thinknexus

D2.3 – NGI Policies, regulations, programmes and networks in EU and US

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement nº 825189. This document reflects only the author's view and the Commission is not responsible for any use that may be made of the information it contains.

Project Title	Think tank for the collaboration on NEXt generation internet between EU- US
Project Acronym	Think NEXUS
Grant Agreement No	825189
Instrument	Coordination & Support Action
Topic	Industrial Leadership / Next Generation Internet
Start Date of Project	1st November 2018
Duration of Project	30 Months

Name of the deliverable	NGI Policies, regulations, programmes and networks in EU and US
Number of the deliverable	D2.3
Related WP number and name	WP5 - Project management
Related task number and name	Task 2.1. Landscape Analysis & Opportunities Definition
Deliverable dissemination level	Public
Deliverable due date	30/06/2019
Deliverable submission date	7/08/2019
Task leader/Main author	Fabrice Clari (inno), Hubert Santer (inno), Lisa Pourcher (inno)

Abstract

This deliverable focuses on policies, regulations, programmes and networks of importance for working groups thematic developments.

Keywords

Next Generation Internet; EU-US collaboration; Policies; US strategies; Regulations.

Revisions

Version	Submission date	Comments	Author
v0.1	01/05/2019	Table of content	Fabrice Clari (inno)
v0.2	16/06/2019	First version available	Fabrice Clari, Hubert Santer (inno)
v0.4	15/07/2019	New content added; overall structure of the document updated	Fabrice Clari, Hubert Santer, Lisa Pourcher (inno)
v0.6	22/07/2019	Sections on AI, spectrum and data flows added	Fabrice Clari, Hubert Santer, Lisa Pourcher (inno)
v1.0	07/08/2019	Final version	Fabrice Clari, Hubert Santer, Lisa Pourcher (inno)

Disclaimer

Acronyms and definitions

Acronym	Meaning
AI	Artificial Intelligence
ECPA	Electronic Communications Privacy Act
FCC	Federal Communications Commission
FFD	Free Flow of Data
FTC	Federal Trade Commission
GDPR	General Data Protection Regulation
GPS	Global Positioning System
ITU	International Telecommunication Union
NBP	National Broadband Plan
NGI	Next Generation Internet
NTIA	National Telecommunication and Information Administration
OECD	Organisation for Economic Co-operation and Development
RIFO	Restoring Internet Freedom Order

Think NEXUS project

The Internet of the future should be more open, provide better services, more intelligence, greater involvement and participation. It needs to reflect the European values". EU's Next Generation Internet initiative is a key opportunity to rethink the way the Internet works today and develop a vision involving voices from across Europe, the US, and beyond, an Internet that embodies the values Europe holds dear, such as openness, inclusivity, transparency, privacy and cooperation.

Thinking globally, the NGI will be successful only if a worldwide consensus is found, enabling the internet a Human-centric process. To that end, collaboration between the EU and the US is essential, both areas being strongly committed to develop the future of Internet, to shape a sustainable landscape for NGI developments. Indeed, the NGI initiative should design specific actions for policy collaboration, shared technology development and interaction between user-communities, with other initiatives in the world where parts of the NGI infrastructure are designed and deployed; and the US are one of the main places where such activities are held.

Think NEXUS aims to reinforce EU-US collaboration, through its dedicated Think Tank, involving major stakeholders (researchers, entrepreneurs, policy makers) from both sides of the Atlantic on NGI-related thematic in three Focus Areas: Science and Technology, Innovation and Entrepreneurship and Policy. Its mission is to become an important and lasting entity, involving stakeholders and disseminating NGI visions in a collaborative approach for tackling NGI challenges, and benefit society at large. More specifically, Think NEXUS is expected to boost the strategic research, industrial partnerships and policy compliances among the respective communities of the NGI areas and thus, result in substantial socio-economic benefits in both the EU and US regions.

Content

Table of figures

1. Executive summary

In Europe, the Future Internet is meant to be human-centric and thus be built upon European values, such as openness, inclusivity, transparency, privacy, cooperation, and protection of data. The Future Internet is not shaped in the same way on the other side of the Atlantic. Harmonising scope and sharing intrinsic values supporting the Future Internet would facilitate cooperation and allow companies to reach EU or US markets. For example, European companies willing to deploy their business in the US, deploy their product and reduce their time-to-market would strive in harmonised policy contexts. Equally, the lack of shared vision and policies would create fragmentation — which would in turn reduce the innovation potential.

The Next Generation Internet (NGI) initiative, launched by the European Commission, aims to shape the future Internet as an interoperable platform ecosystem that embodies the values that Europe holds dear: openness, inclusivity, transparency, privacy, cooperation, and protection of data. As such, NGI applications and services have to be built on top of EU regulations and policies. Moreover, in the context of Think NEXUS, which studies cooperation between EU and US stakeholders on NGI / Future Internet, it is of high importance to understand to which extent policy frameworks on both side of the Atlantic are compliant with NGI needs, in terms of policies and regulations.

In its first section, this report covers policy and regulation frameworks for both the European Union and the US. The European Union being an overarching regulatory body for all the European Member States, it has a justified and required role with regards to NGI: it ensures innovation happens without compromising core values such as privacy. Two of the most important aspects the EU stands for are data protection and privacy. Legislations on those fields have existed in EU Member States and at the European level for decades now. And last year another milestone has been reached: the General Data Protection Regulation (GDPR) entered into force.

The US approach towards Future Internet (NGI being a European acronym) is different from the EU's vision and approach on the subject. In the US, the trend is more sectoral and relies on a combination of legislation, regulation and self-regulation while the EU relates more on heavy regulations. However, numerous laws in the US cover Internet, data security and privacy with the 1974 Privacy Act being the foundation for it all. This regulation aimed at establishing control over the collection, maintenance, use and dissemination of personal information by agencies in the executive branch of the US government. Since the invention of the Internet, the definition of privacy has changed, and new laws were passed as for example the Electronic Communications Privacy Act which was passed in 1986. More recently, in 2018, the FCC launched the Restoring Internet Freedom Order (RIFO) which is aimed at replacing heavy regulations passed in the past with strong consumer protections, increased transparency and common-sense rules and which promote investment and broadband deployment.

Despite differences, it is worth noting that policy framework on both sides of the Atlantic are compliant with Future Internet / NGI services and applications.

The following section presents main US agencies involved in Future Internet activities (research, policies, regulation…) and provided readers with a detailed overview of main US clusters and innovation hubs working in Future Internet areas. It notably presents the four Big Data Innovation Hubs, funded by the National Science Foundation and doing research on the areas in which there are issues in the hub regions. Overall, it shows a strong and efficient clusters and hubs ecosystem.

The report then focusses on four thematic which will somehow support NGI/Future Internet, and which require strong policy frameworks: spectrum, artificial intelligence, data flows and privacy.

Spectrum

Both the EU and the US have set targets for the deployment of ultra-fast broadband to their citizens which will depend on the availability of wireless solutions and consequently on the freeing up and repurposing of the adapted spectrum for the provision of wireless broadband services. And both face similar issues as for example on the way to allocate spectrum, on the assignment of spectrum to users, on the rights to give spectrum users, on the imposition of conditions on usage rights, etc. However, the US has responded faster to embrace market-driven solutions as for example secondary trading with only limited government intervention in secondary markets. On the contrary, in Europe, the shift from a command-and-control towards spectrum trading has been slower.

One of the main issues that both US and EU have to face is the increased need in ultra-fast broadband but there are differences in the way spectrum issues are handled. Indeed, in the US, spectrum management is reserved to the federal government whereas in the EU the Member States have pursued their own spectrum policies within the ITU framework. But since several years, the European Institutions have been acquiring more and more power to harmonise spectrum policies and procedures across Europe.

Artificial Intelligence

In 2019, the American AI Initiative was announced, as a concerted effort to promote and protect national AI technology and innovation. The Initiative implements a whole-of-government strategy in collaboration and engagement with the private sector, academia, the public, and like-minded international partners. It directs Federal agencies to pursue a multipronged approach to advance AI. On the European Union side, the EC's COM(2018) 237 Communication set out a European initiative on AI, which aims to boost the EU's technological and industrial capacity and AI uptake across the economy, both by the private and public sectors and to prepare for socio-economic changes brought by AI by encouraging the modernisation of education and training systems, nurturing talent, anticipating changes in the labour market, supporting labour market transitions and adaptation of social protection systems, while ensuring an appropriate ethical and legal framework, based on the Union's values and in line with the Charter of Fundamental Rights of the EU.

Those two approaches impact the way to consider AI developments on ‘case studies’, applications of innovations to the respective contexts. What appears from such considerations is that the major barrier EU R&D&I stakeholders are / will face when accessing the US AI research and innovation and markets are linked

to the requirements for running the technologies between GDPR/AI ethics compliant tools and US 'unrestricted' data-fed systems.

Are US and EU visions on how to proceed with AI developments contradictory? Probably not, but the barriers set by these economic areas through their (un)regulated approaches will hinder the potential for collaborative developments if remaining differentiated. More importantly, these will also affect the performance of each area's AI ecosystems as well, harming performances within global competition.

On the other hand, EU and US regulation bodies are cooperating within international organisations, such as the OECD or G20 cooperation on common general principles, which is conferring a great opportunity to agree on common principles.

As for many other ICT related topics, finding common 'vocabularies' for certain technologies or applications are the smallest yet most efficient steps to create fertile developments. Regardless of grand schemes or strategies, conferring R&D&I stakeholders with the opportunity to share a common taxonomy of AI technologies with their own authorities and/or partners are key - achievable – steps towards an actionable AI common path.

Data flow

Free flow of non-personal data means unrestricted movement of data across borders and IT systems in the EU. It is a key building block of the Digital Single Market and considered the most important factor for the data economy to unleash its full potential and to double its value to 4% of GDP in 2020.

To further increase the cross-border exchange of data and boost the data economy, in November 2018 the European Parliament and the Council adopted the Regulation (EU) 2018/1807 on a framework for the free flow of non-personal data in the European Union. The purpose of this new regulation is to ensure the free flow of data other than personal data within the Union by establishing rules on data localization requirements, data availability for competent authorities and data porting for business users.

This regulation covers data flow within the EU boundaries. Although it is a big step forward, this regulation doesn't cover data flow between Member States and non-EU countries. However, cross-border data flows are indispensable to Future Internet / NGI and contribute significantly to growth and job creation by permitting business operations for companies of all sizes. At the same time, they allow access to a wider variety of goods and services, eventually of better quality and more competitively priced. The benefits of enabling and facilitating cross-border data flows are therefore global.

In such context, the EU and the US worked together on a shared mechanism, the Privacy Shield Framework, to allow the flow of data between both continents. As per its definition on the Privacy Shield website, "the EU-US and Swiss-US Privacy Shield Frameworks were designed by the US Department of Commerce, and the European Commission and Swiss Administration, respectively, to provide companies on both sides of the Atlantic with a mechanism to comply with data protection requirements when transferring personal data from

the European Union and Switzerland to the United States in support of transatlantic commerce". The framework includes strong data protection obligations on companies receiving personal data from the EU, safeguards on US government access to data, effective protection and redress for individuals and an annual joint review by EU and US to monitor the correct application of the arrangement and can be seen as a required building block of NGI application and services.

Privacy

There is no single principal data protection legislation in the United States. Rather, a jumble of hundreds of laws enacted on both the federal and state levels serve to protect the personal data of US residents. In such context, rather than describing privacy context in the US, the report focuses on explaining impact of GDPR in the US – i.e. which are the consequences of this EU regulation on US stakeholders having business/activities in the EU or with EU citizens.

In order to be compliant with the GDPR rules, US companies have to update their US privacy incident-response playbook in at least ten areas which are presented in section 3.3.4.

It is also worth noting that for the companies that do business internationally, in an EU country, the European security mandate must be adhered to. Moreover, it is likely that the US creates its own set of national data privacy laws. Indeed, in 2018, leading US-based technology companies called on the federal government to pass a law similar to GDPR and in February 2019, the US Government Accountability Office made the same recommendation. Therefore, it is important to highlight and prepare US companies for the needed changes in processes to follow the new data privacy laws. This section also highlights that large firms in the US are just doing the bare minimum to be able to check the GDPR box, but it is not enough to be full GDPR compliant. The companies have to make invasive changes to their business processes and change their business culture.

As report conclusions, it is noted that the US and the EU have different visions and approaches to privacy, data protection and the technology industry. While the US favours a more sectoral approach that relies on a combination of legislation, regulation and self-regulation, the EU tends to rely more heavily on legislation. This complicates the relationship. However, the two sides share the goal of allowing data to flow between Europe and the US while ensuring a high level of protection for their respective citizens' privacy and personal data. A key task for EU officials will be to keep their US counterparts informed about the implementation of the new General Data Protection Regulation.

Technologies and new services deployments will be made possible only if they are supported by strong policies, protecting citizens but without hindering innovation. This is a challenge which is even more true in the context of NGI / Future Internet cooperation between the European Union and the United States of America, as not being synchronized on policies and regulations would create fragmented markets, thus having strong impacts on citizens, on both sides of the Atlantic.

2. Introduction

The Next Generation Internet (NGI) initiative, launched by the European Commission, aims to shape the future Internet as an interoperable platform ecosystem that embodies the values that Europe holds dear: openness, inclusivity, transparency, privacy, cooperation, and protection of data[1]. As such, NGI applications and services have to be built on top of EU regulations and policies. Moreover, in the context of Think NEXUS, which studies cooperation between EU and US stakeholders on NGI / Future Internet, it is of high importance to understand to which extent policy frameworks on both side of the Atlantic are compliant with NGI needs, in terms of policies and regulations.

2.1. Reminder on Think NEXUS strategic outlines

As already detailed in multiple NGI and Think NEXUS developments, the innovativeness of the NGI initiative lies notably in its focus on values, encompassing technological, policy and business considerations at its core.

For analysing this approach, this document builds upon the developments of D1.2 - Think Tank strategic outline, which identified several "strategic domains" within the focus areas defined for Think NEXUS endeavours.

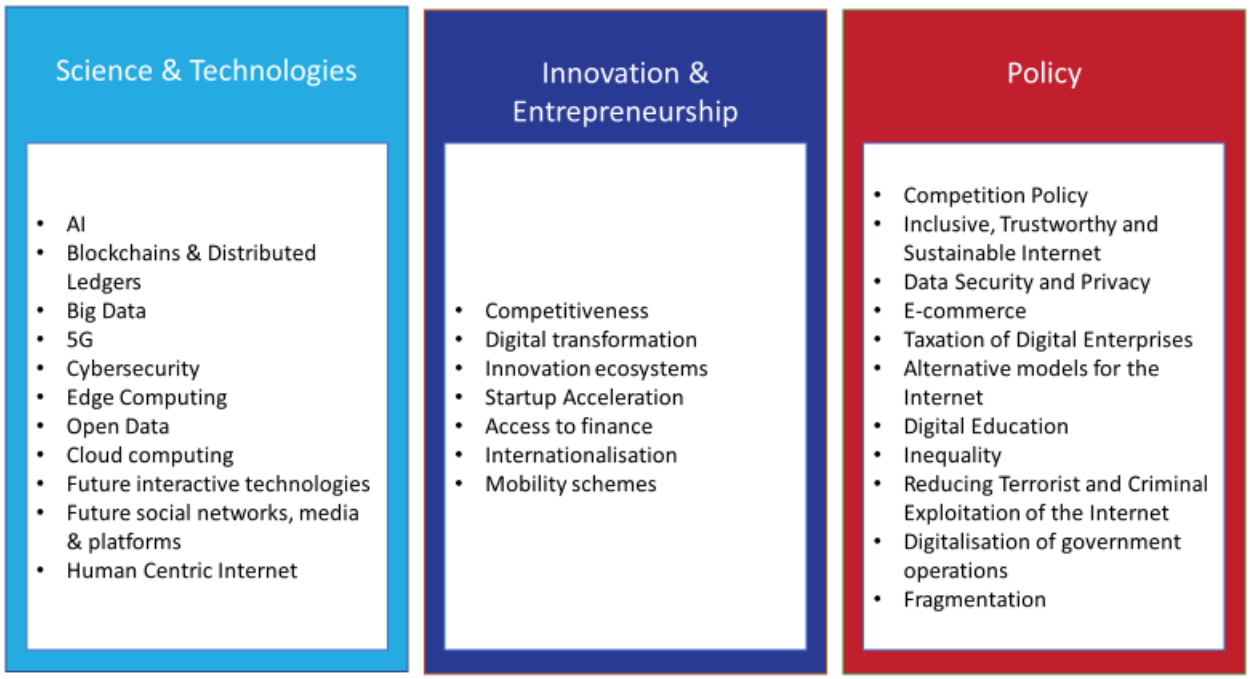

Figure 1 - Strategic thematic for Think NEXUS think tank (source: Think NEXUS deliverable D1.2)

While all these topics are of relevance for the development of the Next Generation Internet, tackling each upfront and analysing the stakeholders, initiatives, etc. linked to these would represent a long-term project in itself and lose the focus set by Think NEXUS partners and experts along its developments.

[1] https://ec.europa.eu/digital-single-market/en/next-generation-internet-initiative

Moreover, multiple sources of information on technologies and policies encompassed in NGI developments exist, notably thanks to previous collaborative projects such as PICASSO, BILAT, AEGIS etc, presented in the figure below.

PICASSO project - http://www.picasso-project.eu

This project tackled various aspects of EU-US collaboration on internet-related technologies: 5G, Big Data, IoT / CPS, as well as ICT policies

AEGIS Project - http://aegis-project.org/

This project aims at facilitating EU-US dialogue and cooperation in cybersecurity and privacy research and innovation (R&I).

BILAT 4.0 - https://www.euussciencetechnology.eu

This EU project (which ended in 2018) provided numerous reports on innovation schemes from both sides of the Atlantic.

Figure 2 - EU initiatives fostering EU-US collaboration

While building upon these initiatives, Think NEXUS does not aim at replicating existing works and thus complements areas which have not yet been covered by previous projects.

2.2. Scope and values for NGI applications

In Europe, the Future Internet is meant to be human-centric and thus be built upon European values, such as openness, inclusivity, transparency, privacy, cooperation, and protection of data. Users want to feel safe when using the Internet and they want to be sure that their personal data will not be shared and/or used against them. They need trust as well. Indeed, identity and trust are the underlying components of the basis of many human interactions and transactions; and in a future where physical and digital life will be integrated, those values must be transposed homogeneously.

Harmonising scope and sharing intrinsic values supporting the Future Internet would facilitate cooperation and allow companies to reach EU or US markets. For example, European companies willing to deploy their business in the US, deploy their product and reduce their time-to-market would strive in harmonised policy contexts. Equally, the lack of shared vision and policies would create fragmentation — which would in return reduce the innovation potential.

In such context, the following sections present policy contexts for both European Union and the United States of America in the areas of Future Internet.

3. Policies and regulations

3.1. EU framework

3.1.1. Background

The European Union being an overarching regulatory body for all the European Member States has a justified and required role with regards to NGI: it ensures innovation happens without compromising core values such as privacy.

Two of the most important aspects the EU stands for are data protection and privacy. Legislations on those fields have existed in EU Member States and at the European level for decades now. For example, in 1995, one of the funding texts of privacy-related directives on its territory, the Data Protection Directive (Directive 95/46/EC) has been adopted and ensured "the protection of individuals with regard to the processing of personal data and on the free movement of such data" at a time when the "public" internet just arrived (the World Wide Web has turned 30 in 2019). A decade later, the "Communication from the European Commission on Promoting Data Protection by Privacy Enhancing Technologies" (COM (2007)228) further developed this approach. Indeed, it recommended developers to integrate privacy and security principles during the design phase of the products. Moreover, it gave some technical measures, the Privacy Enhancing Technologies (PETs), that protect privacy without harming products' features or user experience, such as data anonymisation, end-to-end encryption, or cookie-cutter software. And last year, in 2018, it reached another milestone: the General Data Protection Regulation (GDPR) entered into force.

3.1.2. Main policies

Net neutrality

Concerning net neutrality, the Open Internet regulation was adopted in 2015. It is an EU regulation (Regulation (EU) 2015/2120) which grants, according to the EC website, "end-users the directly applicable right to access and distribute the lawful content and services of their choice via their Internet access service". It includes the principle of net neutrality: Internet traffic shall be treated without discrimination, blocking, throttling or prioritisation. It also allows the EU to manage reasonably their traffic and with the necessary safeguards, specialised services as for example services which assure a specific quality level, required for instance for connected cars or certain 5G applications.

General Data Protection Regulation

In 2016, the GDPR (Regulation (EU) 2016/6796) was adopted. This regulation on "the protection of natural persons regulated the processing of personal data and the free movement of such data" is an essential step to strengthen individuals' fundamental rights in the nowadays digital area and clarifies rules for companies and public bodies in the digital single market. It only entered into force on the 25th of May 2018 because of fragmentation between EU Member States systems and administrative burdens.

For many non-EU stakeholders, this regulation is seen as a strong barrier to innovation. Gary Shapiro, organiser of the CES technology event in Las Vegas for example said (in the context of a French event) that « ... France has a lot of entrepreneurs, but it will miss most future technological waves, because the European Union with the GDPR is extraordinarily focused on defending the privacy of individuals ».

Digital Single Market

To unify EU Member States and ensure a common vision, the European Commission adopted a policy on the Digital Single Market. It "denotes the strategy of the European Commission to ensure access to online activities for individuals and businesses under conditions of fair competition, consumer and data protection, removing geo-blocking and copyright issues".

3.2. US framework

3.2.1. Background

The US approach towards NGI is different from the EU's vision and approach on the subject. In the US, the trend is more sectoral and relies on a combination of legislation, regulation and self-regulation while the EU relates more on heavy regulations. However, numerous laws in the US cover Internet, data security and privacy with the 1974 Privacy Act being the foundation for it all. This regulation aimed at establishing control over the collection, maintenance, use and dissemination of personal information by agencies in the executive branch of the US government. Since the invention of the Internet, the definition of privacy has changed and new laws were passed as for example the Electronic Communications Privacy Act which was passed in 1986 and allows the US government to access digital communications such as email, social media messages, information on the cloud databases, etc. without a warrant or as the Cyber Intelligence Sharing and Protection Act which was passed in 2015 and concerns how to share information on potential cyber threats with the federal government. More recently, in 2018, the FCC launched the Restoring Internet Freedom Order (RIFO) which is aimed at replacing heavy regulations passed in the past with strong consumer protections, increased transparency and common-sense rules and promotes investment and broadband deployment. The RIFO "provides a framework for protecting an open internet while paving the way for better, faster and cheaper Internet access for consumers[2]".

As mentioned before, the US has more a sectorial approach regarding the regulations on NGI than the EU. Therefore, the different organisations responsible for the regulations on the different NGI subjects will be described in the next section and the main regulations on the different NGI subjects will be described in the next chapter.

[2] https://www.fcc.gov/restoring-internet-freedom

3.2.2. Main federal stakeholders on NGI related thematic

Agency / Office	Description / opportunity	Domains
Defense Advanced Research Projects Agency (DARPA)	DARPA funding for AI innovation https://www.darpa.mil/work-with-us/ai-next-campaign Past DARPA AI investments facilitated the advancement of "first wave" (rule based) and "second wave" (statistical learning based) AI technologies. DARPA-funded R&D enabled some of the first successes in AI, such as expert systems and search, and more recently has advanced machine learning algorithms and hardware. DARPA is now interested in researching and developing "third wave" AI theory and applications that address the limitations of first and second wave technologies.	AI Research Applied research
Department of Commerce Office of the Secretary (OS)	https://www.commerce.gov/bureaus-and-offices/office-secretary The Office of the Secretary is the general management arm of the department and provides the principal support to the Secretary in formulating policy and in providing advice to the President. It provides program leadership for the department's functions and exercises general supervision over the operating units. It also directly carries out program functions as may be assigned by the Secretary and provides – as determined to be more economical or efficient – administrative and other support services for designated operating units.	Policy
Department of Homeland Security (DHS)	Science and Technology https://www.dhs.gov/publications-library/science-and-technology The DHS Science and Technology Directorate (S&T) is the Department's primary research and development arm and manages science and technology research, from development through transition, for the Department's operational components and first responders.	Research Development
Federal Communications Commission (FCC)	https://www.fcc.gov/about/overview The Federal Communications Commission regulates interstate and international communications by radio, television, wire, satellite, and cable in all 50 states, the	Policy

	District of Columbia and US territories. An independent US government agency overseen by Congress, the Commission is the federal agency responsible for implementing and enforcing America's communications law and regulations.	
Federal Trade Commission (FTC)	https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions?utm_source=slider	Policy
International Trade Administration (ITA)	Privacy Shield Program https://www.privacyshield.gov/Program-Overview The Privacy Shield program, which is administered by the International Trade Administration (ITA) within the US Department of Commerce, enables US-based organizations to join one or both of the Privacy Shield Frameworks in order to benefit from the adequacy determinations. To join either Privacy Shield Framework, a US-based organization will be required to self-certify to the Department of Commerce (via this website) and publicly commit to comply with the Framework's requirements. While joining the Privacy Shield is voluntary, once an eligible organization makes the public commitment to comply with the Framework's requirements, the commitment will become enforceable under US law. All organizations interested in self-certifying to the EU-US Privacy Shield Framework or Swiss-US Privacy Shield Framework should review the requirements in their entirety.	Policy Entrepreneurship
National Aeronautics and Space Administration (NASA)	https://www.nasa.gov/ames/ocs/aria	Research
National Coordination Office for Networking and Information Technology Research and Development (NITRD/NCO)	https://www.nitrd.gov/about/index.aspx The Networking and Information Technology Research and Development (NITRD) Program is the Nation's primary source of federally funded research and development (R&D) in advanced information technologies (IT) in computing, networking, and software. NITRD is among the oldest and largest of formal Federal programs that coordinate the activities of multiple agencies to tackle	Research Innovation

	multidisciplinary, multitechnology, and multisector R&D needs. The 23 NITRD member agencies now invest approximately $5 billion annually in R&D programs that identify, develop, and transition to practical use the advanced networking and IT capabilities needed by the Federal Government and the Nation.	
National Institute of Standards and Technology (NIST)	https://www.nist.gov/about-nist/our-organization/mission-vision-values To promote US innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.	Cybersecurity
National Science Foundation (NSF)	*See relevant section*	Research Innovation (common program with SBA)
National Security Agency (NSA)	Computer & Analytic Sciences Research The Computer and Information Sciences Research Group leads and manages an advanced technology program that can research, identify, understand, develop, and apply new and emerging technologies for transforming raw data items into actionable information.	Entrepreneurship
National Telecommunications and Information Administration (NTIA)	https://www.ntia.doc.gov/category/grants Internet Policy Task Force	
Office of Science (SC)	Department of Energy https://www.energy.gov/science/initiatives The Office of the Under Secretary for Science has identified six initiatives of special priority for the DOE Office of Science. These initiatives are activities or areas of research that are inherently multidisciplinary—cutting across several scientific fields—or especially promising, or both. They include Advanced and Sustainable Energy, Artificial Intelligence and Machine Learning, Genomics, High	

	Performance Computing, Large-Scale Scientific Instrumentation, and Quantum Information Science.
Office of Science and Technology Policy (OSTP)	National Science and Technology Council https://www.whitehouse.gov/ostp/nstc/ The National Science and Technology Council (NSTC) was established by Executive Order on November 23, 1993. This Cabinet-level Council is the principal means within the Executive Branch to coordinate science and technology policy across the diverse entities that make up the Federal research and development enterprise. Chaired by the President, the membership of the NSTC is made up of the Vice President, Cabinet Secretaries and Agency Heads with significant science and technology responsibilities, and other White House officials. In practice, the White House Office of Science and Technology Policy oversees the NSTC's ongoing activities.
Office of Technology Research and Investigation (OTech)	https://www.ftc.gov/about-ftc/bureaus-offices/bureau-consumer-protection/office-technology-research-investigation The Office of Technology Research and Investigation (OTech) is located at the intersection of consumer protection and new technologies. As a trusted source for research and information on technology's impact on consumers, the Office conducts independent studies, evaluates new marketing practices, and provides guidance to consumers, businesses and policy makers. It also assists the FTC's consumer protection investigators and attorneys by providing technical expertise, investigative assistance, and training. The Office is housed in the Bureau of Consumer Protection and its work supports all facets of the FTC's consumer protection mission, including issues related to privacy, data security, connected cars, smart homes, algorithmic transparency, emerging payment methods, fraud, big data, and the Internet of Things.
Cybersecurity and Infrastructure Security Agency (CISA)	https://www.dhs.gov/cisa/about-cisa The Cybersecurity and Infrastructure Security Agency (CISA) is the Nation's risk advisor, working with partners to

defend against today's threats and collaborating to build more secure and resilient infrastructure for the future.

3.2.3. Clusters & innovation hubs

3.2.3.1 Clusters & innovation hubs

I. Big Data Innovation Hubs

The NSF established four Big Data Innovation Hubs: the Northeast, the West, the Midwest and the South Big Data Innovation Hub. These Hubs are established regionally in order to focus on what is important in the region and on the different issues in the region. The Hubs are local and regional collaboration hubs.

Figure 3 - The Big Data Innovation Hubs in the USA - Regional distribution (source: Northeast Big Data Innovation Hub)

The NSF does not decide upon the priority areas except those on education. All the different hubs do research on the areas in which there are issues in the regions and propose accordingly a program of their future activities to the NSF. The NSF can decide if it funds the activities or part of the activities. The Big Data Innovation Hubs can also be in part funded by several organizations as for example by EmPAWRed and are always looking to expand their funding resources.

Nevertheless, the four hubs have as three principal aims:

- to build and strengthen partnerships across industry, academia, non-profits and government to address societal and scientific challenges
- spur economic development
- accelerate innovation in the nation

In the following subchapters, the states covered by the different Hubs will be listed as well as the regional priorities of each Big Data Innovation Hub.

A. Northeast Big Data Innovation Hub

The Northeast Big Data Innovation Hub covers the following states in the US: Maine, New Hampshire, Vermont, New York, Massachusetts, Rhode Island, Connecticut, New Jersey and Pennsylvania. Its primarily goal is to build partnerships to address societal challenges with data-driven solutions. The Hub serves as a platform for collaboration among their network of stakeholders, harnessing the potential of big data and data science in multi-sector projects no single organisation can tackle in isolation. Its network is composed of more than 200 organisations, universities and companies.

The Northeast Big Data Innovation Hub organizes multi-sector collaborations that are aligned with one or more of their thematic areas and cross-cutting areas:

- Thematic areas: Education, Health, Rural/Urban Spectrum and Science
- Cross-cutting areas: Data Literacy, Data Sharing, Responsible Data Science, Privacy and Security.[3]

B. West Big Data Innovation Hub

The following states are covered by the West Big Data Innovation Hub: Washington, Oregon, Idaho, Montana, Wyoming, Colorado, New Mexico, Arizona, Utah, Nevada, Alaska, Hawaii and California. In this region the thematic areas and cross-cutting areas are:

- Thematic areas:
    - Metro/Urban Data Science: Smart Cities & Connected Communities, Transportation, Housing, Safety, Criminal Justice, Economic Development
    - Scientific discovery and learning: Open Science, Education, Reproducibility and Workforce
    - Precision Medicine: Diagnostics, Treatment, Genomics, Environment and Exposome
    - Natural resources and Hazards: Disaster Response, Sustainability, Agriculture, Water and Energy
    - Big Data Technology
- Cross-cutting areas:
    - Cloud computing task force and infrastructure

[3] http://nebigdatahub.org/about/

- Data hackathons/challenges and storytelling communities of practice
- Groups interested in: public policy, ethics/responsible data science, security, data sharing.[4]

C. Midwest Big Data Innovation Hub

North Dakota, South Dakoda, Nebraska, Kansas, Missouri, Iowa, Minnesota, Illinois, Wisconsin, Indiana, Michigan and Ohio are the states covered by the Midwest Big Data Innovation Hub.

The three specific themes of importance to the region are three broad themes: Society, Natural/built environments and Biomedical science. Integrative themes connect the three themes like data sciences, tools, and services needed to collect, store, link, serve and analyse complex data collections, and educational activities to advance the knowledge base and train a new workforce in the practice and use of data science and services.[5]

D. South Big Data Innovation Hub

The South Big Data Innovation Hub covers the following states of the US: Texas, Oklahoma, Louisiana, Arkansas, Mississippi, Tennessee, Kentucky, West Virginia, Maryland, Delaware, Virginia, North Carolina, South Carolina, Georgia, Alabama and Florida. The priorities in this region of the US and for the South Big Data Innovation Hub are:

- Health and disparities: high impact applications of data science in precision medicine, health analytics, and health disparities
- Smart cities and communities: collection and integration of data on infrastructure, sensors, and behavior to design efficient use of resources and services, and to achieve a higher quality, affordable lifestyle, as well as concrete applications of analytics and machine learning to improve the US's energy production and smart grid
- Advanced materials and manufacturing: access to data infrastructure for creating new materials for advanced manufacturing in every state of the US
- Environment and coastal hazards: prevention and enhanced response to natural and human-induced environmental hazards
- Social cybersecurity: best practices across sectors to ensure private, secure, and ethical data sharing, reporting, and use.[6]

[4] https://westbigdatahub.org/about/
[5] http://midwestbigdatahub.org/about/
[6] https://southbigdatahub.org/about-this-blog/

II. Plug and Play technology center

Plug and Play Technology Center is an innovation platform bringing together start-ups and large corporations. There are three pillars of the Plug and Play technology center:

- Accelerator Programs: which are industry themed to ensure start-ups and corporate partners make meaningful connections for their business
- Corporate Innovation: the technology centre empowers specific business units by pin-pointing their business challenges and matching them to the start-ups with the right solutions
- Investment: the technology centre invests in start-ups and has connections with VCs. The technology centre proposes a favourable ecosystem for start-ups in needs of fund raising.[7]

III. R!OT

RIoT represents a network of technologists, engineers, business leaders, academics, policy makers, and entrepreneurs, all of whom have a stake in the Internet of Things industry. RIoT proposes 3 types of services:

- RIoT ED: RIoT hosts multiple IoT focused education series. The goal is to help educate business leaders, developers and engineers on the IoT economy, how to adapt, and how to scale.
- RIoT Labs: The goal is to provide resources to the start-up community that are not available in typical coworking and start-up incubator spaces across the US. RIoT Labs is a hardware, wireless and software prototyping lab with all the tools for full-stack IoT prototyping. RIoT Labs also connects entrepreneurs to their industry, government and university network through regular Lunch and Learns, Educational programming and collocated office space.
- RIoT Accelerator program: RIoT proposes to start-ups to participate in a 12-week high-touch RIoT Accelerator Program. In the program is included the connection with an industry consortium of more than 75 companies across the IoT technology stack to learn, partner and more quickly bring the product to market and scale.

RIoT is financed by the Wireless Research Center of North Carolina and sponsored by many companies as IBM, Verizon, Microsoft and Lenovo.[8]

IV. Mississippi communications technology alliance

The Mississippi Communications Technology Alliance is an association which aims at promoting and advocating the telecommunications industry throughout the region. This association facilitates the exchange of information, experience and concepts to the mutual benefit of the individual members and their companies.[9]

[7] https://www.plugandplaytechcenter.com/about/
[8] https://ncriot.org/
[9] http://www.mctaonline.org/index.html

V. Advanced Cyber Security Center

The Advanced Cyber Security Center is a member-driven non-profit organization harnessing the power of collective resources for their three main areas of action:

- Enhanced cyber defence: by collaborating on effective security practices, improving decision-making, and promoting resources that reduce duplication of efforts across member organizations
- Workforce development: by making security careers more attractive by improving talent/industry interactions and developing opportunities to strengthen local security community relationships and attract talents in the region
- Community engagement and advocacy: by providing a channel for organizations to engage in cybersecurity policy debates [10]

VI. Center for Commercialization of Advanced Technology of San Diego

The Center for Commercialization of Advanced Technology is an entrepreneurial partnership for technology commercialization that was designed to accelerate the development and application of advanced technologies to solve real-world problems.[11]

VII. Washington Technology Industry Association

The Washington Technology Industry Association aims at consolidating the power of member companies to solve business problems they cannot solve on their own. The Association has three areas of priorities:

- Recruit talent: help SMEs attract and retain technical talent through programs and public policy that makes the region attractive
- Fund education: promote the increase of private and public investments into Computer Science education at all levels
- Train Talents: foster the development of technical and entrepreneurial talent through programs or partnerships with the aim to create a long-term, sustainable technology industry.[12]

3.2.3.2 Clusters supported by the private sector

Innovation and Technology Hubs by Infosys

Infosys is a global leader in technology services and consulting helping clients to create and execute digital transformation strategies. The company's aim is to push innovation and new technologies in the US, and it established 6 Innovation and Technology Hubs in the following states: Arizona, Connecticut, Indiana, North Carolina, Rhode Island and Texas.

[10] https://www.acscenter.org/about-us/index.html
[11] http://lavincenter.sdsu.edu/programs/CCAT
[12] https://www.washingtontechnology.org/about/

The Hubs focus on developing technology skills in such areas as machine learning, artificial intelligence, user experience and advanced digital technologies, including big data and cloud. They aim at developing cutting edge technologies to support American businesses in an increasingly digital future.

Enel Innovation Hub Network

Enel in its open innovation approach has established Innovation Hubs across the world and notably in Silicon Valley and in Boston. Enel Innovation Hub is a physical space where the start-ups can meet and present their projects to Enel. Enel offers the selected start-ups all the necessary tools for take-off like technology consultancy from experts, access to the company's network of partners including investors and the possibility to test innovations in the company's laboratories or plants. Enel can also suggest buying the start-ups or collaborate with them.[13]

Innovation Hub by Merk KGaA

Merck KGaA has established an Innovation Hub based in the Silicon Valley. The hub supports the company's existing businesses and to look between and beyond their existing scopes. The hub has a direct connection to the company's resources, market access, and extensive expertise and is responsible for exploring new technological opportunities by building and maintaining local relationships and partnerships.[14]

Chicago Connectory

The Chicago Connectory was built by Bosch and 1871 on the idea of building and creating a space for the IoT community to meet and collaborate and provide them with the resources needed for their success. The Chicago Connectory is a co-creation space and IoT incubator boasting cutting-edge technology and networking opportunities with IoT experts. Its activities are focused on three main areas:

- Educate about IoT: Building and providing a publicly accessible, immersive IoT experience to educate about IoT and inspire future solutions
- Support start-ups: Growing an ecosystem and resources for start-ups and growth-based companies to support them realize their ideas
- Connecting partners: connecting corporate partners with a network of IoT innovators.[15]

[13] https://www.enel.com/stories/a/2018/12/innovation-hub-enel-network-innovation-startup
[14] https://www.emdgroup.com/en/research/silicon-valley-innovation-hub.html
[15] https://chicagoconnectory.com/our-story

3.2.3.3 Clusters from the CNS (Computer and Network Systems) Division (NSF)[16]

Computer Systems Cluster

The computer System Cluster supports research and education activities that address the requirements in a variety of systems, including distributed, mobile and embedded systems, sensing and control systems, dynamically configured, multiples-component systems, parallel systems and trusted systems.

Currently, the interest areas of the cluster are:

- The organisation of systems (e.g. peer to peer)
- Software architectures that scale to handle thousands of components or a spectrum of heterogeneous components
- How to handle complex combinations of requirements (e.g. meeting real-time constraints and coordinating control in an embedded, failure-prone environment)
- Systems to detect problems and to take corrective action without any human intervention
- Tools to analyse and predict the behaviour of complete computing systems
- Developing and controlling the execution of complex, dynamically changing applications through compiler and runtime techniques
- Low-cost, scalable and reliable storage systems
- Operating systems and libraries for new technologies

Computing Research Infrastructure Cluster

Building prototypes and test beds are important components of experimental computing and require having an experimental infrastructure. The cluster supports the acquisition, enhancement and operation of experimental facilities for all CISE research and education areas. The supported facilities range from instrumentation needed by few projects to major experimental facilities for an entire department. The cluster provides also support to enhance the computational and human infrastructure in minority-serving institutions and to the equipment needs of collaborative, distributed research projects. Moreover, support a wider range of infrastructure needs, research projects and institutions is one of the main aims of the cluster for the coming years.

Education and workforce Cluster

This cluster supports projects that integrate research and education across CISE, study the causes of the current lack of diversity in the information technology workforce, and lead to a broadening of participation by all under-represented groups. The issue the cluster aims to tackle is the following: rapid advances in computing technology lead to the need to transfer research results into the classroom. Indeed, developing and making effective use of new research results requires a well-educated and diverse workforce that is representative of and able to interact with the entire population.

[16] https://www.nsf.gov/cise/cns/about.jsp

Network Systems Cluster

Future networks will:

- Exhibit unpredictable and complex behaviour and dynamics
- Span a broad range of technologies and bandwidths
- Carry increasingly large amounts of demanding traffic.

This cluster supports a range of research and education activities in networking technology and systems. The main aims are to support the science and technology needed to create next-generation networks and to address the limitations of existing networks.

The current projects of interest that are supported are in the following fields:

- Next-generation networks
- Fundamental understanding of large and complex heterogeneous networks
- Evolution of the network by overcoming existing limitations and by adding new capabilities and services

The current targeted focus areas of the cluster are:

- Programmable wireless networks: to exploit the capabilities of programmable radios to make effective use of the frequency spectrum and to improve wireless network connectivity
- Networks of sensor systems: to create architectures, tools, algorithms and systems that will make it easy to assemble and configure a network of sensor systems

3.2.3.4 Other Clusters[17]

The Joint Artificial Intelligence Center

The Joint Artificial Intelligence Center (JAIC) is the Department of Defense's (DoD) Artificial Intelligence (AI) Center of Excellence. It provides expertise to the Department in order to it to exploit all the power of AI in terms of technology development, of requisite policies, knowledge, processes and relationships.

The JAIC's mission is to transform the DoD by accelerating the delivery and adoption of AI in order to use AI to solve large and complex problems. The JAIC's activities include:

- Accelerating the delivery and adoption of AI
- Scaling the impact of AI across the Department
- Defend US critical infrastructure from cyber attacks
- Establishing a common foundation that enables decentralized execution and experimentation
- Evolving partnerships with industry, academia, allies and partners
- Cultivating a leading AI workforce

[17] http://www.clustermapping.us/organization-type/cluster-organizations-and-initiatives?page=1

- Leading in military AI ethics and safety

3.3. Common EU/US concerns for NGI applications and services

3.3.1. Spectrum

In the International Telecommunication Union (ITU), the first sentence stipulates that they recognize "the sovereign right of each State to regulate its telecommunication and having regard to the growing importance of telecommunication for the preservation of peace and the economic and social development of all States"[18]. Indeed, regulation at national, regional and global levels are required to obtain an effective spectrum management. Today, issues around spectrum management and policies have become crucial due to the growing use of spectrum for telecommunications[19].

Both the EU and the US have set targets for the deployment of ultra-fast broadband to their citizens which will depend on the availability of wireless solutions and consequently on the freeing up and repurposing of the adapted spectrum for the provision of wireless broadband services. And both face similar issues as for example on the way to allocate spectrum, on the assignment of spectrum to users, on the rights to give spectrum users, on the imposition of conditions on usage rights, etc. However, the US has responded faster to embrace market-driven solutions as for example secondary trading with only limited government intervention in secondary markets. On the contrary, in Europe, the shift from a command-and-control (meaning "the direct regulation of an industry or activity by legislation that states what is permitted and what is illegal"[20]) towards spectrum trading has been slower.[21]

Europe is seen as having strict consolidation rules, privileging analysis on market shares and number of competitors. But since 2012, European regulators and politicians have increasingly recognised the competitive advantage and productivity enhancement that deployment of the latest telecom infrastructure can provide. Therefore, they have started to shape policies in order to attract and support the necessary investments.[22]

In the European Union, "the Member States coordinate their spectrum management approaches in a common regulatory framework to support the internal market for wireless services and to foster innovation in electronic communications and other sectors"[23]. Therefore, the EU's Radio Spectrum Policy's main objective is to support the internal market for wireless services and equipment and to foster innovation in electronic communications and other sectors. Nevertheless, the allocation and management of spectrum in the EU is under the responsibility of the national administrations. The European Commission only ensures that the use and management of radio spectrum in the different EU countries take into account all relevant EU policies. A

[18] http://www.soumu.go.jp/main_content/000171442.pdf
[19] https://ieeexplore.ieee.org/document/7763240#full-text-section
[20] McManus, P. (2009) Environmental Regulation. Australia: Elsevier Ltd.
[21] https://www.squirepattonboggs.com/~/media/files/insights/publications/2011/10/spectrum-trading-in-the-eu-and-the-us--shifting-__/files/tel12_squire-sanders_ver4/fileattachment/tel12_squire-sanders_ver4.pdf
[22] https://www.telefonica.com/es/web/public-policy/blog/articulo/-/blogs/europe-vs-usa-telecom-regulatory-models-and-policy-objectives-new-rules-for-new-times-1-regulatory-models-
[23] https://ec.europa.eu/digital-single-market/en/content/eus-spectrum-policy-framework

framework for Radio Spectrum Policy was launched in the EU by the 2002 regulatory framework for electronic communications, and particularly by the Radio Spectrum Decision which defines the policy and regulatory tools to ensure the coordination of policy approaches and harmonised conditions for the availability and efficient use of radio spectrum for the internal market.[24]

As the mobile digital economy is expected to have an important impact on growth, productivity and progress throughout the 21st century, it has been of interest for Europe to create a single wireless market through the Digital Single Market proposal. It proposes to centralise its spectrum management functions, to harmonize regulations and to allow for industry consolidation to fit the scale of a single market.

Moreover, regarding spectrum trading, spectrum auctions and procedure to facilitate spectrum trading have not been prevalent in most EU Member States. But in 2007, the European Commission observed that spectrum is rigidly allocated to specific technologies or for specific usage. Therefore, they revised the Framework Directive through the Radio Spectrum Policy Programme (RSPP) adoption, including various measures designed to make the spectrum assignment process more efficient by encouraging liberalisation and trading of spectrum. Moreover, according to the RSPP, EU Member states, in cooperation with the European Commission, will be required to take "all steps necessary to ensure that sufficient harmonised spectrum for coverage and capacity purposes" is allocated within the EU[25]. This was adopted on the basis that spectrum trading "can be an effective means of increasing efficient use of spectrum, as long as there are sufficient safeguards in place to protect the public interest, in particular the need to ensure transparency and regulatory supervision of such transfers".[26] The RSPP also specifies a number of measures that Member States may take in order to promote effective competition in mobile markets and "prevent any potential anti-competitive outcomes"[27] which include[28]:

- The power to limit the amount of spectrum granted for rights of use to any operator or attach conditions to those rights including the provision of wholesale access, national or regional roaming;
- The capacity to reserve certain parts of a spectrum band or groups of bands for new market entrants
- The right to allow new usages or to refuse new rights of use in certain bands,
- The ability to amend existing rights in accordance with the Article 14 of the Authorisation Directive;
- The prohibition or imposition of conditions on the transfer of spectrum rights of use which are not subject to national or EU merger control.

[24] https://ec.europa.eu/digital-single-market/en/content/eus-spectrum-policy-framework
[25] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32012D0243&from=EN
[26] Revised Framework Directive, Recital (19)
[27] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32012D0243&from=EN
[28] https://www.squirepattonboggs.com/~/media/files/insights/publications/2011/10/spectrum-trading-in-the-eu-and-the-us--shifting-__/files/tel12_squire-sanders_ver4/fileattachment/tel12_squire-sanders_ver4.pdf

In the US, the spectrum is managed by the National Telecommunication and Information Administration (NTIA) for governmental applications and by the Federal Communications Commission (FCC) for non-governmental applications.

It is the role of the National Telecommunications and Information Administration (NTIA) to manage the Federal government's use of spectrum and ensuring US's domestic and international spectrum needs are met while efficiently use this limited resource. Specifically, the NTIA's missions are[29]:

- Establishing and issuing policy regarding allocations and regulations of spectrum
- Developing plans for the use of spectrum
- Assigning frequencies
- Maintaining spectrum use database
- Certifying spectrum is available for the federal agencies' telecommunications systems
- Providing the technical engineering expertise needed to perform specific spectrum resources assessments and automated computer capabilities needed to carry out these investigations
- Participating at the Federal communication emergency readiness activities
- Participating at the Federal telecommunication and automated information systems security activities

It is the FCC who decides upon the use cases for the specific spectrum portions and who will have access to those. It is also this Commission who regulates the physical layer technologies to be employed.

The National Broadband Plan (NBP) was designed and published by the FCC in which it is noted that "Spectrum policy is the most important lever government has to help ensure wireless and mobile broadband thrive"[30]. Therefore, and due to the increasing need of broadband, the NBP also recommenced reallocating spectrum for mobile broadband. Moreover, it recommends that the FCC "ensure greater transparency in spectrum allocation and utilisation, reserve spectrum for unlicensed use, and make more spectrum available for opportunistic and secondary uses"[31]. Thanks to this NBP and the increase demand in broadband, the US Congress has been taking actions to free up additional radio spectrum for mobile broadband and public safety services. The NBP proposed to reallocate 120 MHz of spectrum from broadcast television services for wireless broadband use. The Plan proposes to organise incentive auctions designed to encourage TV broadcasters in major markets to voluntarily give up spectrum rights in exchange for a portion of the proceeds from the auction.[32]

One of the main issues that both US and EU have to face is the increased need in ultra-fast broadband but there are differences in the ways spectrum issues are handled. Indeed, in the US, spectrum management is reserved to the federal government whereas in the EU the Member States have pursued their own spectrum

[29] https://www.ntia.doc.gov/category/spectrum-management
[30] https://transition.fcc.gov/national-broadband-plan/national-broadband-plan.pdf
[31] https://transition.fcc.gov/national-broadband-plan/national-broadband-plan.pdf
[32] https://www.squirepattonboggs.com/~/media/files/insights/publications/2011/10/spectrum-trading-in-the-eu-and-the-us--shifting-__/files/tel12_squire-sanders_ver4/fileattachment/tel12_squire-sanders_ver4.pdf

policies within ITU framework. But since several year, the European Institutions have been acquiring more and more power to harmonise spectrum policies and procedures across Europe.[33]

3.3.2. Artificial Intelligence in the U.S.

On February 11, 2019, President Trump announced the American AI Initiative, which is a concerted effort to promote and protect national AI technology and innovation. The Initiative implements a whole-of-government strategy in collaboration and engagement with the private sector, academia, the public, and like-minded international partners. It directs Federal agencies to pursue a multipronged approach to advance AI, including:

- promoting sustained AI R&D investment;
- enhancing access to high-quality cyberinfrastructure and data;
- removing regulatory barriers, ensuring that America leads in the development of technical standards for AI;
- providing education and training opportunities to prepare the American workforce for AI;
- developing and implementing an action plan to protect US technological advantage in AI[34].

Figure 4 - Key agencies involved in U.S. AI presidential initiative

The overall philosophy behind this initiative is summarised in this statement: *"*We will create a national climate where scientists and technologists successfully develop their new AI inventions here in the United States. Under this Administration, **we are removing regulatory and other barriers to the safe development and**

33 https://www.squirepattonboggs.com/~/media/files/insights/publications/2011/10/spectrum-trading-in-the-eu-and-the-us--shifting-__/files/tel12_squire-sanders_ver4/fileattachment/tel12_squire-sanders_ver4.pdf
34 https://www.whitehouse.gov/ai/executive-order-ai/

testing of AI technologies, to enable the creation of new AI-based industries and the adoption of AI by existing industries."

In operational terms, the National AI R&D Strategic Plan: 2019 Update[35] establishes a set of objectives for Federally funded AI research, identifying the following eight strategic priorities:

- Strategy 1: Make long-term investments in AI research. Prioritize investments in the next generation of AI that will drive discovery and insight and enable the United States to remain a world leader in AI.
- Strategy 2: Develop effective methods for human-AI collaboration. Increase understanding of how to create AI systems that effectively complement and augment human capabilities.
- Strategy 3: Understand and address the ethical, legal, and societal implications of AI. Research AI systems that incorporate ethical, legal, and societal concerns through technical mechanisms.
- Strategy 4: Ensure the safety and security of AI systems. Advance knowledge of how to design AI systems that are reliable, dependable, safe, and trustworthy.
- Strategy 5: Develop shared public datasets and environments for AI training and testing. Develop and enable access to high-quality datasets and environments, as well as to testing and training resources.
- Strategy 6: Measure and evaluate AI technologies through standards and benchmarks. Develop a broad spectrum of evaluative techniques for AI, including technical standards and benchmarks.
- Strategy 7: Better understand the national AI R&D workforce needs. Improve opportunities for R&D workforce development to strategically foster an AI-ready workforce.
- Strategy 8: Expand public-private partnerships to accelerate advances in AI. Promote opportunities for sustained investment in AI R&D and for transitioning advances into practical capabilities, in collaboration with academia, industry, international partners, and other non-Federal entities.

These strategies are applied by the federal agencies in charge of the 15 application domains listed in the figure below, emphasis being put on Transportation; Healthcare; Manufacturing; Financial Services; Agriculture; Weather Forecasting; National Security & Defense.

35 https://www.whitehouse.gov/wp-content/uploads/2019/06/National-AI-Research-and-Development-Strategic-Plan-2019-Update-June-2019.pdf

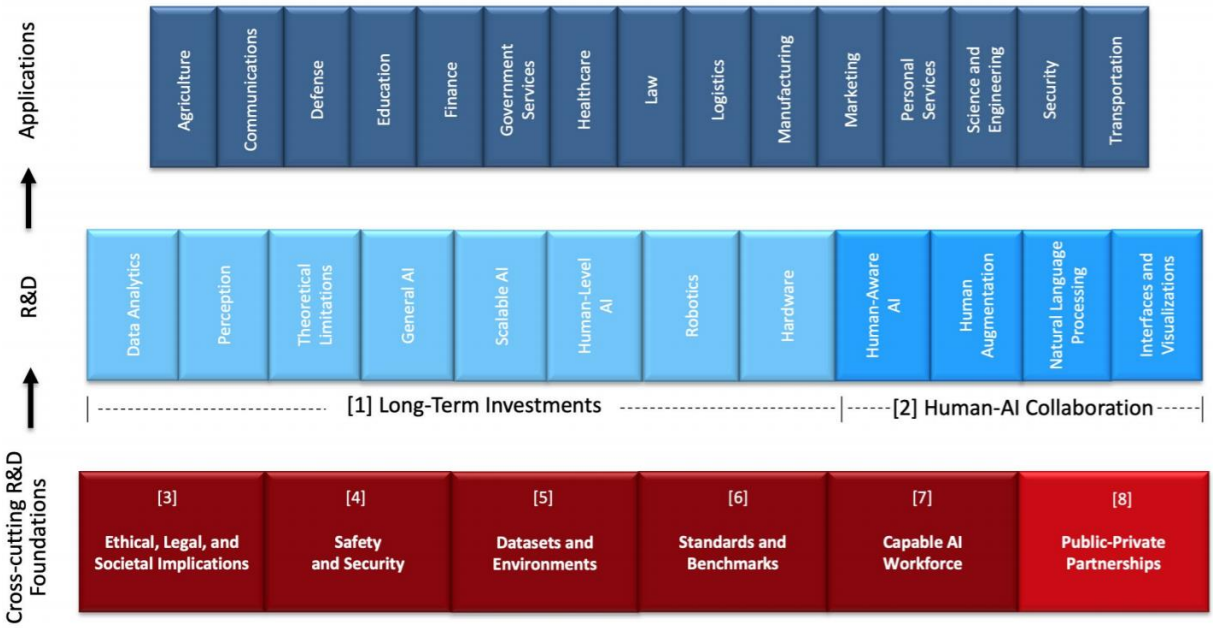

Figure 5 - Organization of the AI R&D Strategic Plan (source: National AI R&D strategic plan: 2019 update)

European approach

EC's COM(2018) 237 Communication set out a European initiative on AI, which aims to:

- Boost the EU's technological and industrial capacity and AI uptake across the economy, both by the private and public sectors. This includes investments in research and innovation and better access to data.
- Prepare for socio-economic changes brought about by AI by encouraging the modernisation of education and training systems, nurturing talent, anticipating changes in the labour market, supporting labour market transitions and adaptation of social protection systems.
- Ensure an appropriate ethical and legal framework, based on the Union's values and in line with the Charter of Fundamental Rights of the EU. This includes forthcoming guidance on existing product liability rules, a detailed analysis of emerging challenges, and cooperation with stakeholders, through a European AI Alliance, for the development of AI ethics guidelines.

Moreover, in its Communication on a Coordinated Plan on Artificial Intelligence - COM(2018) 795, the EC set the frame “to maximise the impact of investments at EU and national levels, encourage synergies and cooperation across the EU, including on ethics, foster the exchange of best practices and collectively define the way forward.[36]”, each member states being encouraged to draft national plans in line with these common objectives.

[36] https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=56017

The Commission is increasing its annual investments in AI by 70% under the research and innovation programme Horizon 2020. It will reach EUR 1.5 billion for the period 2018-2020. It will:

- Connect and strengthen AI research centres across Europe;
- Support the development of an "AI-on-demand platform" that will provide access to relevant AI resources in the EU for all users;
- Support the development of AI applications in key sectors.

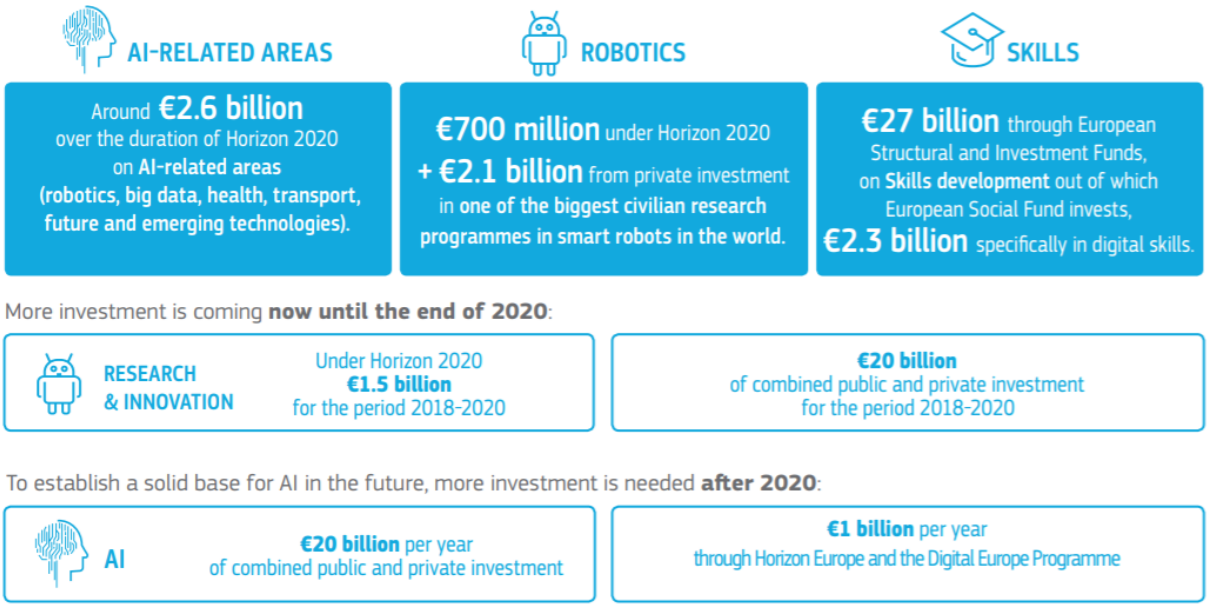

Figure 6 - EU investment in AI (Source: Artificial Intelligence for Europe factsheet[37])

The European Commission has set out its vision for AI, which is to be trustworthy and human-centric. Three pillars underpin the Commission's vision:

- Increasing public and private investments in AI to boost its uptake;
- Preparing for socio-economic changes;
- Ensuring an appropriate ethical and legal framework to protect and strengthen European values.

As such, the European AI strategy and the coordinated plan "put forward trust as a prerequisite to **ensure a human-centric approach to AI**. The AI HLEG presented a first draft of the Guidelines in December 2018."

EU-US collaboration on AI

As for many other NGI-related topics, EU and US tend to differ in their approach on AI developments. US approach for innovation implies to enforce minimal regulations on the private sector. The understanding is that a free market-oriented approach of AI progress would require little intervention from the government. The EU's

[37] http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=51610

first approach is to concentrate on the public sector by ensuring that ethical framework is carried through without bias from the industry.

An interesting article [38] details how these two approaches impact the way AI developments on 'case studies', applications of innovations to the respective contexts is considered. What appears from such considerations is that the major barrier EU R&D&I stakeholders are / will face when accessing the US AI research and innovation and markets are linked to the requirements for running the technologies (thus compatibility issues) between GDPR/AI ethics compliant tools and US 'unrestricted' data-fed systems.

Are US and EU visions on how to proceed with AI developments contradictory? Probably not, but the barriers set by these economic areas through their (un)regulated approaches will hinder the potential for collaborative developments if remaining differentiated. More importantly, these will also affect the performance of each area's AI ecosystems as well, harming performances within global competition. Centre for Data Innovation recent event[39] on that topic proved that while there is a common understanding on the necessity to settle for cooperative schemes between the EU and US by highlighting the pitfalls of non-cooperative approaches, no concrete actions are planned.

On the other hand, EU and US regulation bodies are cooperating within international organisations, such as the OECD or G20 cooperation on common general principles, which is conferring a great opportunity to agree on common principles.

What can concretely be done for enhancing EU-US cooperation on AI?

As for many other ICT related topics, finding common 'vocabularies' for certain technologies or applications are the smallest yet most efficient steps to create fertile developments. Regardless of grand schemes or strategies, conferring R&D&I stakeholders with the opportunity to share a common taxonomy of AI technologies with their own authorities and / or partners are key - achievable – steps towards an actionable AI common path.

[38] https://towardsdatascience.com/looking-at-ai-focused-case-studies-139e0bb98ff5
[39] https://www.datainnovation.org/2019/07/event-recap-enhancing-transatlantic-cooperation-on-ai/

3.3.3. Data flow

The European approach

The European Union's Internal Market allows the free movement of people, capital, goods and services in the European Union. In recent years, the digital market has grown, and it has become necessary to adapt European law to take this dimension into account. The idea of the European Digital Single Market is to create a common market and the conditions for stronger competition between digital service providers. This requires removing online barriers to citizens' access to goods and services, thus also removing constraints businesses and start-ups in the Internet sector are facing. Free flow of data across national borders is therefore a strong need of the Digital Single Market; removing the remaining restrictions on data flows within Europe is a central part of the Digital Single Market Strategy.

The figure below highlights the situation before the Free flow of non-personal data regulation.

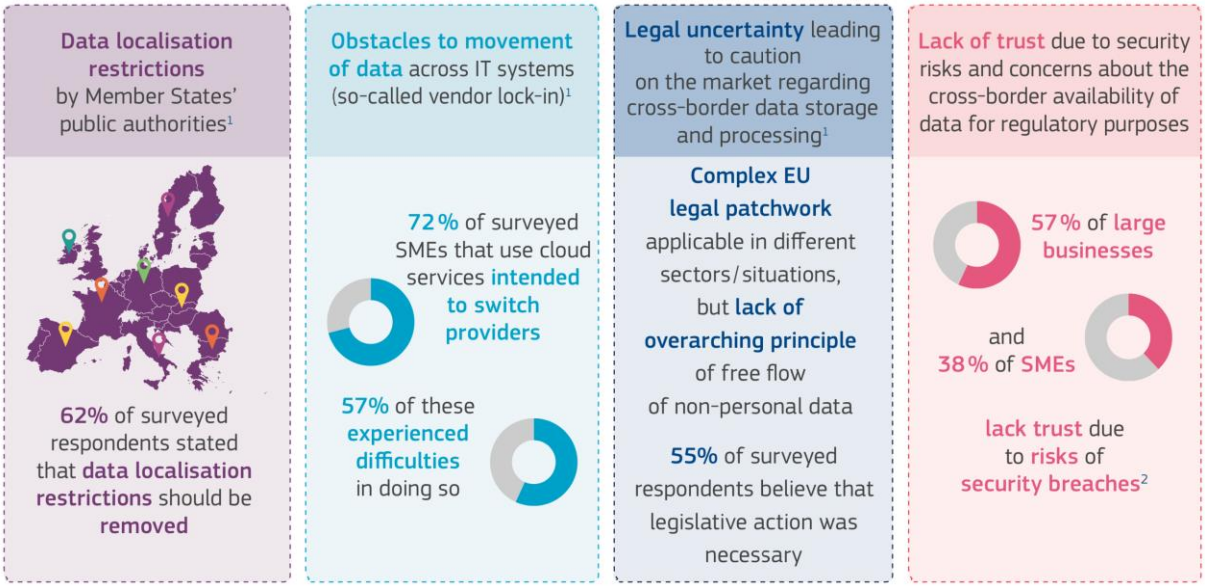

Figure 7 - Situation before the EU data flow regulation (source: European Commission – Free flow of non-personal data factsheet)

Free flow of non-personal data means unrestricted movement of data across borders and IT systems in the EU. It is a key building block of the Digital Single Market and considered the most important factor for the data economy to unleash its full potential and to double its value to 4% of GDP in 2020[40]. The new measures are in line with already existing rules for the free movement and portability of personal data in the EU and will bring new benefits for EU stakeholders, such as lower costs for data services, greater flexibility in using cloud providers, easy access to new markets (across EU borders) for SMEs…

To further increase the cross-border exchange of data and boost the data economy, in November 2018 the European Parliament and the Council adopted the Regulation (EU) 2018/1807 on a framework for the free flow of non-personal data in the European Union. The Regulation entered into forces on the 28 May 2019. The

[40] https://ec.europa.eu/digital-single-market/en/news/free-flow-non-personal-data

principle of free movement of personal data is already laid down in Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (the 'General Data Protection Regulation'). As a result, there is now a comprehensive framework for a common European data space and the free movement of all data within the European Union.

The purpose of this new regulation is to ensure the free flow of data other than personal data within the Union by establishing rules on data localization requirements, data availability for competent authorities and data porting for business users.

One single principle across the EU, i.e. guaranteeing the free flow of non-personal data, has been agreed, and sets the following rules[41]:

- The free flow of non-personal data principle removes unjustified data localisation restrictions imposed by public
- authorities, enhancing legal certainty and raising trust.
- The principle of data availability for competent authorities makes sure that the data remains accessible for regulatory and supervisory control also when stored or processed across borders in the EU.
- Actions to encourage cloud service providers to develop self-regulatory codes of conduct for easier switching of provider and porting data back to in-house servers, which must be implemented by mid-2020.
- Security requirements on data storage and processing remain applicable, also when businesses store or process data in another Member State. The same applies when they outsource data processing to cloud service providers.
- Single points of contact in each Member State, to liaise with other Member States' contact points and the Commission to ensure the effective application of the new rules on the free flow of non-personal data.

The interaction between the Free Flow of Non-Personal Data Regulation and the General Data Protection Regulation - mixed datasets

As the General Data Protection Regulation (GDPR) already provides for the free movement of personal data within the Union, associated with the data flow regulation, both regulations ensure a coherent approach to the free movement of all data in the EU, enabling the free flow of any data within EU borders and thus creating a common European space for data. In such context, and to provide more clarity to businesses, the European

[41] http://ec.europa.eu/newsroom/document.cfm?doc_id=47000

Commission has published an informative guidance which aims at highlighting principles of both regulations and guiding stakeholders on how to handle data across EU borders[42].

The guidance aims to help users understand the interaction between the Regulation on the free flow of non-personal data and the General Data Protection Regulation (GDPR), especially as regards datasets composed of both personal and non-personal data.

Examples of mixed datasets:

- A company's tax record, mentioning the name and telephone number of the managing director of the company;
- Datasets in a bank, such as those with client information and transaction details;
- A research institution's anonymised statistical data and the raw data initially collected, such as the replies of individual respondents to statistical survey questions;
- Analysis of operational log data of equipment in the manufacturing industry.

Personal versus non-personal data:

- The GDPR's free flow provision applies to the personal data part of the dataset
- The free flow of data (FFD) Regulation applies to the non-personal data part of the dataset

If a business processes mixed dataset, neither the FFD nor the GDPR obliges it to separate or store personal and non-personal data separately. If it decides not to separate them and process them as mixed datasets, the data protection rules will apply to the entire mixed dataset. The FFD and the GDPR together create legal certainty for companies, and guarantee that personal and non-personal data (even when they are included in a mixed dataset) can move freely within the EU. Therefore, companies can decide to store, transfer or process the mixed dataset anywhere in the EU, where they think it is the most beneficial for them.

EU-US data flows

The FFD covers data flow with the EU boundaries. Although it is a big step forward, this regulation doesn't cover data flow between Member States and non-EU counties. However, cross-border data flows are indispensable to global trade and contribute significantly to growth and job creation by permitting business operations for companies of all sizes. At the same time, they allow access to a wider variety of goods and services, eventually of better quality and more competitively priced. The benefits of enabling and facilitating cross-border data flows are therefore global.

In such context, the EU and the US worked together on a shared mechanism, the Privacy Shield Framework, to allow the flow of data between both continents. As per its definition on the Privacy Shield website, "the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks were designed by the U.S. Department of Commerce, and the European Commission and Swiss Administration, respectively, to provide companies on both sides of the

42 https://ec.europa.eu/digital-single-market/en/news/practical-guidance-businesses-how-process-mixed-datasets

Atlantic with a mechanism to comply with data protection requirements when transferring personal data from the European Union and Switzerland to the United States in support of transatlantic commerce."

This mechanism is a self-certification mechanism for companies established in the US that has been recognized by the European Commission as offering a level of adequate protection for personal data transferred by a European entity to companies established in the United States. This mechanism is therefore considered to offer legal guarantees for such data transfers.

As highlighted by the European Commission[43], the framework includes:

- strong data protection obligations on companies receiving personal data from the EU;
- safeguards on US government access to data;
- effective protection and redress for individuals;
- an annual joint review by EU and US to monitor the correct application of the arrangement.

Before transferring personal data to a US-based company that claims to be certified to the Data Protection Shield, European companies must ensure that the US company has an active certification and that certification covers the data in question. In order to check whether a certification is active and applicable, European companies should consult the Data Protection Shield List which is published on the US Department of Commerce website[44]. All US companies that have successfully completed the self-certification process are listed. The Data Protection Shield List further specifies the type of personal data for which a US company has self-certified (HR or non-HR data) and also provides information on the services it offers.

The US Department of Commerce also lists companies that are no longer part of the Data Protection Shield. These companies are no longer allowed from the end of their membership, to receive personal data relating to persons from the EU under the Privacy Shield framework. For the transfer of personal data to companies that are not or no longer members of the Data Protection Shield, other EU-approved transfer mechanisms may be used, such as the Rules for the Protection of Data binding contracts or the Standard Contractual Clauses for the transfer of personal data relating to persons from the EU to companies established in the United States.

Follow-up

The European Commission must prepare an annual report on the experience gained from the Privacy Shield and forward it to the European Parliament and the European Council. This audit commissioned by the Commission is carried out in cooperation with the US Department of Commerce as well as experts from US

[43] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/eu-us-data-transfers_en
[44] https://www.privacyshield.gov/list

and European data protection authorities with the assistance of non-governmental organisations and "other interested third parties". In such context, in its latest report[45] (published in December 2018), the European Commission concludes that the United States continues “to ensure an adequate level of protection for personal data transferred under the Privacy Shield from the Union to organisations in the United States”.

3.3.4. Privacy

There is no single principal data protection legislation in the United States. Rather, a jumble of hundreds of laws enacted on both the federal and state levels serve to protect the personal data of US residents. At the federal level, the Federal Trade Commission Act (15 U.S. Code § 41 et seq.) broadly empowers the US Federal Trade Commission (FTC) to bring enforcement actions to protect consumers against unfair or deceptive practices and to enforce federal privacy and data protection regulations. However, rather than describing privacy context in the US, this section rather focuses on explaining the impact of GDPR in the US – i.e. which are the consequences of this EU regulation on US stakeholders having business/activities in the EU or with EU citizens.

In order to be compliant with the GDPR rules, US companies have to update their US privacy incident-response playbook in at least the following ten areas[46]:

10 areas	In the US privacy rules	In GDPR rules
Definition of a data breach	A data breach is defined as an “unauthorized access or acquisition” only of a limited set of data as Social Security number and credit card numbers	A data breach is defined as a “breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data” and “personal data” includes any data that can be directly or indirectly associated with a living individual
Risk of harm threshold for reporting	There are no specific rules for which the breaches must be reported	It is specified that breaches that must be reported are those that pose a risk of harm to individuals “rights and freedoms”
Safe harbour for strong security measures	The safe harbour for non-reporting is limited to data that is encrypted in storage and transit	“If appropriate technical and organizational measures” were implemented to protect the data, the companies do not have to report the breach

[45] https://ec.europa.eu/info/sites/info/files/report_on_the_second_annual_review_of_the_eu-us_privacy_shield_2018.pdf

[46] https://www.pwc.com/us/en/services/consulting/cybersecurity/library/broader-perspectives/gdpr-differences.html

Timing of the notifications	The companies have to notify individuals in the 5 to 30 days after the breach	Companies must make notifications "without undue delay and, where feasible, not later than 72 hours after having become aware of it"
Recipient of the notifications	The companies have to notify the affected individuals, state attorneys, general and federal agencies	If the breach causes a risk to the rights and freedoms of individuals, the companies must notify their lead data-protection authority and if the breach is of high risk for the individuals they have to be notify as well
Content of the notifications	The content of the data-breach notification letters depends on the US states and federal agencies	The standardized letters must specify the nature of the compromised data, the number of data affected, the name of the company's DPO, contact information, the likely consequences for the data subjects and measures taken to reduce the risks to individuals
No credit-monitoring expectation	Remedies such as credit monitoring to individuals are not mandatory but companies do it most of the time in order to meet the public relations expectation	It is not mandatory for companies to provide any such remedy to data subjects
No "walls of shame"	There is a public-facing website listing of data breaches reported to several US state attorneys general and the US department of Health and Human Services	No EU stakeholder maintains a similar website, but it is required that EU data-protection authorities maintain public lists of data-protection impact assessments
Obligations for processors to notify	The holding of third parties accountable to provide timely notification of breaches to their clients depends on the clients' contracting and vendor-management processes	It is required that the third-party data processors report to clients data breaches involving their clients' data "without undue delay after becoming aware"
Post-mortem documentation	A post-mortem process for continuous improvement is a best practice in the US – some laws even require this step	The companies who have experienced a data breach have to document the facts related to the breach and remedial action taken to prevent a reoccurrence

For the companies that do business internationally, in an EU country, the European security mandate must be adhered to. Moreover, it is likely that the US creates its own set of national data privacy laws. Indeed, in 2018, leading US-based technology companies called on the federal government to pass a law similar to GDPR and in February 2019, the US Government Accountability Office made the same recommendation. Therefore, it is important to highlight and prepare US companies for the needed changes in processes to follow the new data privacy laws.

In the case a company does not apply to these rules there can be several types of consequence to it:

- a fine equalling two to four percent of the company's global annual revenue for the most recent fiscal year;
- costs associated with data breaches including legal fees for any counselling or action taken by the company in its defence, civil and criminal penalties under US federal regulations and potential lawsuit pay-outs;
- non-financial costs: a loss to the company's reputation and integrity, a loss in the company's customer base[47].

For many US-based the threats of those consequences are real. Formal complaints were filed by seven EU countries against Google in 2018 concerning its Android operating system and its GPS tracking system that could not be turned off by disabling the "Location History" option (the "Web and App Activity" has to be also disabled. Moreover, the important scale at which Google tracks and monetizes the users' every move is disappointing for many. Therefore, Google could be fined up to 4% of its annual revenue which represent $4 billion. For Facebook, the threat of facing charges of violating GDPR is also real since the company did not handle well the data breach that occurred in 2018 that compromised more than 50 million accounts: under GDPR rules, data breaches should be notified by the company within 72 hours of discovering its existence but Facebook did not respect this timeline. Uber also received a GDPR fine in 2018 for how it handled a data breach (the company attempted to cover the data breach) of $158 million.

Moreover, as a consequence of this GDPR rule, US states are taking actions to pass GDPR-style data protection laws as it is the case for California which Governor, Jerry Brown, signed the California Consumer Privacy Act of 2018 (also called the "GDPR Lite") that will go into effect in 2020 or the US Senator Ron Wyden of Oregon which submitted a GDPR-like privacy bill (but it has not been passed yet, in 2019).[48]

Also, a recent IBM poll has revealed that for 78% of US respondents a company's ability to keep their data private is "extremely important", and only 20% "completely trust" organizations with their data and their privacy. And this has an important impact on the company's business. Indeed, the same poll revealed that 75% of the

[47] https://www.semshred.com/the-impact-of-gdpr-on-us-companies-and-organizations/
[48] https://www.datanami.com/2018/12/05/six-months-in-gdprs-impact-uncertain-in-the-u-s/

respondents will not buy a product from a company, no matter how great the products are, if they don't trust the company to protect their data.[49]

In 2018, the status of the US companies' compliance to GDPR rules were as following for the two sectors in which data privacy is critical and which are known for having slow-moving cultures, processes and technology adoption, health and finance: 14% of US healthcare companies have only completed 25% of the GDPR compliance process and 21% of US finance companies have only completed 25% of the process[50].

Moreover, in the technology industry what is expected according to security experts to affect the most the companies are the legislation (53%), online retailers (45%), software companies (44%), financial services (37%), online services (34%) and retail (33%)[51].

Globally, large firms in the US are just doing the bare minimum to be able to check the GDPR box but it is not enough to be full GDPR compliant. The companies have to make invasive changes to their business processes and change their business culture. To do so, one of the most effective ways is to hire a chief data officer[52]. This change towards GDPR compliant systems is globally taking time in the US because it has important impacts on the companies' systems, processes and resources. For 10% of companies this change is expected to cost them more than $1 million according to a Business Insights article[53], for 24% of the US companies between $100 000 and $1 million and for about two-thirds (66%) it is expected to cost them between $50 000 and $100 000.

[49] https://www.sparkpost.com/blog/effects-gdpr-us-financial-services-businesses/
[50] https://www.sparkpost.com/blog/effects-gdpr-us-financial-services-businesses/
[51] https://www.emarketer.com/content/how-us-companies-are-becoming-gdpr-compliant
[52] https://www.datanami.com/2018/12/05/six-months-in-gdprs-impact-uncertain-in-the-u-s/
[53] https://businessinsights.bitdefender.com/as-businesses-rush-to-comply-with-gdpr-some-face-costs-of-over-1-million

4. Conclusions

The US and the EU have different visions and approaches to privacy, data protection and the technology industry. While the US favours a more sectoral approach that relies on a combination of legislation, regulation and self-regulation, the EU tends to rely more heavily on legislation. This complicates the relationship. However, the two sides share the goal of allowing data to flow between Europe and the US while ensuring a high level of protection for their respective citizens' privacy and personal data. A key task for EU officials will be to keep their US counterparts informed about the implementation of the new General Data Protection Regulation.[54]

In such context, and as conclusion, Sir Tim Berners-Lee, inventor of the WWW, can be quoted: "Governments must translate laws and regulations for the digital age. They must ensure markets remain competitive, innovative and open. And they have a responsibility to protect people's rights and freedoms online. (...) Companies must do more to ensure their pursuit of short-term profit is not at the expense of human rights, democracy, scientific fact or public safety. Platforms and products must be designed with privacy, diversity and security in mind. (...) And most important of all, citizens must hold companies and governments accountable for the commitments they make, and demand that both respect the web as a global community with citizens at its heart".

Technologies and new services deployments will be made possible only if they are supported by strong policies, protecting citizens but without hindering innovation. This is a challenge which is even more true in the context of NGI / Future Internet cooperation between the European Union and the United States of America, as not being synchronized on policies and regulations would create fragmented markets, thus having strong impacts on citizens, on both sides of the Atlantic.

54 https://www.chathamhouse.org/sites/default/files/publications/research/2018-04-11-future-united-states-europe-irreplaceable-partnership.pdf