs) come together, in the sense that their interactions can be clearly recognised. At the same time, we do not think that this replicates the focus or concerns of national or higher-level (e.g. EU) "communities policy", which have a clearly distinctive basis and constituency. We recognise clearly that communities in the above sense are clusters where people can clearly recognise and act on shared interests and interdependencies. Technologies – especially those considered here – obviously affect this, because they reduce the distances between people and change the nature of their interchanges. But this concept of community works because of its limited and local nature; at the same time, the technologies are global and designed to scale. This is why the topic needs separate consideration.

In the abstract, a society will develop and implement technologies in ways that reflect its shared values and also its internal conflicts. Thus, these values are embedded in the way technologies are used and in the types of technologies that are developed. This applies to communities if they have an effective voice in developing the technologies that transform (brown-field) or define (green-field) them. It also applies to societies made up of such communities – at whatever level technologies are developed, deployed, shaped by policy and regulated.

The technologies and associated applications, services and infrastructures can be scaled up to global level; this is often given high priority as an implicit or explicit objective for policy and commerce alike. This *can* strengthen communities to the extent that use of common technologies fosters interoperability and can allow them to learn from each other and to pursue alignment and coordination where needed without necessarily harmonising or converging on a single approach. This linked diversity preserves comparative advantage, freedom of expression and the resilience of the society in which these communities exist.

But this benefit is not a guaranteed or inevitable consequence of scaling; if technologies or approaches (e.g. 'Smart City' or 'Smart factory' models) are scaled up by imitation or adoption, without stripping out or at least recognising embedded values and biases, the process may weaken local communities and the functions they uniquely perform (most of which do not – and arguably should not - scale), suppress necessary or efficient diversity or even evoke resistance resulting in needless and harmful fragmentation.

A further specific link between the community perspective and the internationally collaborative ICT R&I focus of PICASSO is the need for similarity of form and function. Many of the issues affecting communities span jurisdictions, including national or EU boundaries within which policy is made, regulation promulgated and R&I support and targeting arranged. The range of different approaches to common problems in different communities provides a collective resource vastly more valuable than the sum of its parts, whether this involves capturing the lessons of the past or conducting experiments to explore possible futures. Moreover, the hidden embedding of local values in technologies and applications means that the 'right kind' of scaling (as discussed in the preceding paragraphs) can only be identified and implemented by research teams that cross disciplinary *and* international lines. In this sense, just as communities in isolation drive and are driven by technological change, jurisdictions and national policy both drive and constrain R&I efforts to rebalance the technological, societal and commercial dimensions of digitisation.

This applies in particular to research and policy 'communities', where it calls for a particular kind of multistakeholderism. In order to retain the power of disciplinarity, researchers must be able to participate in relatively homogeneous research teams using well-understood and tested methods to investigate specific research questions. The results, inevitably, involve other interests and perspectives – sop the social, engineering and natural sciences must interoperate. But neither the separate nor the joint activities should crowd out the other, or lower its internal standards. Therefore, a network of connected non-spatial communities is needed to understand the reciprocal impacts of digitisation and community – and thereby the relation among societal challenges, technologies and policy. Therefore, it seems reasonable for each of the disciplinary communities to meet with the others in order to gain a rough sense of their concerns, which can help ensure that the detailed fruits of specialised R&I can be integrated. In other words, R&I policy should – in this domain at least – be:

- specified in an internationally and interdisciplinary collaborative forum;
- pursued in internationally-collaborative -but not necessarily interdisciplinary – projects; and
- used to inform other policies in an interdisciplinary/evidence-based - but not necessarily internationally-coordinated - fashion.

In other words, the most sustainable and effective approach to collaborative ICT-focused R&I is likely to one that embraces a structured multistakeholder model and the multi-homed nature of scientific, commercial and policy networks.

The specific digital community perspective on the PICASSO policy domains (privacy, security, standards and spectrum) and technology areas (5G, IoT/CPS and Big Data) is sketched in Annex D and discussed in more detail in the Digital Communities Policy Brief.

The future of digital is driven by communities, and vice versa

Digital communities will continue to evolve and transform the policy landscape. Communities have long been the source of policy demands (e.g. for collective solution to common problems) and the basis on which such problems are addressed (e.g. circular economies and local civil society activities). At the same time, such communities can distort political institutions, consultation and evidence-based regulation. As this evolution proceeds, some old problems may cease to require policy intervention (this is the aspiration of initiatives from 'digital humanitarianism' to 'Fix My Street' local initiatives); others may be resolved in new ways; and still other issues may arise exclusively in digital communities or as a direct consequence of digitisation.

In order to assess policy, to ensure that the 'right kind' of digital community formation occurs and to understand recent and future history, appropriate data capture and analysis strategies must be implemented, and a range of research questions addressed.

Some of these are technical in nature. For example:

1. Future development of wireless access technologies[102], especially those that can provide gigabit+ class Internet with multiple classes of service in rural areas, thereby assisting the emergence of dispersed and diverse communities; of particular interest are advanced or wireless technologies, although the modes of provision and management may need to be adjusted to coexist with other uses.
2. To foster innovation and the emergence of ad hoc communities, it is also important to invest and conduct research into the extension of communication networks into unregulated or differently regulated spectrum bands (e.g. TVWS).

To support community development over these communication infrastructures, it is also necessary to improve individual and shared 'edge computing', which can provide local, low-latency, self-reliant, and resilient

technology support to a wide range of data gathering and sharing, data processing and functional capabilities needed by digital communities. Unlike cloud resources in well-controlled and managed data centres, edge computing capabilities must be capable of wide environmental ranges, autonomous operation, self-association, self-healing, dynamic reconfiguration to match needs, ability to handle data securely, self-protecting against malware and attacks, and the ability to work cooperatively with other edge facilities placed by competitors or other jurisdictions[103]. Digital communities are necessarily open and diverse; they have to work with lesser – or more granular - standardisation and their functional, security and related requirements may need more resilience and less robustness than 'closed' and purpose-orientated applications.

These computing facilities need data on which to operate. Communities form when distances are reduced and common interests and opportunities become visible; the "sensorisation" of potential communities can help to shrink distances (especially in rural areas, but also in urban environments where the visibility of different groups is limited or biased) and raise awareness of common interests and complementary capabilities. But this is not inevitable; the same data-intensive approach can reduce relations among community residents and between them and community services to flows of data, weakening the essential human content when development is driven by one side's concept of efficiency.

In such settings, research into collaborative, cross-functional sensing meshes with multiple-application slicing, heterogeneous priorities, and self-protection will be especially valuable, as will social science research into e.g. the economics of such systems and the data they capture and the ethics of their use (which could in turn be folded into new policy designs).

There is also scope for joint research into the services and functionalities needed to meet the needs and smooth the functioning of nascent and mature digital communities "over the top" of the communications infrastructure. Most of these are already being pursued from commercial or public service standpoints, but the needs of communities may be different and under-served by existing R&I. These include:

- Healthcare, examples include:
  - Inexpensive at-home sensors to give telehealth professionals objective information on short notice.
  - At-home hospital-quality monitoring of chronic conditions.
  - At-home physician-controlled medical drug synthesis and dispensing.
  - Passive continuous health monitoring. (While applicable everywhere, continuous monitoring may help predict acute events which would help mitigate the longer rural response time to such events.)
- Education; examples include:
  - Access to learner-directed research resources.
  - Richer forms of distance education such as being able to observe the reactions of other students in the class to make distance and computer-based education more of a social experience, and simultaneously being able to see the whiteboard, the instructor, and other objects / media / presentations.
  - Real-time access to remote scientific and engineering instruments.
  - Engaging cross-generational educational discussions, giving personal attention to students and an ability for seniors to contribute.
- Public Safety; examples include:
  - Better data sharing technologies that protect privacy while allowing cross-jurisdictional mutual aid efforts to be more effective.
  - Just-in-time AI support for volunteer first responders, especially less-experienced volunteer first responders.
  - Better remote-expert support for volunteer first responders (e.g., physicians to EMTs)
  - Better resource awareness (of volunteers and other public safety assets) and more reliable communication among them.

Research needs to involve (perhaps in a structured multistakeholder way as outlined above) collaborative teams representing the social, economic, cultural, safety and technological dimensions of each research challenge. End-users of applied research are especially important to involve from the beginning[104].

.

4. Conclusions and recommendations

Policy aspects are an important factor in EU/US ICT R&I collaboration. An improved understanding of this linkage could make R&I collaboration significantly easier, more focused and thus more successful. This has broader significance as well; acting together, EU and US R&I can have more weight in the global development of ICT – and when EU and US R&I activities reflect our common values, they too will have more weight in global environment in which ICT is not both a result of and a catalyst for further globalisation. This will make it easier for our ICT-related development at home to preserve and refine our values (e.g. by limiting an offshoring 'race to the bottom') and reduce damaging policy fragmentation around the world. Is this good or bad? It surely cannot be stopped, and its direction can best be influenced by acting, participating … and leading where possible. This section collects and integrates conclusions and policy recommendations that follow from our analysis of four important policy perspectives: privacy, security, standards and spectrum policies related to ICT development.

General aspects

Overall aspects that provide the framework in which these policy domains work out have a major influence on how the parts of the puzzle come together. Competition between domains, and the coordination mechanisms we use determine how we can best assure a sustainable way forward in which both EU and US values are respected, and how societal issues are pursued. Below we explain how.

Competition between domains.

Stakeholders can provide informed inputs to policy and can address policy problems from their own perspective. Like any other interested party, however, harnessing this level of insight and ensuring compliance and active participation in subsequent policy requires a platform to elicit, balance and integrate competing perspectives especially when used to address horizontal policy areas or areas where technological neutrality is strongly emphasised. The problem is one of *time-consistency* (as illustrated by the 2.6 GHz auction example on page 28); today's most persuasive technology area may or may not be the most relevant in the long run; but a disproportionate influence or level of strategic engagement with policy or R&I support) may lock in a long-run advantage that can crowd out better technologies or even prevent them from developing and demonstrating their advantages. This path-dependence is potentially worse in globalised contexts, due to the leverage regions exert over each other's' development.

In particular, the need to compete for R&I money, policy recognition and regulatory forbearance is involving scientific and engineering communities in ways that depart from traditional participation in the formulation of evidence- and science-based policy.

One conclusion is that transatlantic R&I collaborations that cross technology domains and R&I preferences for policy could produce a more balanced way of identifying and implementing technology-neutral policies, taking into account that apparently-neutral approaches may not in fact be neutral because one area currently appears to be more promising or is better-placed to 'bid' for support. Multistakeholder, multi-technology and multinational collaboration (at the level of designing R&I programmes even if they are implemented at national level) is the only way to ensure time-consistency and avoid the 'picking winners' fallacy.

Coordination models

Over the years, again and again cooperation opportunities were missed through lack of alignment of support for collaboration on both side of the Atlantic. Mis-alignment of availability of appropriate budget, or even misunderstandings because of semantic meaning of concepts has led to not being able to fully develop potentially fruitful collaboration. Collaborative R&I can help to identify the most appropriate form of policy alignment between the EU and the US in this domain, and we believe should be further pursued. Possible ways forward:

- Establish a pure bilateral model, in which extraterritoriality arrangements regarding existing laws are negotiated between the European Commission and the US Government;
- Adopt a regulatory alignment approach amounting to EU-US harmonisation of parochial rules (which would have greater spillover effects regarding data flows to or from the rest of the world;
- Ensure EU-US engagement in international and supranational fora and coordination with trade and other policies to ensure the world remains friendly to the approaches we wish to take; and/or
- Develop a conscious and concerted effort to develop a shared position of global leadership (where R&I is combined with other measures) in order to ensure convergence on common rules and frameworks that embed our common values (this presumes a prior agreement on what those are).

Key policy domains

As described above, we found that four specific policy domains were key in ensuring a common understanding of possible joint approaches – areas that truly require debate and insight to make it possible to collaborate in the specific areas of 5G networks; Big Data; and IoT/CPS. Conclusions and recommendations for each of these areas are described below.

Privacy and Data Protection

Privacy and data protection have become key for both Europeans and US Americans over the last years, and there is a lot of public and political attention for it on both sides of the Atlantic. Taking this forward in PICASSO context lead to the following two recommendations:.

1. A framework for ICT collaboration (whether privacy-specific or not) needs fully to reflect our shared democratic and individual rights-based values, expressed globally in Universal Declaration of Human Rights, in Europe by the European Convention on Human Rights, the Lisbon Treaty and the Charter of Fundamental Rights and in the U.S. by the Constitution. To do this, such a framework also needs to reflect the differences that enrich our interaction.
2. Solutions need to be found to allow services to develop that respect (European and US) privacy and data protection frameworks and – where appropriate – challenge their provisions. EU-US cooperation on privacy-relevant matters is complicated and enriched by: the fundamental-economic right divide; the data protection-privacy distinction; positive vs. negative privacy rights; and interference between commercial and crime/security objectives.

The following discussion develops this theme in more detail.

- Privacy and beneficial exploitation of data can help or hinder each other. Consultation within the project confirmed that industry should explicitly consider human behaviour and the feasibility, proportionality and importance of choice and consent from the outset when developing industrial solutions.
- There is a pressing need[105] to improve the awareness – and understanding - of policy makers, citizens, consumers and the commercial world regarding what is technologically possible, economically

advantageous, socially acceptable, politically viable, legally allowed and ethical. Those charged with important decisions or exposed to the consequences too often have only limited insight into what is happening on the ground.

- This awareness should recognise that laws *and business models* change slowly relative to technologies and market behaviour; they are thus likely to interpret and prioritise privacy (and other concerns) differently. For instance, despite increasing protests from the privacy community it took GDPR to fully spur businesses around the world into action. Sometimes businesses and lawmakers act out of panic – given the often irreversible nature of change, it is particularly important for responses to technology developments and public concerns to come from an open dialogue among the government and business actors.
- There is no way – and no reason – to restore the *status quo ante*. It will also take time to develop a full and shared understanding of what GDPR means for all kind of use of data – the predecessor Directive was being reinterpreted until it was superseded. But it is equally clear that the sustainable way forward for new services is to take privacy sensitivities – as well as privacy rules – fully into account. At the same time, online privacy policy development should not forget about offline privacy.

Privacy policy is linked specifically to the three PICASSO domains.

- 5G networks: sensors and tracking will become ever more ubiquitous in networks designed to focus on data collection and exchange. EU/US policies do not seem to directly impair the ability to collaborate in 5G ICT research and innovation, but may enrich the set of research topics.
- Big Data: there are two related challenges; explicit intent and consent requirements for sharing personal data and the potential of algorithms and machine learning to create new levels of personal data outside those currently regarded (by the law or data subjects) as subjects of concern. Here, clear adaptations – if possible - to preserve proportionate and effective consent, including explicability and/or algorithmic regulation will be needed to ensure big data services operate legally and that protections are not bypassed.
- Cyber Physical Systems and IoT: CPS are not (currently) intended to sense/track individuals, yet they may have that effect. It will be very important to determine which data are privacy sensitive and how this relates to intended use and consent, particularly as IoT as such is a big data generator.

Across all domains, attention is needed to algorithms that combine data from different sources and create links to individuals. Because many of these data are not collected for that purpose, subjects do not (and in some cases cannot effectively) fully consent. There is an increasing recognition of the need to insist that data are combined "in law abiding ways" and a resulting need for research to understand what that means in technical, operational, commercial and legal terms – i.e. to avoid combining data in ways that *adversely* affect individual privacy while not foreclosing innovations that advance their interests (including privacy). This supports the recognition that privacy should not be defined solely in terms of data types, processing or intended/possible uses considered in isolation or set in stone; regulation should flexibly reflect all these dimensions and invite innovation – including changes in regulation as behaviour, technology and practice evolve. This requires a taxonomy related to new ICT services; clear privacy *principles*[106] that can be applied on both sides of the Atlantic to standards, technology and system design, contracts and codes of conduct as well as legal instruments and an observatory combined with dispute resolution mechanisms to ensure that the principles are fairly applied to sanction harmful behaviour, and encourage beneficial change among all stakeholders.

Some technological 'solutions' may not have the intended effects. For instance, end-to-end encryption may prevent third parties from seeing the plaintext of messages, but observing the timing or size of encrypted messages may nonetheless convey valuable information that can be used in ways that damage the interests and even the rights of data subjects.

EU-US ICT collaboration in relation to privacy is based on the global impact of these technologies and the flows of information to which they apply. Restricting data mobility enhances the power of local laws, but at a cost which at the moment cannot even be assessed. To develop and implement a principles-based approach that can span countries, technologies, uses and time without choking off progress or creating new problems requires a global, fundamental discussion on the evolving meaning of privacy and the impact of new technologies. This

needs to build on discussions taking place around the world on the balance between private and public interests. Specific answers will not be the same for each society; even some of the underlying principles are not universal and cannot be made so. But a common baseline can and must be established, which goes beyond the current rights-based charters. This debate must give voice to policy makers, businesses, technology developers and citizens. Platforms such as the Internet Governance Forum can support such multistakeholder debate, backed by industry (and individual) self-regulation and multilateral government initiatives.

Privacy and data protection also offer opportunities for innovation; legislators should ensure that "responsible innovation" is possible both as a matter of R&I and in terms of the collection and curation of a relevant evidence base. Privacy in this sense is both a *right* (which through laws and reputations constrains innovation and economic growth) and an *influence*[107] on individual and organisational decisions that creates new opportunities for innovation and 'gains from trade'. This role, too, brings challenges for collaborative R&I to take into account human attributes and to demonstrate this in an open and credible fashion. This can encourage partnership with data subjects (so each side understands the other), enable market 'discipline' of firms' behaviour and facilitate cooperation in the development and application of regulation.

ICT Security

Security of ICT devices, data and services are broadly seen as a top priority and a concern that needs to be addressed. Without appropriate security in ICT, trust in use of the products and services that are based on ICT erodes and this reduces the opportunities to reap the benefits.

With regards to EU/US collaboration, a framework for ICT collaboration needs fully to reflect:

- Security
- Privacy
- Awareness

As the security landscape continues to evolve, so will the threat actors. Currently, there are highly capable threat actors, capitalizing on the prolific black market to buy and sell capabilities and information. This will only continue to grow as additional devices and data sources come online. The growing volume and exchange of data require new technology to protect the user device and data entity. Particular attention will need to be given to adaptive, self-defending, autonomous capabilities. Considering this, the following conclusions specifically relate the three PICASSO domains with ICT security policies.

The same technologies that foster these threats can, however, help to mitigate them. The reliability and complexity of communications offered by 5G can remove some security threats immediately or provide the capabilities needed for implementing powerful security arrangements. The big data analytic techniques used to expose secure information (e.g. pattern recognition) can be used to detect new threat signatures, and the sheer volumes of data involved make it harder to interfere with or corrupt a significant proportion. And cyberphysical systems can internalise security arrangements or even extend them to the IoT by requiring suitable standards adherence. As discussed in the Future Outlook chapter starting on page 34, these protections are not perfect, but they can deal with some of the most pervasive and disruptive threats. More importantly, collaborative and interdisciplinary R&I focussed on security issues can improve general understanding of the dimensions of the problem, thus enabling other control mechanisms (e.g. hard and soft law and commercial arrangements) to be implemented and – perhaps most importantly – reducing the extent and harms due to subjective insecurity.

In the future, we see

- Innovation, industry and governments must seek the right balance between free-market development and regulation. There will be advances in the interoperability of connected objects to drive the value for larger, connected ecosystems, like cars, cities, and industry solutions. There will also be increasing regulatory change, and companies will continue to struggle with it. Regulation will be characterized by the inconsistency

of laws among countries, different levels of social responsibility, and business competition. Regulation can also be a senior management focus—and distraction— due to the operational cost of meeting regulatory requirements, with the setting of standards usually being a long, drawn-out process taking up to 10 years. In the meantime, siloed *de facto* security standards will proliferate. This in turn calls for collaborative development of a security taxonomy of ICT developments

- Mesh networking will become commonplace and data will be everywhere, so security will have to be everywhere, accordingly. Data will be on every device and transit—as necessary for use. Most IoT devices will have sensors for communications with peers. So, there will be new security functions all along the chain— sensors, devices, and intermediaries.
- Communications require tools and techniques for securing networks that are enhanced with built-in resilience because it depends more heavily on multiple node interactions and may equate to operational reliability.
- Outdated security model—Traditional IT security policies and controls will be untenable. The security model for it will need to transform to support all of the new aspects of operational technology security and transition to a data-centric aspect. Security will need to be automated, distributed, context aware, and real time.
- "things" on the Internet need to be designed for security, upgradability, and resiliency. Hewlett-Packard[108] recommends to focus on the following underlying attributes:
    - Secure access management—key processes, which include identification, authentication, and authorization, will become more important because of the sheer quantity and variety of IoT systems;
    - Self-protection—IoT also needs self-protecting and self-healing systems. These attributes are important since systems will no longer have the advantages of a defined perimeter or enterprise-class managed environment. Security solutions will need to leverage the added value of crowd-sourcing and peer intelligence to help form a self-protecting mechanism.
    - Privacy controls—because data will be created in increasing quantities and situated everywhere, it's imperative that solutions give clear control of the data to the owner or source. Ownership will be complicated due to the distributed nature of the systems and complexities of the governing environments. Security and privacy will need to be addressed directly at each device and interaction—transaction and communication.
    - Embedded security—Security will need to be deeply integrated in hardware and application software layers. The diverse functionality and small form factors won't be able to withstand generalised, bolted-on security mechanisms. The technical designs will need to use context aware, adaptive security that senses and responds to a range of trust mechanisms.

Towards the future we will need to develop biologically inspired security. With IoT and underlying interconnections, there's a significant risk with IoT devices providing a back door to enterprise systems and data. Using biological constructs, we can identify attacks before they happen, and also incorporate dynamic defence by directing resources to the appropriate area.

Standardisation

Standardisation processes have changed dramatically, but struggle to keep pace with the evolution and outputs of collaborative R&I. Convergence onto platforms, devices, protocols, etc. is not so strong as to enable us to hope for a similarly-converged set of standards or even standardisation processes, but interconnectedness (beneficially and intentionally or otherwise) is sufficiently pervasive and important as to frustrate moves towards a unified and federated alternative. Even traditional 'stovepipes' (e.g. technology domains or economic sectors) will not contain this growth. This messy mix of data, logical, service, hardware etc. standards for overlapping purposes will persist, which is precisely why joint research on the nature of standardisation is required (since it is not simply a design or control problem). Moreover, the standardisation implications of technological R&I must be better understood when it is planned and conducted; this requires interdisciplinary and international collaboration. Globalisation also plays a role; nationally oriented standards are only useful when aligned with

international developments and secular interests can threaten the coherence of standardisation and technology development.

Possible ways forward towards better collaboration would include on a general level:

- Relinquishing the hope that national policies will provide "competitiveness by exclusion";
- Better use of IP for society and economy to benefit from new insights; and
- Specifically for EU/US collaboration, considering both EU and US values in order to trade effectively and to become relevant to multiple regions of the world.

5G developments are already well-advanced and diverse across the world. Specifically much 5G development is considered "commercial" in the US, but public support for collaborative R&I is still available in Europe. [This may be partially down to different definitions; there is a big overlap between US research on Advanced Wireless Broadband and EU supported research on "5G"].

Big data goes global and needs to have global solutions, as well as adaptations to local laws. GDPR is an important driver in the generation of standards towards ensuring privacy of individuals, but ethical challenges remains, especially with regard to AI.

IoT devices are used all over the world and data are exchanged between objects and aggregates in big data sets – sometimes by purpose-built IoT ecosystems, at other times through big data techniques.

At this point our conclusion is that also for EU/US collaboration it mostly makes sense to stimulate participation of sponsored research and innovation in global standardisation platforms, such as IETF, ITU, IEEE etc., rather than at regional level.

Our second conclusion is that standards should aim at setting a minimal responsible level, and not less than that. This is because every application of standards will also need to adapt to the specific requirements of that application.

Spectrum

Spectrum use has changed dramatically over the last decades, and is bound to change even more. Primarily, these changes will bring activity in from the extremes towards a more varied and dynamic centre ground:

- The modalities of spectrum management will shift away from static, long-term licensing to a mixture with dynamic and uncontrolled regimes, within broad limits on interference;
- Spectrum allocation will become less likely to be restricted to specific uses or to all uses by specific single 'owners' of a particular band;
- Spectrum use will become far more agile in time, with today's long-term exclusive licences superseded by short-term, local, transferrable and 'recombinant' alternatives; and
- The intersection of spectrum policy and regulation will no longer be the exclusive domain of telecommunications regulators, but will increasingly involve other public entities (e.g. competition, privacy, financial, health etc. regulators) and a mix of industry and civil society stakeholders, in order to reflect the increasing diversity of uses and impacts of spectrum choices. Therefore, spectrum policy will be part of a more integrated set of digital policies.

It has become clear that 5G development requires increased availability of specific types of spectral resource, not only to traditional users but to an increasingly varied population of new players. Therefore it puts into sharp relief almost all the spectrum policy issues considered in this paper and those being fought over in policy and legal circles today. However, 5G, despite its close and obvious dependence on wireless communications, is not the only use or set of users. Therefore, its specific needs should be balanced against those of other technologies

and stakeholders (e.g. those coming from the IoT/CPS and Big Data communities of interest) if spectrum policy is to be fit for the future.

IoT/CPS requires spectrum availability in both very local and more regional contexts, and thus may require a layered structure of negotiable rights. Moreover, its requirements for bandwidth, latency, reliability and other characteristics may be more flexible, or at least may become more flexible if the incentives for technology development provided by spectrum policy dictate. This includes, in particular, the very different timescales and data volumes associated with e.g. sensor nets, M2M communications and autonomous mobile devices. These requirements may also be context-dependent, meaning that special spectral management regimes may evolve for use in e.g. Smart Cities, Smart factories, etc. The resulting tensions between potentially incompatible access and utilisation regimes can be dealt with 'by design' in both the physical architecture of the various devices and through the standards that govern their communications and interactions.

Finally, the flows of data through the wireless networks of the future are bound to increase in scope and volume, even if not necessarily to the exaflood levels that some have foreseen. Volumes can be reduced by analytics and modelling, and data can be used to manage data (e.g. by analysing traffic to adjust spectrum access). This self-reflexive quality can open the door to new forms of 'smart spectrum regulation' in which many of the competing policy considerations (from efficient use of scarce resources to reconciling competing use priorities or protecting communication privacy and security) can be dealt with endogenously, automatically and in ways that are transparent but hard to manipulate.

Our conclusion is that EU/US research collaboration should mainly focus on understanding our common challenges and the ways in which those aspects of these technologies that span our two legal, commercial and societal environments can be equipped both to robustly work around the world and to support joint research that exploits these technologies to resolve common problems ranging from food security and environmental damage to financial trading and privacy. Among the various aspects, the possibilities and implications of agility in spectrum allocation and management constitute perhaps the most promising research area.

Lessons learned from Digital Communities

5G networks, Big Data and IoT hold great promises to further integration and facilitation of Digital Communities – whether they are in close geographic proximity, or consist of geographically dispersed groups with a common interest. However, in order to allow all communities to benefit from the new potential it will be crucial to:

- 5G networks: Ensure that in regions with lower geographical density proximity of people and devices get adequate access to communication services that both serve low latency, high mass needs as well as critical communications, and high bandwidth communications. As we learned from the past, this may not go automatically. Different than in the past is that availability is not solely depending on major network operators, anymore: local networks can be set up and connected through backbones with the world, where needed.
- Big Data: Benefiting from the data driven economy as such is less related to access to networks as to access to data. For some applications, amounts of data will be such that high bandwidth is required, or time criticality will require high reliability of networks. But most of that is related to exchange of data between devices in IoT networks (Cyber Physical Systems). Big Data can support any community in enabling applications as well as feedback loops comparing data of activities within any Digital Community with data from other Communities. Geographic proximity is not an important factor here.
- IoT/CPS: the applications that would serve digital communities, both those in geographic proximity as more geographically dispersed communities, are many and more to come. Mostly, these applications will be developed for specific sectors, such as crop maintenance, disaster warning systems, health maintenance and home care, etc. etc. More research can be done how applications can be used across sectors, and across communities: i.e. learning from practice and innovation in application next to innovation of the underlying technologies itself.

All together it is clear that with the development of 5G networks, Big Data applications and IoT applications, geographic proximity matters less, and communities (community formation as well as coherence) matter more. Learning from practice is a huge opportunity for both EU and US researchers, as is working together on the underlying technologies to ensure they are secure enough, allow interconnectivity, have privacy addressed from the outset and make good use of available spectrum.

Strategic proposals for the way forward

Considering all we learned during the course of the study, we conclude with the following strategic proposals for possible ways forward, that we believe will be supportive to effective, further enhanced ICT R&I collaboration between the European Union and the United States of America.

1. *Privacy*: Solutions need to be found to allow services to develop that respect (European and US) privacy and data protection frameworks and – where appropriate – challenge their provisions. This will require policy collaboration that is looking forward to joint and sustainable solutions aimed at ensuring an even higher level goal than preserving privacy: that of preserving "human dignity" in a digital age, ensuring that we can still live as humans in our digital environment

   a. These approaches should not treat current laws as fixed constraints, but as natural experiments that can shed light on how to improve the ethical character of law and practice, and at a deeper level on the ethics of privacy itself;
   b. As part of this, the adequacy of principles such as user empowerment, consent and restricting privacy policy attention to data protection should be examined theoretically, practically and empirically.

2. *Security*: Recognising basic security is key to whatever we want to ensure: set up joint EU/US research collaboration to develop biologically inspired security. With IoT and underlying interconnections, there's a significant risk with IoT devices providing a back door to enterprise systems and data. Using biological constructs (in particular those relating to immune responses and contagion), we may be able identify attacks before they become widespread and respond in a proportionate and dynamic fashion by directing resources to the appropriate area. As part of this

   a. Security roles and responsibilities should be explored as negotiable, flexible and layered, especially as regards technological, operational, commercial and regulatory domains; and
   b. The common aspects of security and privacy (both of which concern access to information and the functions and systems it enables) should be recognised and a common technical, operational, business and legal basis explored.

3. *Standards*: Stimulate participation of sponsored research and innovation in global (IETF, ITU, IEEE etc.) rather than regional standardisation platforms for EU/US collaboration. As part of this

   a. Standards at various levels (e.g. technical, operational, functional, legal and ethical) should be developed explored in one forum to identify and exploit their possibilities as complements and substitutes; and
   b. The interaction of standards with other activities (especially innovation, but also business and regulatory policy development) should be examined and actively pursued by strengthening the 2-way links between R&I and standards bodies.

4. *Spectrum*: Set up joint EU/US research collaboration on developing agility in spectrum allocation and management to ensure that ubiquitous connectivity enabling digital services to work becomes possible, not being held back by (slow and ineffective) spectrum allocation negotiations. As part of this

a. Flexible combinations and forms of licensed and unlicensed use should be designed and explored experimentally; and
b. A clear and consistent economic, regulatory and technical basis for evaluating spectrum policy should be agreed between the US and the EU, especially to mediate the claims and requirements of different spectrum-using technologies.

5. *Communities*: Support exchange of good practice experience between Communities in EU and US; many societal challenges are common to both regions and different types of communities and the potential of many solutions that have already been devised for adaptation elsewhere and optimisation *in situ* remain under-explored. As part of this

a. Efforts should go beyond a conventional compendium of good practices and case histories, to encourage curation and improvement of the dispersed body of community knowledge and to enable intentional experiments spanning many different community concepts; and
b. Complementary, social scientific and/or multidisciplinary transatlantic R&I collaborations should be undertaken to ensure that community implementation and evaluation and the impact of policies on digital community formation and function are understood.-

-

Annexes

Annex A. Security considerations

Conceptual considerations

Data and its uses and abuses

The economic and commercial significance of data led to three strands of data economics.

1. *The economic value of data*. Policy often treats data like other assets, regulating their use by property rights to data themselves. For personal data, these rights may be fundamental or economic[109]. The data economy literature deals with personal data, IPR and clinical trial data, commercial secrets, etc. Rights and regulations are adapted from other contexts, including domains (e.g. financial trading) where data are the principal source of value. This is linked to individual security, because policy that enhances the security of data controllers' claims strengthens their ability to bear responsibility. It is also linked to collective security; data as a public good[110] derives value from controlled *access* rather than *consumption*; it is an aspect of societal security like environmental, food, energy and defence security.
2. *A data-driven economy*. Connecting people, services, etc. by *data flows* irreversibly changes socioeconomic structures, and the performance of societal mechanisms (e.g. markets, governments, laws and voting). Traditional regulation of the economy by market trades, national regulators and formal and slow trade policy is everyday refuted by experience. This calls into question economic policies like competition, taxation and consumer protection rules and their use to address other issues[111]. Complex, massive and high-speed data flows cannot easily be governed by traditional 'crash barrier' rules, which complicates the design and analysis of security policies[112]. It also creates new insecurities; doubts about the quality and reliability of information and the accuracy and fairness of others' decisions weaken the benefits of trustworthy systems.
3. *New uses of data*. The use of algorithms and ML creates some new security issues e.g. around algorithmic regulation. Such systems are very hard to understand or regulate *ex ante* or *ex post*; algorithms are often regarded as a 'secret sauce' to be jealously protected, but disclosure is needed if regulations are to be adapted. Policy-relevant outcomes also depend on how data and algorithms are combined and interactions among 'pockets' controlled by different entities; for some of the most important cyber-security issues, no-one is in control, no-one understands what is happening and no-one can usefully be held responsible.

Definitional issues

How does system security follow from data security? Cyber-security rests on data and processing; fake news and compromised algorithms produce widespread and consequential insecurities. Cyber, data, system, legal and commercial security are distinct concepts, understood differently in different contexts (including EU-US) and a potential focus or stumbling block for collaborative effort.

How do rules relate to behaviour? Policy rules must anticipate the actions of affected parties. However trusted and trustworthy the architecture of a system, outcomes are determined by real people, organisations and nations. Our legal and regulatory frameworks evolved independently of the current Internet; existing laws and legal principles (e.g. consent as the primary basis for coercive regulation) cannot fully 'handle' all issues arising on and in relation to the Internet but are affected by changes linked to the Internet.

Identification and authentication

Authentication or identification are sometimes *necessary* to hold users responsible or insulate from liability those who accept identity in good faith. Even where technical means of identity verification exist, it may not be ethical or efficient[113] to rely on them to assign or shift responsibility. Stronger identification can make mistakes less likely but more serious and harder to correct. Identification may be used even when it isn't necessary. Therefore, security rules or standards should be differentiated based on the 'security sensitivity' of *combinations of* individuals, technologies, services and contexts. As a result of such complexities, there is no internationally-agreed identity system that does not suffer from validity and security problems, patchy use[114] or serious social objections. But lack of a universal system makes it difficult to determine responsibility and thus to discourage malware and fake news or properly to extend money laundering, taxation, etc. laws to networked environments.

Cyber-crime and cyber-enhanced crime

Another security-related policy area concerns cyber-crimes. Many nations' legal systems make it difficult to take such cases to court, prosecutions do not deter future crimes and legal decisions from other jurisdictions are not mirrored or recognised. This has led to the perception that laws do not recognise cybercrimes or provide legal tools to counter ICT-enhanced conventional crimes. This perception is not generally correct[115], though the initiatives mainly address new, specifically cyber, crimes. Within these overall provisions are new categories of crime linked to specific technological domains. Examples include: DDOS attacks on 5G networks, including functional degradation, etc.; Ransomware/DDOS attacks on Data Analytics facilities, esp. those linked to e.g. algorithmic trading, analytic engine or data centre compromise; and interference with autonomous devices and CPS control systems, as illustrated by the Stuxnet[116] worm that specifically targeted programmable logic control systems in industrial processes to degrade system operation and damage or destroy industrial hardware.

Policy will increasingly have to adapt to technology-linked changes in the law enforcement landscape; facilitating or impeding existing crimes[117], evidence-gathering and analysis and payment services for criminal enterprises.

Encryption

Encryption is another area of tension where policy and technology address similar problems albeit sometimes with different objectives. Encryption can secure data held by public authorities and communication in insecure environments. Service providers and users employ encryption to protect information (including IPR and personal data) against espionage, hacking – and against legitimate law enforcement, security and regulatory access.

As a technical means of access control, most encryption applications are agnostic as to contents and uses; they lack the subtlety of contracts or regulation while offering potentially greater protection. Neither approach is necessarily stronger or more transparent. Businesses may prefer shifting liability to consumers to taking effective precautions, which is why cumbersome passwords have thus far dominated secure biometric technologies (even for banks and payment service providers) and instances of identity theft rarely result in compensation.

One approach is to legitimise certain forms of access and legislate to regulate them.

Example: The UK's Investigatory Powers Act 2016 seeks to accomplish three overall objectives:

- To consolidate powers already available to UK law enforcement, security and intelligence agencies to obtain the content of, and data about, communications;
- To overhaul the mechanism for authorising and overseeing these powers; and
- To ensure that powers afforded in existing legislation are fit for the digital age.

The Act had a controversial passage through Parliament because it gives government agencies far-reaching powers to require technology and communications businesses (inside and outside the UK) to retain their customers' personal data. Its two most relevant provisions are:

- Bulk powers and encryption removal: The Act gives certain government agencies access to large volumes of data through bulk interception and bulk equipment interference warrants, provided the main purpose is to acquire intelligence about individuals outside the UK (even when the conduct occurs within the UK). Similarly, interference with the privacy of persons in the UK is only permitted to the extent necessary for that purpose. When served with a notice, *communications service providers* may be required to remove encryption to assist in giving effect to interception warrants. The Act also future provides for future regulations to oblige technology providers to remove encryption.
- Overseas enforcement: The Act allows enforcement of certain obligations and powers to be against overseas companies through proceedings for an injunction or specific performance, together with local enforcement in the applicable overseas country using appropriate bi- or multi-jurisdictional enforcement agreements.

Such provisions – in particular 'official' repositories for potentially-accessible information or enhanced access requirements for data stored and 'in transit' - raise the possibility that those means of access may be employed by unauthorised entities, including other governments and their agents. This is not limited to law and security; similar risks and ambiguities arise in contract and tort law – it is not always clear who, if anyone, is liable for potential violations of security when data storage, transmission and processing cross nation boundaries.

In recent years, the complexities of enhanced access have become evident through e.g. the Apple[118], Microsoft[119] and Google/FBI[120] cases. In the US, access requests are often linked to the 'all writs' act under which the US demanded decryption (or access to the plaintext).

For EU-US collaborative R&I and security policy, the key points include the following:

- Many issues involve technology supplied by one region and used to provide services in another;
- Increasingly, the EU and the US face security threats that target EU *and* US entities, systems, services and users but originate or are based outside both (e.g. China and Russia);
- Legal and policy developments reflect *extraterritoriality*:
  - data held in one region may are sought by authorities in another,
  - communications or technology service providers are asked to cooperate with other regions' authorities,
  - access to data about a region's citizens or businesses by their authorities may reveal data of another region's citizens or businesses due to joint records, server farm location or 'incidental surveillance' and
  - tax and product liability rules create a desire to conceal information that spans oceans.

A dialogue between technology and policy

Engineers tend to think of security as something that can be designed to be user-friendly and hardened against identifiable attacks and abuses. Policy analysts would respond that it must first be decided whether technology will make its contribution before or after policy and the economy have acted. If technology 'moves first', policy can set regulatory limits; if policy moves first, technology can fix gaps and problems created by market[121] and regulatory inadequacies[122]. Because technology and law do not move in sequence, each domain should articulate

design principles to manage their interface. This section discusses some technological security principles[123] from a policy standpoint, to kick off a dialogue on device-level security and the architecture of standards and law.

Product security in the Internet of Things

Security at device level is essential to progress towards a dependable environment. The interconnection of devices into dynamic cyberphysical systems makes the following aspects particularly important.

Design it right

1. *Be paranoid*, by conducting risk assessments and mitigations for everything that could happen;

   Rejoinder: this requires a suitable Precautionary Principle and analysis of ways to share risk, information, cost and (inevitably) liability. It thus needs assessment methodologies, to deal with unquantifiable risks, mitigation priorities and precautions against adverse selection[124] and moral hazard[125].

2. *Standard technology is better than home grown,* to maximise interoperability, scale economies and learning.

   Rejoinders:

   - don't design everything (some things should be left as is or left to evolve unless and until more is known);
   - standard technology may be vulnerable to standard attacks, attacks motivated by the spread of vulnerabilities or simple contagion (esp. reuse of standard approaches in very different apps);
   - using standard approaches to cut liability (Safe Harbour principle) exacerbates monoculture risk; and
   - Security and competition objectives may conflict[126].

3. *The more eyes the better*, to ensure that general risks and emerging patterns are picked up, involving:

   - *Shared penetration tests because* a lively and aware whole-ecosystem approach is far superior to localised or controlled tests, provided it can be secured against manipulation; and
   - *A culture of responsible disclosure and collaboration*.

   Rejoinder: information sharing changes competitive and cooperative relationships. It is necessary to bring competition authorities into the discussion to guard against capture, foreclosure and corruption; competitive efficiency and dynamism should no more be sacrificed to the 'God of insecurity' than privacy and civil liberties. Also, not all 'eyes' are equally trustworthy; commercial partners may strategically use, withhold or distort reviews and reports and the knowledge of surveillance may directly undercut trust. This has been seen at international and systemic level in relation to the well-known 5 Eyes and 14 Eyes initiatives.

4. *Build a safety net and a future*, including making sure that all systems can be monitored and updated *in situ*.

   Rejoinders:

   - It is also necessary to spread costs and responsibilities;
   - Do not go too far; 'push' updates have crashed systems, bricked devices and imposed huge costs; and
   - Where systems are tightly interoperable, highly optimised and vital or mission-critical, rapid updating (even for security) can be catastrophic, especially after extensive bottom-up or user-led innovation, because those deploying upgrades may not know enough to anticipate and manage consequences.

5. *Rough consensus and running code* (the architecture of policy) - it has long been recognised that rapid development mandates a 'don't get it right, get it done' ethos which optimises learning from experience.

   Rejoinders:

   - Why should 'rough consensus' be applied to standards (which may be 'sticky') while Precautionary Principle applies to technology (which can be modified, upgraded or abandoned)?
   - There are 'soft' ways to implement these; law offers certainty, contracts offer adjudicated flexibility.
   - This might work better in Common Law jurisdictions; smooth consensus can lead to inoperative code.

- The right approach depends on interdependencies; ICT has largely used one of two polar approaches:
  - best effort, which is friendly to experimentation and meritorious or instructive failure; or
  - weakest link (advocated for irreversible global risks), more associated with Precautionary Principle.

  But a synthesis can be created through the design of a system of 'natural experiments.'

Annex B: Standards

Drivers

ICT standardisation has technical, social, economic and political drivers. In general, the technical community seeks interoperability, stability and security of the Internet; business R&I aims to serve markets conducted over the Internet. For them, R&I needs ultimately to contribute to sustainable profitability by creating and defending market niches and/or growing shares in existing markets while minimising development and operational costs[127].

Going a bit deeper we note that, next to industry and governments, much of the work that has led to today's Internet was voluntary, performed for minimal or no remuneration and often at a great personal cost. Since the beginning of the Internet the technology community has been motivated by curiosity *and* an interest in developing something that works; as it spreads, this has been extended by social and other motivations for the activities of others enabled by the democratisation of design and programming. This mix of drives has produced the current Internet's achievements and shortcomings in terms of stability, interoperability and functionality.

This desire to improve the Internet also drives many participants in Internet standards organisations like the Internet Engineering Task Force (IETF). Although a large part of the technical community works for corporate entities, many chose to do so in order to work on specific components, technologies or topic areas in which they have become experts and to which they have devoted their professional lives. Many, if not most, of them value technical "correctness" above the narrow interests of corporate sponsors or employers. One often sees employees of the same company at odds with each other within a technical standards organisation e.g. when one is loyal to a qualitative open standard while another favours a closed proprietary standard. This can be seen as a conflict of preferences for aggregate societal benefits or the interests of indirect stakeholders vs. those of suppliers or as a conflict between ethical principles. At the same time, there is growing evidence of corporate efforts to control and influence research (in public institutes to which they donate) and technical inputs to policy (including standards). The fact that the scientists involved are not actively seeking to promote commercial interests does not necessarily 'sanitise' the efforts of these corporates with sometimes high commercial stakes.

This does not rule out an element of corporate social responsibility (CSR), spanning financial return (which may be devoted to other 'good works', the adoption of welfare-enhancing standards and the accumulation of policy influence. This does not mean render financial considerations irrelevant; even social enterprises must pay their suppliers, investors and personnel. This net revenue may come from end users paying for products, public or civil society funding of groups or initiatives seen as supporting society or from specific interest groups. In addition, CSR is known to bring market rewards through enhanced reputation and regulatory forbearance.

Social drivers

Social drivers for standardisation are linked to the level and importance of communication and online sharing of data and services. Individuals and the groups to which they belong are part of many networks, so interoperability receives high priority and co-determines technology interfaces and services – indeed, platform enterprises and service models have emerged precisely to exploit this market for interoperability. A related, increasingly salient concern is the non-neutrality of technological standards. The Internet's architectures and protocols are widely recognised as having profound good and bad effects on society. Standards work increasingly takes account of

the potential of protocols and architectures to influence: civil and political rights; freedom of expression and association; economic, social and cultural rights of access to knowledge; rights to participate in the life of the community; individual and cultural rights of self-determination; and the right to participate in government and free elections. One example of socially driven standardisation is the consensus decision by the IETF to make security and encryption the default in their protocols in the light of pervasive surveillance.

Technology drivers

As mentioned, technical standards are in large art driven by a desire to guarantee the stability and function of the Internet, in particular via interoperability. Internet standardisation enables permissionless innovation of applications, technologies and services that build upon existing infrastructures to deliver services as part of a larger system of services and/or directly to end users. In essence, standards facilitate evolution by enabling small or localised innovations to function within larger systems and increase the competitive contact between firms and by enabling small and/or innovative firms to participate.

Standards allow developers offer "things" that can be used immediately, while making it easier for something better to replace them if they fail to deliver the quality needed or fall behind emerging needs. According to Patrik Fältström (Chair of ICANN's Security and Stability Advisory Council), security is not prioritised because time to market is such a major sales driver; rather than emerging from an extensive and prolonged testing process, products are put on the market to be tested in "real-life" circumstances. Another reason why security is often set aside is that it requires extra code and testing, increasing capital expenditure and (usually) price. Moreover, security is only valued if it protects against 'clear and present danger.' If customers cannot not be convinced that they need the extra overhead of security, they will balk the complexity and price. The system has responded with cyber-security insurance, but the ever-changing threats and the risks of 'security monocultures' have limited the emergence of standard coding and operational 'best practices' analogous to those for more stable risks.

Internet protocols are often refined in step-wise fashion. Proposers must show running code to get standards accepted; they therefore often release products with nonstandard and incomplete implementations in an attempt to capture a new market. The standardisation process then requires consensus on a first version, which means that original code and first-to-market products must to be changed to support interoperability. Later, as experience with the standardised protocol accumulates, it may be further refined.

Standards bodies (and providers with a large installed base) always try to maintain backwards-compatibility, but this is not always possible. Sometimes, large-scale updates over the Internet are required. This can only work if older versions of products using the protocol can be updated or replaced when needed. This imposes both risks and costs far beyond those most closely connected to the original protocol, and can lead to generational lags that threaten large systems[128].

This was the case with Wannacry, which affected obsolete software used in large, cash-strapped systems used to deliver key public services. Updates should be pushed automatically, but tested before implementation. Where this is infeasible, the patch may do more harm than the problem it addresses. In addition, automated patches may themselves become an attack vector; the situation is complicated by software/hardware interdependencies, the conflicted ownership status of the associated risks and the fact that information needed to assess challenges and assign responsibility or blame may be masked by attacks and/or failed patches.

Economic Drivers

Standardisation can be driven by scale, scope and network economies and the desire to constrain abuses of market power without damaging efficiency and innovation. Standards reduce uncertainty that limits investment in common infrastructures and general-purpose technologies and innovation by improving the chances that the resulting goods and services will rapidly become available to and used by a critical mass on the network. Beyond this, standards have the effect of establishing and clarifying market boundaries, potentially improving both

performance and regulation. But this openness and ease of switching come at a price; users may switch to compatible alternatives "too fast." This can produce three distinct harms:

- Fixed costs may not be recovered and firms may concentrate on features that drive switching (visible characteristics like price) rather than those of greatest long run value (quality, security or customisability);
- Easy switching may choke off less-obvious forms of value creation, for instance when users discover new uses in their particular context or adjust their own processes to the possibilities offered by products. Such discoveries take time and will be lost if it is too easy to switch to slightly-better but incompatible products;
- Switching between apps that share a standard when the application interface (API) is not stable and backwards-compatible is almost certain to weaken investment in maintaining and improving complementary "platforms" because
    - it reduces the returns available to app developers that are shared with platform providers and
    - it may constrain improvements to platforms that would require a change of app-level standards.

In the face of these risks developers and providers tend to prefer proprietary standards that lock in users by making it impossible or painful to switch to technologies from other providers. Further down the road, this way of creating and exploiting market power may provoke inefficiently strong regulatory responses and limit standardisation's self- or co-regulatory role. One strategy is for a market leader or disrupter to release products with a proprietary protocol and only then to seek acceptance by a standards body. This gives a market leader or disrupter a first-to-market advantage that can last for months or even years.

Beyond this essentially static view lie some interesting dynamic drivers. As new technologies are developed and new products offered, standards will have to adapt to support new requirements for access and interaction (including new limits driven by security, privacy, regulatory imperatives and economics considerations). This "standards ecosystem" is itself evolving as individual and linked clusters of standards change, wither or converge.

Organisational roles

The role of standards organisations

Standards organisations can be classified by their role, position and influence on the local, national, regional and global standardisation arena. They can also be categorised based on whether the power to set the terms of reference, frame alternatives and make final decisions rests with the technical community, industry, intergovernmental and/or civil society organisations.

By geographic designation, there are international, regional and national standards bodies. By technology or industry designation, there are standards developing organisations (SDOs) and standards setting organisations for specific purposes (SSOs), also known as consortia. Standards organisations may be governmental or involve government participation, endorsement or support[129]. SDOs are often institutionalised and sectoral in nature, whereas consortia are often more dynamic, set up for specific purposes (such as 5G).

Most SDOs have specific rules to facilitate development and consensus on standards. In respect of standards related to the global internet infrastructure, different SDOs are often have responsibilities that focus on specific layers of the architecture. For example, the World Wide Web Consortium (W3C)[130] is focussed on the web, the Internet Engineering Task Force (IETF)[131] deals with logical infrastructures such as the Internet's transport and applications layers and organisations like the IEEE[132] concentrate lower layers and physical connectivity.

The role of governments

Governments generally leave it to industry to generate and control standards. Governments are mainly interested in ensuring that processes, procedures and legislation work for standards and (ideally) step in only

when needed to protect the public interest and when for legislative and other governmental purposes. In general, the role is minimalist and supportive rather than directive. At the same time, governments are keenly aware of the economic and policy importance of the 'right' standards and support economically advantageous industry standards; this may lead to standards competition between regions, or standards that constitute disguised trade barriers and standards that reinforce 'picking winners' industrial policy, unless explicitly addressed. The network of mutual recognition and cooperative development links among national standards bodies provide an official basis for authoritative standards. This reinforces their public value and encourages adoption by ensuring that standards give access to public markets and demonstrate regulatory compliance.

For instance, the UK Government is relatively active in the domain of ICT standard making. The British Standards Institution (BSI), recognised as the UK's national standards body, covers part of the ICT area. The Government also sponsors research and liaises with SDOs at the standards policy level via ETSI's board, the ITU, the EU ICT Multi Stakeholder Platform (MSP) etc. The Government believes that targeted in-depth participation is needed to get the best results in standards making and recognises that building up confidence is key to getting influence.

Governments may want to make sure areas of public interest are covered, as generally industry does not invest in areas where there is no business case. Governments can also influence other Governments to back standards at international meetings and in intergovernmental organisations e.g. OECD, WTO and G20/G7 meetings. Governments' primary participation in standardisation is often done through intergovernmental organisations like the International Telecommunication Union (ITU)[133] where they work in cooperation with industry.

EU perspective

Within the Digital Single Market, the European Commission pursues harmonisation of the European ICT industry by funding joint R&I and public procurement of ICT, sometimes leading to "European Standards".

The EC does not have many enforcement/regulatory tools for standards development. The Public Procurement Directive 2014/24/EU provides rules for how standards are used. Article 42 of the Directive says that the EC can only require bidders to comply with European or national (Member State) standards.

The EU 1025/2012 Regulation on European standardisation endorses the WTO principles of coherence, openness, consensus, transparency, voluntary application, independence from special interest and efficiency and promotes Open Standards.

The EC's overall framework for standardisation activity is based on Regulation 1025/2012, "ICT Standardisation Priorities for the Digital Single Market" (COM(2016)176), the annual Union work programme for European standardisation for 2017 (COM (2016) 357) and the Rolling Plan for ICT Standardisation[134], a multi-annual overview of needs for preliminary or complementary ICT standardisation in support of EU policy developed by the Multi-Stakeholder Platform on ICT standardisation and the Joint Initiative on Standardisation.

US perspective

US government agencies play various roles depending on their mission. These include: technical contributor to standards development via e.g. NIST (approximately 30% of the almost 1200 technical staff participate in the development of consensus standards); enforcement agency e.g. through competition agencies; or standards consumer, e.g. the Department of Defence.

Federal government agencies' participation in private sector-led standards development is strongly encouraged by policy[135]; federal agencies' participation makes SDOs aware of government standards needs and enables agencies to encourage standards suitable for government uses or supportive of government policies. The NIST approach combines: lightweight agreements; participant responsibility for securing resources; virtual meetings; open documents; a voluntary and consensus-based approach; a focus on existing technologies and deployments; and technological and business-model neutrality.

The key objectives of U.S. government participation in standardisation activities are to ensure development of standards that are timely, relevant, cost-effective and in conformity with regulatory, procurement and policy

objectives. The government wants to ensure that standards and standardisation promote and sustain innovation and foster competition. By engaging in standards development and related activities, the US government also seeks to champion approaches that support growth and competitiveness, market access, non-discrimination, trade, technology, innovation and competition and to encourage other countries to live up to their international obligations relating to standards development and their use.

Annex C: Spectrum

IoT and CPS from the spectrum perspective

This annex is provided to 'drill down' into the above discussion of spectrum policy issues as they relate to IoT/CPS in order to differentiate the two.

Internet of Things

The **Internet of Things** is a network of physical objects containing embedded technology that enables them to communicate, sense or interact with their internal states or the external environment. Depending on what aspect is to be discussed, this definition in terms of 'thing layer' can be extended to include related layers e.g.:

- (tech layer) efficient wireless protocols, improved sensors and cheaper processors; and
- (user layer) consumer, business and industrial Internets.

The 'vertical' linkages among these layers enable a *potentially* open, global network connecting people, data, and things. However, it is not obvious that all such connections will or should be made:

- The openness, geographic reach, range of connected entities and possible or permitted uses will fall some way short of what is technically feasible;
- These limits may be efficient or inefficient from the perspective of multiple stakeholders; and
- The realisation or inhibition of these possibilities will in turn affect the evolution of the Internet.

The IoT often uses the platforms to connect 'intelligent' things that collect, process and transmit a broad array of data. These platforms allow entities from the 'thing', 'tech' and 'user' layers to 'find' each other and interact; to do this, the platforms may host people, organisations, applications and functionalities. This platform capability helps to create services that would not be obvious without this connectivity and analytical intelligence. Therefore the development of the IoT is linked (at present) to the characteristics, economics, operation and governance of platforms and in turn to transformative technologies such as cloud, things, and mobile.

Cyber-Physical Systems

Cyber-Physical Systems (CPS) represent 'next generation' embedded intelligent ICT systems that are interconnected, interdependent, collaborative and (to an extent) autonomous. They provide computing and communication, enabling monitoring and control of physical components and processes in various applications, creating "one logical system of objects and services". Their development can be described in stages.

1. Creation and interconnection of virtual 'models' of physical systems (often as computer simulations) to facilitate operation and control – a 'twinning' of the cyber and the physical;
2. Allowing each of the cyber and physical planes to go beyond their counterparts;
3. Enabling and exploiting joint capabilities (including emergent functionalities) that could not be implemented in either a purely physical or a purely cybernetic system; and
4. Restoring the understanding of the cybernetic plane to its original definition (Weiner, 1948) as "the scientific study of control and communication in the animal and the machine."

From this perspective, we can delineate some requirements of future CPS. They will need to be:

- *Appropriately* scalable, distributed and decentralised;
- Capable of interaction with interaction with humans, physical and societal environments and machines while being connected to Internet or to other networks; and therefore
- Endowed with a range of features or functions such as adaptability[136], reactivity, optimality, resilience and security – and possibly even pro-active or first-mover' versions of these.

These features may be embedded, designed or simply emergent, because CPS are already forming an invisible 'neural network' of our society and will do so even more in future.

Link to spectrum

The way the IoT and CPS will develop and the effects of that development will inevitably be shaped by the communication and interaction possibilities – hence the link to spectrum policy. In particular, the demands of the thing and user layers of the IoT, filtered through the tech layer (esp. wireless protocols) will determine their demands for spectral resources and the coexistence possibilities with other uses. This topic requires careful investigation due to its feedback loops; the availability/scarcity and 'cost' of spectrum will drive both the design and the competitive evolution of IoT devices, which will in turn impose constraints on other uses and on the form of spectrum rights and allocations. This is particularly pressing because 'things' are likely to be so many, so small and so complex in terms of ownership and control that treating them as 'rights-holders' in the standard spectrum management sense will be unworkable.

This challenge is, if anything even sharper for the second and third stages of CPS development, because the 'cyber' aspect can be implemented in a distributed way via wireless connections that can go well beyond what may be physically possible. This transcendence is specifically linked to wireless connections, which are less tightly coupled to a physical plane of wired or fibre infrastructure and its far more limited possibilities for sharing and changing 'rights of way'.

TV White Space (TVWS)

About a decade ago, TVWS seemed a promising and revolutionary resource that had the potential to take the success of Wi-Fi to a whole new level, using radio bands that could travel farther and better penetrate walls, buildings, and other obstructions. This proved technically challenging due to the 'coexistence problem':

- If white space devices (WSD) assess channel availability when there is a very weak signal from a TV station (esp. DTT – digital terrestrial television) very far away, they may create interference;
- High-power TV broadcasts can interfere with or even saturate WSD receivers operating properly on adjacent vacant channels; and
- WSDs properly operating on vacant channels can interfere with nearby TV receivers tuned to an adjacent TV channel.

Technical 'fixes' (devices that looked for and used unoccupied space) proved ineffective, so most countries (including the US and the UK) opted for a database (WSDB) approach.

These databases identify channels that can safely be used at a given location and time without interfering with incumbent users (TV, low-power wireless microphones, etc.). WSD certification requires compliance with radio emission standards and WSDB interfacing requirements.

Regulatory approaches being used or developed range from requiring licence holders to maintain WSDBs and make them available to requiring them to provide the information to regulatory authorities, who will in turn make them available.

The database approach is being used to some (limited) extent in at least 18 countries in US, Europe, Asia, and Africa, but has not yet 'taken off' – in part due to the lack of a suitable international standard.

There are some standards, such as IEEE 802.22 for the rural market and 802.11af for the Super-Wi-Fi market, but they have not been adopted by industry and no dedicated low-cost Application-Specific Integrated Circuits (ASICs) are currently available, though several have been developed. TVWS vendors have therefore tended to rely on general-purpose processors, which offer the flexibility required for this emerging market.

There are also some interesting clashes between different sectors; Microsoft has put a lot of effort into encouraging the use of TVWS for rural broadband delivery, but major telcos are less keen – perhaps because the frequencies are inconveniently low and because there are limited opportunities for 'ownership'[137].

Beyond this, it is worth noting that various countries are developing regulations (US, Canada, UK, EU, Singapore), but regulatory initiatives are far less visible in the developing world. The UK provides a good example of the approach being taken in many developed countries; Ofcom has built TVWS explicitly into their plans by:

- Committing to unlicensed access;
- Implementing regulatory requirements to disclose and publicise available TVWS spectrum via public databases; and
- Studying and making arrangements for 'coexistence' between digital terrestrial television and TVWS devices.

Other initiatives underway for using this 'digital dividend include:

- Anatel in Brazil and SRFC in Russia adoption of the 450 MHz band for 3GPP as LTE band 31, which will compete with other bands for rural markets; and
- The FCC is considering the 600 MHz band (providing almost 100 MHz of TVWS spectrum) and other countries are expected to follow suit.

Annex D: future developments

This section provides a slightly more detailed discussion of some of the future developments used in Chapter 3 to contextualise our findings.

Trends

The Sharing economy

This term refers to "an economic system in which assets or services are shared between private individuals, either free or for a fee, typically by means of the Internet." [138] Its growth requires *user convenience*. Interoperability related standards will be market driven, while for safety and quality for quality and safety there is regulation in place, such as consumer protection regulation etc. The sharing economy has grown significantly, taking in cars, bikes to power tools and services (e.g. UBER and AirBnB). Many well-established industries have been transformed into new models built around this concept and approach towards consumption of goods and services. This degree of sharing beyond the well-worked bounds of formal contracts and transactions with or among legally defined corporations raises new challenges in all of the domains listed above. For instance:

- The privacy protections built into laws such as the CLOUD Act and GDPR primarily bind commercial and government entities – even where their language is broader, they are unlikely to be enforced on individuals in informal arrangements, as can already be seen in the struggles of governments to bring them adequately within scope of such visible and easily-quantifiable domains as labour law. The most common way forward is to attempt to hold ISPs and other enabling bodies responsible, but it is not obvious that this can be done in an effective and proportionate way, especially across international boundaries or in respect of informal, small-scale and local interactions or that it can be extended to informal *ad hoc* networks. These may be relatively insignificant at present, but it is at least possible that

the existence of regulatory lacunae will encourage a migration that weakens legal protections. On the positive side, sharing economy interactions allow the formation of localised and fully consensual conventions around privacy that can operate in a far more light-touch and equally informal manner that may be friendlier to innovation, the evolution of privacy norms and the protection of individual privacy and other interests outside or opposed to data protection.

- When assets and services are shared, so too is responsibility for the security of systems used for sharing; while privacy may operate on a best-effort basis, security is often both subjective and subject to weakest-link dynamics. In sharing economy settings, it may be harder to identify the parties best placed to bear risk, to assign responsibility and to monitor and assess their behaviour. Even the existence of sharing economy networks may be imperilled by security threats, whether they arise from technological or operational flaws or from human frailty or ill intent. On the positive side, in such contexts it may be easier to view security as a local public (or 'club') good and to develop informal mechanisms to supplement the protections offered by law, technology and managerial practices.
- This fast-growing and constantly changing marketplace requires standardised but customisable platform facilities and tools to help aid policy development and better protect users, consumers and industry – ICT standards are a key enabler in this.

Technologies become invisible

Ambient intelligence brings computational capacity to everyday environments and makes them responsive to people. It requires *seamless* interoperability and connectivity. Ambient intelligence (AmI) research builds upon advances in sensors and sensor networks, pervasive computing and artificial intelligence. Recent growth in these contributing fields has strengthened and expanded AmI research. As it matures, the resulting technologies promise to revolutionise daily human life. But this ubiquity requires high levels of low-burden interoperability and thus interchange standards. For better or worse, it will also facilitate privacy and surveillance, changing the expectations underlying privacy and security laws and requiring different types of standard.

Blockchain

As used here, this term indicates a ledger without single owner, which provides trustless authenticity. It is not clear whether this facilitates secure interoperability, or indeed how people can rely on such unsecured structures. The transactions recorded in such ledgers are globally published, generally in unencrypted form.

- If they involve personal data, this creates regulatory and legal problems. An obvious solution is to store only encrypted data, but the data may not be accurately recoverable if decryption keys are lost or corrupted; if keys are stolen and published, all the data is forever decrypted in the blockchain since the data cannot be altered. On the other hand, blockchains can be used to protect data; they decouple security (in terms of immutability) from privacy. It is possible to design immutable, tamper-resistant transactions, but they can be seen at every node in the network[139]. This may not fully address the problem; privacy-enhancing technologies still produce metadata, so statistical analysis will reveal partial information. Even if, for example, the data are encrypted, this will allow pattern recognition by means of machine-learning. These solutions also do not currently scale; the consensus process used to maintain the integrity of the blockchain is currently too expensive – and too slow. Ethereum is currently capable of 2.8 transactions per second, while Bitcoin manages only 3.2 transactions per second, due to the time needed to validate consensus on each transaction by means of proof of work or proof of stake.
- However, blockchain can also help to improve defensive cyber-security strategies, especially in terms of identity and access. For instance, cyber security can be compromised by a man-in-the-middle (MITM) attack enabled by getting a Certificate Authority (CA) to provide a user with forged public keys (Public-Key Substitution MITM attack). This can enable decryption of sensitive information – or worse. A partial solution is for users to put their public keys in published blocks, which are distributed over participating nodes with links to previous and following blocks. This renders their public keys immutable and makes it harder for attackers to publish falsified keys. In addition, the CA, representing a single point of failure, is distributed, making it much harder to bring the service down.
- As far as standards are concerned, the Standards Australia report on the work of the Secretariat for ISO/TC 307 surveys efforts to shape the future of international blockchain standards. Their close

collaboration with stakeholders and the standards development activities undertaken by ISO/TC 307[140] will be informed by the Roadmap for Blockchain Standards and the recommendations contained in that report. Priorities suggested in the report include:

- ISO/TC 307 should initially develop blockchain terminology standards as a means to clarify definitions in the sector and set a platform for the development of other related blockchain standards. The standards for terminology could by developed in close coordination with the ISO/IEC committee JTC 1 SC 38 Cloud Computing and distributed platforms.
- Privacy, security and identity issues are commonly sighted as concerns for most blockchain and DLT technologies. As such these issues can be addressed collectively through the development of one or a suite of standards under ISO/TC 307. These standards could be developed in association with ISO/IEC committee JTC 1 SC 27 IT Security techniques.
- Governance and risk-related issues should also be addressed by ISO/TC 307 after the foundational standards for blockchain and DLT terminology. These standards could be developed with reference to existing ISO and ISO/IEC documents including ISO 31000 Risk management principles and guidelines and ISO/IEC 38500 Governance of IT for the organisation.
- The development of standards for terminology, privacy, security, identity, risk, governance and other key issues relating to standards paves the way for the later development of a reference architecture standard for blockchain under ISO/TC 307. A reference architecture standard would provide stakeholders with a framework for developing and using blockchain and DLT. This should be considered as part of a future work program by ISO/TC 307.
- Establishing interoperability amongst blockchain systems should be an overarching objective of ISO/TC 307. Standards for interoperability are more likely to be achieved after more fundamental matters are addressed such as the development of a consistent terminology and appropriate measures for managing privacy, security and identity.

- Artificial intelligence – Machine learning and artificial general intelligence (AI for short, though this is something of a misnomer) will eventually be part of how our systems will help us manage complexity and increasingly pervasive and salient interactions. AI is already beginning to interact with data, connected systems and other 'intelligence' on the Internet. Since it cannot practically be audited, controlled or even understood in real-time, it cannot be left unsupervised; standards will have to form part of the regulatory mix. Such standards will necessarily need to deal with matters of ethics and the embedding of legal rules. Their development will inevitably interact with governmental and Intergovernmental scrutiny in relation to sensitive issues like privacy and security, not least because inevitably its development means transferring to machines decisions that are currently under human control, and for which the law holds humans accountable. This is not limited to AI in the strict sense; the field of algorithmic regulation has arisen in response to the increasing importance of formulae that learn from and respond to data flows to make critical decisions; examples range from the Gaussian Copula formula, whose ungoverned use has been cited as a primary cause of the recent economic crisis to algorithmic collusion, in which automated systems for collecting and responding to rival's pricing decisions have the effect of enabling firms to reap the rewards and inflict the damage of conspiracy without conscious intent. The growth of AI has effects beyond data analysis, as well; it both creates new challenges and offers new solutions to spectrum policy, for instance, that can help it address the needs of 5G and IoT/CPS.

These and other developments firmly indicate what we can learn from the past: the future, 10 years from now, will contain elements and characteristics that are currently beyond coherent imagination. 10 years ago, few thought data would be as abundant as they are, mobile services would pose so much challenge to fixed-line networks, and the Internet of Things and AI would be as far out of the starting blocks as they are.

Digital Communities perspectives on policy and technology areas

How do communities relate to the 4 policy domains?

Communities and their needs shape policies – whether they relate to specific *problematique* of less densely populated regions or to specific opportunities for communities collaboration, within or beyond geographic proximity limitations. Below, we present these insights and put them in context of the subject at hand.

Privacy & data protection

One of the most contested issue sets across the board concerns personal data protection and the closely-related but distinct issue of privacy. This issue set is not only a matter of deep concern to the private sector and to civil society, but is also an increasingly-fraught bone of contention in the government sphere, where national governments and supranational governance entities tussle over criminal justice, national security and other vital national (e.g. economic) interests. The increasing awareness by individuals of rights to privacy and to personal data protection put this even more directly at the heart of policy discussions and practical developments. In addition: laws and regulations on both sides of the Atlantic have to be respected and the concerns of non-government stakeholders have adequately to be addressed if ICT developments are to be <1> legally acceptable on both sides of the Atlantic and <2> trusted enough, for now and the years to come, to be adopted – and adapted – for wider use in society.

People within the EU and US – and around the world - want and deserve ICT products and services that serve their interests and can be trusted by them, and need ICT products and services to deal with 'wicked' societal challenges. Specifically in less dense regions, there is a challenge of access to broadband and services, as compared to the more densely populated regions. However, scalability of solutions increases the ability to put lower capacity (thus cheaper) equipment in less dense places, and new use of spectrum (5G networks, use of unregulated space and TVWS) make extension of services to anywhere less costly, more scalable and thus more affordable. The emphasis is on "constant communications" and sharing of data. When regions are going increasingly digital, more data become available, and it is relevant to consider that these may more easily related to private individuals – even if they are not mend to be collected as such. For instance, where location data in an area with a population density of 27,000 people per square mile (New York, 2015 data) may relate to anyone of those frequenting the area, in regions where density is much lower it may be relatable to one or a small group of individuals. In addition, data owned by certain bodies in the region may be seen by local people that know many of the other locals, which leverages the relatability to private individuals which is an important concern in a society where more and more "facts" become available in digitised format.

ICT Security

Cyber-security is high on the agenda of policy makers throughout the world. The growing incidence of adverse and highly-publicised events, including massive distributed denial of service attacks on the Internet (e.g. the Dyn attack in 2016, and witnessing more recent attacks to continue to grow in capacity requiring better responses and more collaboration), malware (e.g. the WannaCry Ransomware attack in 2017 etc.), hacking (leading to data breaches and unauthorised use of services), man-in-the-middle attacks (MITM), and unauthorised penetration of critical services and sensitive data (including the many breaches of customer data at Yahoo and other organisations over the years) has seriously disrupted networks and compromised privacy and national information security.

There is no magic cure for the serious security issues that that have become endemic throughout the underlying infrastructures and services that have become so fundamental to the way we communicate, access information, and interact. Even more so: each 'cure' sets the stage for the next set of issues. Network security is not confined

to the technical layer, but spreads to all layers and beyond to the user community. Progress made in one domain can be undermined by contagion or reinfection from others. The challenges are no different in rural areas or remote regions: they are global and need to be addressed head-on by all stakeholders; governments who have the monopoly on the coercive power of the law, end users who must act knowledgeably and responsibly, ICT developers who are responsible both for security 'by design' and for critical vulnerabilities and businesses using and/or deploying ICT and ICT-based or –enhanced services in more or less responsible ways. A proper balance between responsible action by individual entities and collaboration among stakeholders is essential for sustainable progress.

ICT Standards

The implementation of standards in industry and commerce grew in importance with the onset of the Industrial Revolution and its requirements for high-precision machine tools and interchangeable parts. Originally such standards were set at the level of specific sectors; in many ways, this focus continues. However, flows of information pervade most sectors and an increasing range of economic, scientific and societal activities; the 'generic' nature of information services means that same ICT technologies or services are used in multiple sectors and for diverse purposes. Standards setting and development within a single sector often does not keep pace with evolving business interests across sectors and standards competition.

To the extent that ICT-driven convergence is a real threat to existing standards, it is worth bearing in mind that it spans sector boundaries (e.g. aviation, logistics, health care, etc.), societal roles (commerce, science, civil society, administration) and subject domains (i.e. merging transmission protocol and encryption standard-setting). These "crossovers" argue for a networked (as opposed to a federated or hierarchical) structure of standardisation.

With regards to less densely populated and more remote regions, standards are needed that allow scalable solutions that make delivery of digital services affordable and effective. In this, it is clear that solutions need to relate to the privacy and safety sensitivity of the specific services to be delivered. For instance: disaster warning systems are less privacy sensitive (such as measuring of water levels) but should be reliable. And services such as road toll can be quite privacy sensitive, and at the same time incidental non-availability does not lead to big problems: some people may get away with free use of a road whereas otherwise they would have been tracked and charged.

Spectrum

As noted, all the PICASSO technological domains rely on connectivity. Even though the Internet has a global reach, its infrastructures do not and radio connections are no exception; even satellite backhaul depends on uncongested local bandwidth. Thus spectrum policy is always to some extent a local public good, and one that is particularly critical in sparsely-populated and-or remote areas where fixed-line connectivity with the necessary degree of quality and ubiquity may be infeasible and/or uneconomic. Both 5G and spectrum use such as TVWS facilitate better communications for specific purposes, and extend the ability for delivery of many digital enabled services to remote and less densely populated regions.

How do Communities relate to the Picasso technical domains?

Within PICASSO, the focus is on 5G networks; Big Data; and the Internet of Things, specifically Cyber Physical Systems. From the background reflected above, we focus on these three domains, below.

5G networks

5G networks will facilitate communications among people, but even more among devices (IoT). M2M traffic will likely manifest in two broad groups – massive applications and critical applications:

1. Massive applications involve minimal data traffic among many devices. Normally, these applications use low-bandwidth connection technologies such as GSM, but some mobile operators are already rolling out low-power WAN (LP-WAN) networks to facilitate this group.[141]
2. Critical applications require ultra-high reliability and availability with very low latency. Examples include health and medical monitoring devices, telepresence (e.g. remote surgery and remotely-controlled vehicles), industrial infrastructure command-and-control and autonomous cars. These applications need specialised, higher-bandwidth connection technologies such as LTE and Wi-Fi in order to function.

These same applications will drive the adoption of the 5G network, which will support and extend the transport layer, enabling new IoT technologies. The uptake of 4G and its increased data and services was incredibly fast, but there is a gap widening between 4G-based services and the needs of services that could benefit from 5G.

This development will significantly affect mobile networks in different ways. For less densely populated areas, investment to implement infrastructures is much less available, so real business cases will need to be made both to ensure their development and to forestall widening 'digital divides.' Massive applications will not need much bandwidth or frequent communication, so data transport revenues will not replace the mobile revenues of old, even if there is a massive rise in connected and communicating objects. Moreover, operators will need to work closely with local stakeholders to ensure that necessary levels and types of communication services are identified and made available.

The necessary technologies already exist, and will become even more scalable with the roll-out of 5G networks. Yet, as with broadband, access can remain scarce unless positive action for implementation leads to 5G coverage, including in those areas that are less frequented by 5G providers' current customers – less populated and remote areas. Ensuring that digital divides are reduced or bridged and that broadband networks and services attain the greatest national coverage and use are priorities for both EU and US governments. Policies to promote competition and private investment, as well as independent and evidence-based regulation, have been tremendously effective in extending coverage, according to the OECD[142]. In doing so, they have developed and exploited synergies between market forces, public expenditure and regulation, thus extending the reach of these instruments. However, it should be stressed that coverage or access are not the same as subscription or use; these developments are removing or reducing technical barriers to the development of digital communities that connect and empower remote populations, but in some cases more is required to ensure effective and efficient uptake of these capabilities. This can be seen in the fact, noted by the OECD report, that most of these developments have been associated with universal service obligations and coverage targets; usage or uptake targets are far less prevalent[143].

Big Data

Beyond the acknowledged and well-understood contributions of data analytics to facilitating the ordinary and innovative aspects of joint living (at scales ranging from Smart Homes through digital villages to Smart Cities), Many digital community services are enabled and enhanced by Big Data tools and techniques, from the automation of routine services (especially locally-critical service infrastructures) to the empowerment of local government on one side and local democracy on the other[144]. One critical aspect of this type of Big Data-led digitisation is the feedback between data use and data availability – this can be positive (visible benefits and trusted data analytics services leading to greater willingness to measure and share data) or negative (greater reliance on data-based decision-making leading to a perception that individuals don't matter or only matter in relation to their observable artefacts, leading to a decreased availability, reliability and quality of data and even greater dissatisfaction or distrust). This is closely-related to the ethics of Big Data in studying [145] and implementing[146] digital communities. Aspects of this ethical challenge that are being studied include algorithmic regulation, explicability of machine learning and the selection and incentive effects of data access and governance rules, which are gaining policy prominence with the entry into force of the EU's General Data Privacy Regulation and the US CLOUD Act.

Beyond this, Big Data and its affiliated technologies (e.g. analytics, machine learning, and algorithmic decision-making) are increasingly recognised as facilitating communitarian awareness and action in response to crises[147]. This not only extends the reach of digital communities, but also democratises the response far beyond the traditional 'humanitarian response elite' nations, institutions and people. This, in turn, can reduce the asymmetry and potential for corruption of e.g. disaster relief by increasing the density and responsiveness of human connections via the greater visibility, transparency and accountability of activities[148].

Internet of Things/Cyber-Physical Systems

IoT is a massive enabler of services in any community – whether smart city or digital community. In order to serve IoT environments, connectivity is key. With the emergence of 5G, much becomes possible in areas where 5G services are available and reliable. Where 5G coverage is not serving the needs of the community, alternative options to establish network links between objects and people are available, ranging from low latency networks using TVWS to satellite connections etc.

Scalability is particularly relevant when it comes to IoT; it is still an emerging technology in the sense of its continued development and finding its place within various industries. It also remains unknown how its traffic patterns might manifest themselves in future iterations of IoT applications and how that might impact mobile operators. Put simply, there's a lot we don't know about IoT. So investing in one particular aspect of the technology now is a huge risk, while an investment in a cloud platform that is ready to take on whatever ensues is significantly less risky. With local governments creating a space where innovation has low thresholds, yet takes into account a number of key success factors (including how it deals with data that can be connected to persons) can really boost uptake by business to experiment with new offerings to citizens and businesses.

Specifically in rural regions, IoT may focus on issues such as precision agriculture (water regime, nutrients, weather and possibly pests), water systems monitoring and management, and weather data collection, but also garbage collection and possible monitoring and improvements of electricity systems (street lights, etc.). And whereas a very high bandwidth application such as remote surgery may be not possible anywhere, health care can benefit from IoT supported solutions such as mobile devices combined with physiological sensors to gather casualty data and aid rural first responders in managing a patient before paramedic (ambulance) services arrive on scene. Or support in aftercare for operations: patients monitor their own wounds using an app which reminds them how and when to do it, and how to react if a concern arises. This includes telephone advice from a nurse specialist; the transmission of high quality photographs for assessment by a consultant; or a three-way web enabled consultation between a remote specialist and a co-located GP and patient.

In order to fully benefit from IoT, security of IoT is crucial. This is also recognised by the US Senate, following a specific hearing on this in 2017 on the importance and even possible implementation of IoT technology in rural areas of the United States, while recognising that connectivity is still an important issue they have to solve. At that point, there were no accurate data available on which areas have or lack reliable broadband internet. And all participants acknowledged the importance of cyber-security in an IoT infrastructure and echoed concerns on the risks of DDoS attacks by corrupt IoT devices turned into botnets.

[1] Not to be confused with deregulation, given the profound nature of the spillovers from these technologies.
[2] Including legacy knowledge and data.

[3] The policy implications will be discussed during the 2nd Annual Transatlantic Symposium on ICT and Policy (18th-19th June 2018), in Washington DC, co-organised by the PICASSO Project and the Woodrow Wilson Centre.

[4] E.g. the Mutual Legal Assistance Treaty (MLAT) and national or Community data privacy rules in the countries where data is stored.
[5] This comprises: i) a draft Regulation allowing judicial authorities to directly request that service providers (or their legal representatives) in another Member State to disclose ("production order") or retain ("preservation order") data about their users; and ii) a draft Directive that would require Member States to enact legislation compelling foreign service providers offering services in the European Union to designate EU-based legal representatives to respond to cross-border production or preservation orders. See: http://europa.eu/rapid/press-release_IP-18-3343_en.htm.
[6] Independent of founding documents such as the TFEU, as explicitly reflected in the recent European Court of Justice ruling invalidating the Safe Harbour Agreement on the grounds of incompatibility with "fundamental rights and freedoms, notably the right to privacy" (cf. http://static.ow.ly/docs/schrems_3OHQ.pdf.
[7] The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108).
[8] See Articles 17 and 19 of the General Data Protection Regulation – note that Article 17(2) requires data controllers to notify third-party processors that an erasure request has been made, and makes them liable. See text at: http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0212&language=EN.
[9] E.g. the Privacy Rule in the Health Insurance Portability and Accountability Act, the Fair and Accurate Credit Transactions Act, the Gramm-Leach Bliley and Sarbanes-Oxley Acts and the Payment Card Industry Data Security Standards (PCI DSS).
[10] Peter Hustinx according to Mark Say in the article "Big data needs big guidance" in FT, December 29, 2014. Retrieved http://www.ft.com/cms/s/0/fab4bae8-7f88-11e4-86ee-00144feabdc0.html#axzz3O8I1GAvc on 2015.01.07
[11] See also: Europe's policy options for a dynamic and trustworthy development of the Internet of Things, RAND, June 2013
[12] See e.g. the opinion by current EDPS Giovanni Butarelli (2015) "Opinion 4/2015, Towards a new digital ethics: Data, dignity and technology" EDPS, 11 September 2015 or Cave, J. (2016) "The ethics of data and of data science: an economist's perspective" *Phil. Trans. R. Soc. A*, *374*(2083), 20160117.
[13] We focus on security of ICT – not on the potential contribution of ICT to physical security.
[14] application, operating system, platform and network protocol
[15] It was build up in a trust environment; the pioneers recognise its inherent flaws and devote considerable effort to making the Internet (and email) more robust by use of open standards such as DNSSEC, TLS (https) and (for email) DMARC, DKIM, SPF. If today's operators would use *state-of-the-art* technical standards (open internet standards) instead of *state-of-practice*, the Internet already be more robust.
[16] Especially distributed cloud services available over the Internet and ubiquitous wireless and mobile access.
[17] Especially when systems do not require individual password protection and/or do not allow upgrades of existing systems.
[18] These have shown up in attacks on the Domain Name System (DNS), denial of service (DDOS) attacks and a continuing stream of flaws in Internet security mechanisms.
[19] As opposed to standalone applications or web sites.
[20] SDN: decoupling the network control and data planes.
[21] See http://ieeexplore.ieee.org/document/7226783/?reload=true and https://arxiv.org/pdf/1603.03409.pdf
[22] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN.
[23] Securing the Internet of Things - Explore security and privacy in an interconnected world; Hewlett-Packard Viewpoint, December 2015
[24] Much of this has been going on since the 1970's. Such efforts like Multics, capability organized computer systems, and the fruits of industrial activities by e.g. IBM and Intel can be used to create such systems.
[25] including support for R&I, infrastructure investment & deployment and regulation
[26] Meaning no party's interest or shared objective could be made better off without making another worse off.
[27] Ranging from technical measures to contract changes (with users, suppliers, etc.).
[28] On national/ international and governmental/intergovernmental levels, creating 'reasons to collaborate' – this includes e.g. security of critical systems including ICT-enhanced transport, energy and even political mechanisms.
[29] These are discussed in greater detail in the Security Policy Brief.
[30] As shown by the widespread resistance to proposals for universal biometric identification (UBID), though solutions continue to be proposed, especially as fingerprint sensors become more widespread as means of securing devices and the information to which they give access.
[31] e.g. via an audit trail showing data provenance and history (access, modifications, processing, uses and cross-linking).
[32] Secure from data protection enforcement and data subject scrutiny, if not from re-use and abuse.
[33] Note that data responsibility allows data controllers to shift undefined amounts of accountability.
[34] Due to the temporal, resource and cognitive limits of human beings and unequal access to ICT resources.

[35] It may be objected that machines cannot have privacy rights – if so, information flows will be routed to unprotected channels and exploited there, depriving humans of both powers f scrutiny and claims on the benefits of using 'their' data.
[36] EU: GDPR, NISD, ePrivacy Directive, etc.; US: CLOUD, FISA, etc.; Joint: Privacy Shield.
[37] I.e. innovation efforts that focus on products and services that may lead to large profitable businesses in the near term.
[38] See also Science:Business (2018) "Tale of two cities: Brussels and Washington struggle to cooperate in science" at: https://sciencebusiness.net/tale-two-cities-brussels-and-washington-struggle-cooperate-science.
[39] Due to the different vertical industries involved.
[40] E.g., Software Defined Networking (SDN) and Network Functions Virtualisation (NFV).
[41] Ensuring that data are secure from unauthorised access, available for authorised use and retain their integrity and quality.
[42] Ball, R. C., Diakonova, M., & MacKay, R. S. (2010) "Quantifying emergence in terms of persistent mutual information" *Advances in Complex Systems*, **13**(03), 327-338.
[43] This depends on different parties' access to information, objectives or motivations, powers of action, level of understanding and ability to engage in 'bargaining' and contracting to reallocate risk as necessary.
[44] Hardware and software that monitors and controls physical devices – see "Securing the Internet of Things - Explore security and privacy in an interconnected world" Hewlett-Packard Viewpoint, December 2015 at: https://hpe-enterpriseforward.com/securing-the-internet-of-things/.
[45] Accenture 2013 CIO Mobility Survey

[63] Source, McKinsey.

[65] Core areas of 5G, Big Data, Internet of Things/CPS and derived areas such as Machine to Machine (M2M) communications, Broadcasting, Cloud Computing, Internet access and Smart Cities.
[66] This is discussed separately in Annex B.
[67] E.g. harmonised spectral bands and usage conditions to foster the creation of global markets for hardware and to make interoperability smoother and more efficient.
[68] Spectrum cost and availability determine the socio-economic role and profitability of technological and service approaches.
[69] By legal, contractual or technological means.
[70] 'Resources' range from spectral space (defined by location, time, frequencies and power limits) to access to necessary hardware (e.g. masts).
[71] E.g. Spectrum Utilisation Licences
[72] Ranging over the necessity for real-time/linear access vs. bursty transmission to connection frequencies ranging from continuous to occasional and from static to scheduled to on-demand.
[73] Strictly, the amount of guard band spectrum technically required varies with the adjacent technologies (some pairs have particularly severe interference problems) and can be mitigated to some extent by sharp filtering and careful network planning. But as a matter of policy, a 5MHz guard band was recommended by CENELEC and baked into e.g. the UK's 2.6 GHz auction design. Note also that, according to GSMA "Studies performed and discussed in technical international fora show that a minimum guard band of 5 MHz is necessary to address potential interference between TDD and FDD systems operating in adjacent bands in the same geographical area." (GSMA "The 2.6GHz Spectrum Band: An Opportunity for Global Mobile Broadband" at: https://www.gsma.com/spectrum/wp-content/uploads/2012/07/Spectrum-The-2-6GHz-band-Opportunity-for-global-mobile-broadband-English.pdf).
[74] See e.g. Marsden, R., Sexton, E., & Siong, A. (2010). Fixed or flexible? A survey of 2.6 GHz spectrum awards. DotEcon Discussion Paper or Ofcom (2008) "Award of available spectrum: 2500-2690 MHz, 2010-2025 MHz" at: https://www.ofcom.org.uk/__data/assets/pdf_file/0013/43006/statement.pdf.
[75] E.g. providing the equivalent of mobile telephony facilities as well as Wi-Fi.
[76] Including an ultra-high-speed 5G delivered with low cost devices.
[77] I.e. that will work seamlessly across frequency ranges, use cases and actors.

[78] More specifically, for the World Radiocommunication Conference 2019 (WRC-19), the CEPT has prioritised the following bands for potential 5G use: i) 24.25-27.5 GHz (adjacent to the US 28 GHz band); ii) 40.5-43.5 GHz (adjacent to the US 29 GHz band); and iii) 66-71 GHz (considered in the frame of 57-71 GHz for licence-exempt use). For more details of the current situation, see e.g. Tomimura, D. (2018) "New spectrum: bands under study for WRC-19" ITU presentation at: https://www.itu.int/en/ITU-R/seminars/rrs/RRS-17-Americas/Documents/Forum/9_ITU%20Diana%20Tomimura.pdf.
[79] This is "Citizens Broadband Radio Service", which is an FCC-authorised wireless shared access arrangement for 3.5 GHz spectrum previously reserved for US military uses. It uses the same radio interface as licensed LTE and unlicensed 5 GHz spectrum, but with assignment requires users to request and be assigned bands by an automated Spectrum Allocation Server (SAS), which checks RF density and channel availability using terrain and radio propagation data. The assignment is automatically freed when no longer needed.
[80] E.g. via geolocation databases.
[81] This only obliges users to register on a database and meet specified operational conditions.
[82] At the moment, use drops off steeply with frequency.
[83] This denotes Fixed Wireless Access, which entails providing Internet access to homes using mobile network technology rather than fixed lines; it works best where existing fixed-line coverage is poor or inadequate.
[84] The mobile services may also need agile/cognitive capabilities.
[85] E.g. manufacturing (Industry 4.0/Factories of The Future), automotive, health, energy, media & entertainment. See https://5g-ppp.eu/wp-content/uploads/2016/02/BROCHURE_5PPP_BAT2_PL.pdf.
[86] E.g. smart towns, cars, trains, airports, universities, industrial plants, or parks.
[87] In the 2.6 GHz allocations, such 'legacy spectrum' delayed the auctions by up to 4 years (due to lawsuits by bidders without pre-existing licences on the boundary of the allocated blocks).
[88] E.g. on machine learning and predictive analytics to reduce the volume and increase the utility of collected and processed data.
[89] The reason for experimentation is that a 'predict and provide' approach is neither technologically feasible nor sensible in view of the adaptiveness of Big data/Machine Learning approaches, which balance new data acquisition against the reuse of models estimated from existing or prior data.
[90] These terms mean: volume - data volumes approaching multiple petabytes; velocity - data generated and ingested for analysis in real-time; variety - tabular, documents, e-mail, metering, network, video, image, audio, etc.; and complexity - different standards, domain rules, and storage formats for each data type, increasingly including unstructured data flows whose characteristics are endogenous.
[91] See Thelen-Bartholomew, R. (2017) "Bringing the worlds of Spectrum Management, Policy, and Monitoring together through Big Data analysis" at the ITU-D Spectrum management Conference: https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Events/2017/Spectrum%20Management/Robert_LS%20telcom%20Thelen_Bartholomew.pdf
.
[92] See SAS TDWI Best Practices Report "Operationalizing and Embedding Analytics for Action" available from https://www.sas.com.
[93] Estimates range from 8.4 billion (see: https://www.gartner.com/newsroom/id/3598917) to much larger numbers quoted by Ericsson (initially set at 50 Billion (https://www.ericsson.com/thecompany/press/releases/2010/04/1403231) but now considerably scaled back (see e.g. https://spectrum.ieee.org/tech-talk/telecom/internet/popular-internet-of-things-forecast-of-50-billion-devices-by-2020-is-outdated).
[94] E.g. sensors in streetlights or fire alarms that notify responsible organisations when they need servicing.
[95] E.g. remote temperature, traffic or pollution sensors.
[96] This access will come in particular – though not exclusively – over the Internet. Here, we must use the term Internet broadly; there is no reason to suppose that these communications will employ the Internet protocol. For instance, information-centric networking (ICN) or Constrained Application Protocol (CoAP) have been proposed as wholesale replacement for the IP protocol or as extensions to its capabilities to enable the Internet (in a classical sense) better to serve the needs of IoT/CPS. See Trossen, D., Reed, M. J., Riihijärvi, J., Georgiades, M., Fotiou, N., & Xylomenos, G. (2015) "IP over ICN-the better IP? an unusual take on information-centric networking" *arXiv preprint arXiv:1507.04221* or Fotiou, N., Xylomenos, G., Polyzos, G. C., Islam, H., Lagutin, D., Hakala, T., & Hakala, E. (2017, September). ICN enabling CoAP Extensions for IP based IoT devices. In *Proceedings of the 4th ACM Conference on Information-Centric Networking*: 218-219.
[97] The complexity dimension is important; it may not be possible to detect evolving situations and emergent challenges at a systemic level, or to respond in a timely fashion. Moreover, the decentralisation of sensing and response may help in giving critical CPS the necessary level of 'robust-yet-fragile' adaptiveness.
[98] This does not require high-bandwidth communications; indeed, highly redundant *ad hoc* networks may prove a superior substitute or valuable complement to 'conventional' (and congested) fixed and wireless connections.
[99] This might entail some combination of dynamic spectrum access, unlicensed spectrum or approval- or rule-based approaches as indicated in the previous section.

[101] They may be formed among those who use given technologies (e.g. the gamer community, those who work on specific technologies (the 5G community), and those who arise in response to problems arising on or sharpened by use of technologies e.g. the cybersecurity and privacy communities.
[102] This is further discussed in Policy Brief 4: Spectrum Policy
[103] Including a wider range of BYOD interoperability challenges than is usual in large-scale commercial applications.

[104] For example, on-demand services may be harder to execute outside of densely-populated areas; sending a driver with a car on a two-hour drive to deliver a single package in a rural community will burn through the driver's time, gas wear away at the delivery vehicle and reduce availability of the service to others. One solution involves the use of drones and autonomous vehicles. These are efficient, low-cost and timely. Implementation of next generation technologies like driverless cars, trucks and drones will help make deliveries, even in sparsely populated areas, more efficient. Recent examples show rural areas being favoured for early implementation of next generation delivery and transportation methods (e.g. Uber's successful cross-Colorado beer delivery and Amazon's drone delivery in rural U.K.). The wide-open spaces present fewer risks when trialling new delivery and transportation methods, whether it concerns drones or autonomous cars.
[105] Exposed by recent activities surrounding Facebook and the implementation of the CLOUD Act and GDPR.
[106] Implying *inter alia* principles-based rather than rule-based regulation.
[107] Both in an ethical sense and as something that people value; they are willing to pay to protect their data and can trade with others who are willing to pay to use it.
[108] *Securing the Internet of Things: Explore security and privacy in an interconnected world*, Hewlett Packard Enterprise, December 2015
[109] e.g. the idea that data generation, control and use would improve if data 'owners' are identified and empowered by giving them claims to the value of their data in use or mandating policies that allow them to withhold, modify or control their use.
[110] It is *non-rivalrous* (my use of data does not limit your ability to use it, though it may change its value) and *non-exclusive* (if we cannot deny access to data, we cannot use pricing to establish its value for policy and other decisions).
[111] E.g. innovation policy, control of harmful or illegal content or the fight against radicalisation and terror.
[112] E.g. attacker-defender polarity and prioritising security objectives and legal responsibilities ahead of other considerations.
[113] Technical capacity to preserve prior placement of responsibility can allow system architects or operators to escape responsibilities they should bear (e.g. age verification for access to online pornography).
[114] Like US Social Security Numbers – which are often found to be insecure.

[115] At EU level: the 2001 Framework Decision on combating fraud and counterfeiting of non-cash means of payment, defines fraudulent behaviours that EU States need to consider as punishable criminal offences; the 2002 ePrivacy Directive required providers of electronic communications services to ensure the security of their services and maintain the confidentiality of client information; t, addresses new developments in the online environment, such as grooming; and Directive 2013/40/EU[115] aims to tackle large-scale cyber-attacks by requiring Member States to strengthen national cyber-crime laws and introduce tougher criminal sanctions. These are all backed up by the activities of the European Cybercrime Centre (EC3). The US also has laws at both State and Federal level: see http://www.hg.org/computer-crime.html.

[116] https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/
[117] E.g. fraud, theft, tax evasion, money laundering, perverting the course of justice.
[118] This concerned a demand by the US FBI for Apple to provide access to encrypted data stored on a deceased suspect's mobile device - see e.g. https://www.wired.com/2016/03/apple-fbi-battle-crypto-wars-just-begun/.
[119] This concerned a US order instructing Microsoft to hand over a customer's email that was stored in Ireland, which was struck down in the courts - see e.g. https://www.ft.com/content/6a3d84ca-49f5-11e6-8d68-72e9211e86ab.
[120] In this case, which in effect reversed the decision in the Microsoft case, Google was ordered to hand over emails stored outside the country in order to comply with an FBI search warrant - see e.g. https://techcrunch.com/2017/02/04/google-told-to-hand-over-foreign-emails-in-fbi-search-warrant-ruling/.
[121] Failures due to incomplete information, market power, etc.
[122] Laws must be unambiguous, uniformly applied and changed only through slow, deliberate and transparently accountable processes and strong and validated evidence.
[123] The principles were taken from points raised at the ONE Conference - see https://www.ncsc.nl/conference.
[124] Attracting the wrong users or uses.
[125] Perverse incentives.
[126] To stand out, cultivate differential rather than collective reputation or to escape regulatory burdens placed on rivals.

128

[136] Including the ability to be updated or to update themselves.
[137] See e.g. https://steepsteel.com/microsoft-registers-trademark-for-airband-tvws-initiative-report/

[139] The most promising current research on privacy (or private transactions) for blockchains is currently zkSNARKs, as implemented by zCash and Ethereum. The combination of both technologies makes it possible to implement anonymous

payments, blind auctions, and voting systems. See e.g. https://blog.ethereum.org/2017/01/19/update-integrating-zcash-ethereum or http://zerocash-project.org/media/pdf/zerocash-extended-20140518.pdf.

[141] http://telecoms.com/opinion/the-mnos-path-to-5g-and-iot-is-paved-in-the-cloud/, Fintan Lawler, 19 August 2016.
[142] Bridging the Rural Digital Divide, OECD Digital Economy Papers, Feb 2018, no 265, by Lorrayne Porciuncula and Sam Paltridge at: https://www.oecd-ilibrary.org/science-and-technology/bridging-the-rural-digital-divide_852bd3b9-en.
[143] The disparities in uptake are not the same as those in access; the urban-rural uptake divide is particularly wide in e.g. Greece, Hungary and Portugal, while in Belgium, Luxembourg and the United Kingdom, higher proportions of rural households have Internet compared to urban households.
[144] See e.g. Sharma, R. S., Ng, E. W., Dharmawirya, M., & Keong Lee, C. (2008) "Beyond the digital divide: a conceptual framework for analyzing knowledge societies" *Journal of Knowledge Management*, **12**(5), 151-164 and Helbing, D., Frey, B. S., Gigerenzer, G., Hafen, E., Hagner, M., Hofstetter, Y., & Zwitter, A. (2017) "Will democracy survive big data and artificial intelligence?" *Scientific American*, **25**.
[145] See e.g. Fiesler, C., Wisniewski, P., Pater, J., & Andalibi, N. (2016, November) "Exploring Ethics and Obligations for Studying Digital Communities" in Proceedings of the 19th International Conference on Supporting Group Work (pp. 457-460). ACM.
[146] See e.g. Crawford, K., Faleiros, G., Luers, A., Meier, P., Perlich, C., & Thorp, J. (2013) "Big data, communities and ethical resilience: A framework for action" *Data Policy: Big Data, Communities and Ethical Resilience: White paper* at: https://blog.p2pfoundation.net/big-data-communities-and-ethical-resilience/2013/12/25.
[147] See e.g. Meier, P. (2015) Digital humanitarians: how big data is changing the face of humanitarian response CRC Press, Burns, R. (2015) "Rethinking big data in digital humanitarianism: Practices, epistemologies, and social relations" *GeoJournal*, **80**(4), 477-490 or (for a more critical view) Read, R., Taithe, B., & Mac Ginty, R. (2016) "Data hubris? Humanitarian information systems and the mirage of technology" *Third World Quarterly*, **37**(8), 1314-1331.
[148] E.g., where aid is needed, how it is used and what effects it has.