D3.5 Policy briefs repertoire – EU-US NGI policy recommendations

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 | Policy briefs repertoire – EU-US NGI policy recommendations
Number of the deliverable | D3.5
Related WP number and name | WP3 - Think NEXUS Community Building and Expansion
Related task number and name | Task 3.1 Think NEXUS Stakeholder Management
Deliverable dissemination level | Public
Deliverable due date | 30/11/2020
Deliverable submission date | 04/12/2020
Task leader/Main author | Fabrice Clari (GAC)
Contributing partners | GAC
Reviewer(s) | Hubert Santer (GAC)

Abstract
This deliverable collects the collection of policy briefs and white papers released by Think NEXUS Policy Expert Group.

Keywords
Next Generation Internet; EU-US collaboration; Policies; Digital Policy; Regulations.
Revisions

<table>
<thead>
<tr>
<th>Version</th>
<th>Submission date</th>
<th>Comments</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>v0.1</td>
<td>17/11/2020</td>
<td>Table of content</td>
<td>Jose Gonzalez (AUS)</td>
</tr>
<tr>
<td>v0.2</td>
<td>19/11/2020</td>
<td>Content</td>
<td>Fabrice Clari (GAC)</td>
</tr>
<tr>
<td>v0.3</td>
<td>3/12/2020</td>
<td>Quality review</td>
<td>Hubert Santer (GAC)</td>
</tr>
<tr>
<td>v1.0</td>
<td>04/12/2020</td>
<td>Final version</td>
<td>Fabrice Clari (GAC)</td>
</tr>
</tbody>
</table>

Disclaimer

This document is provided with no warranties whatsoever, including any warranty of merchantability, non-infringement, fitness for any particular purpose, or any other warranty with respect to any information, result, proposal, specification or sample contained or referred to herein. Any liability, including liability for infringement of any proprietary rights, regarding the use of this document or any information contained herein is disclaimed. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted by or in connection with this document. This document is subject to change without notice. Think NEXUS has been financed with support from the European Commission. This document reflects only the view of the author(s) and the European Commission cannot be held responsible for any use which may be made of the information contained.
# Acronyms and definitions

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>CEO</td>
<td>Chief Executive Officer</td>
</tr>
<tr>
<td>CTO</td>
<td>Chief Technology Officer</td>
</tr>
<tr>
<td>EC</td>
<td>European Commission</td>
</tr>
<tr>
<td>EU</td>
<td>Europe/ European Union</td>
</tr>
<tr>
<td>ICT</td>
<td>Information and Communications Technology</td>
</tr>
<tr>
<td>NGI</td>
<td>Next Generation Internet</td>
</tr>
<tr>
<td>NSF</td>
<td>National Science Foundation</td>
</tr>
<tr>
<td>R&amp;D</td>
<td>Research and Development</td>
</tr>
<tr>
<td>SME</td>
<td>Small and medium-sized enterprise</td>
</tr>
<tr>
<td>STEM</td>
<td>Science, technology, engineering, and mathematics</td>
</tr>
<tr>
<td>US/ USA</td>
<td>United States of America</td>
</tr>
</tbody>
</table>
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.
# Table of contents

Executive Summary .................................................................................................................. 8

1. Objective ............................................................................................................................. 9
   1.1. Policy Briefs .................................................................................................................... 9
   1.2. White Papers .................................................................................................................. 10

2. State of Play ......................................................................................................................... 12
   2.1. List of Publications ....................................................................................................... 12

3. Next Steps ............................................................................................................................ 16

Annex 1 – The future of EU-US data flows ............................................................................. 17

Annex 2 - Artificial Intelligence – Comparison of US’s and EU’s approaches ....................... 18

Annex 3 - Digital Services Act (EU) vs COPRA (US) ............................................................... 19
Table of figures

Figure 1 – Design of Think NEXUS Policy Brief ................................................................. 10
Figure 2 – White Paper Characteristics vs Other Content (Source: Publicize) .................. 11

Table of tables

Table 1 – References Publication #1 .................................................................................. 12
Table 2 – References Publication #2 .................................................................................. 13
Table 3 – References Publication #3 .................................................................................. 14
Table 4 – References Publication #4 .................................................................................. 15
Executive Summary

One of the most important objectives aimed by Think NEXUS is to share and spread out insights and recommendations set out by the members of the Expert Groups, comparing the European perspective against the United States, but also conveying into principles shared by both regions. To that end, the project established a plan to edit and release a collection of publications addressing relevant topics to the scope of each group, aligning with the priorities defined for the think tank in the series of deliverables outlining the strategy throughout the project lifetime - i.e. D1.2 (v1, January 2019), D1.3 (v2, October 2019) and D1.4 (v3, July 2020).

This deliverable D3.5 gathers the publications released by the ‘Policy’ Expert Group on topics identified as important for the EU-US cooperation: data flows, Artificial Intelligence and the Digital Service Act. Additionally, this report includes the summary of the NGI chapter prepared by Think NEXUS for the “ICT Policy, Research, and Innovation: Perspectives and Prospects for EU-US Collaboration”, published in November 2020.
1. Objective

One of the most important objectives aimed by Think NEXUS is to design and disseminate insights set out by the members of the Expert Groups, comparing the European perspectives against U.S. contexts with the final objective to provide the European Commission with recommendations on key topics for future EU-US cooperation on NGI-related areas. To that end, the project established a plan to edit and release a collection of publications addressing topics relevant to the scope of each group, aligning with the priorities defined for the think tank in the series of deliverables outlining the strategy throughout the project lifetime.

The series of deliverables D3.3, D3.4 and D3.5 assemble the repertoires/compendium of these publications, covering the research lines of Science & Technology, Innovation & Entrepreneurship, and Policy Expert Groups respectively.

The types of publications considered in this scope are ‘Policy Briefs’ and ‘White Papers’, detailed below.

1.1. Policy Briefs

Policy briefs are short publications that present findings and recommendations of a single research topic to government policymakers and other stakeholders interested in formulating or influencing policies. These items are straight to the point, based on evidence and framing the big picture. We can consider two basic types:

- **Advocacy brief** argues in favour of a particular course of action;
- **Objective brief** gives balanced information for the policymaker to make up his/her mind.

Think NEXUS targets advocacy briefs directed to the European Commission - most particularly to the Next Generation Internet Unit - with the ambition to identify friction points between Europe and the USA in critical aspects affecting the NGI vision and strategy. In addition, they shall also pinpoint and recommend specific measures to reinforce the Transatlantic cooperation in forthcoming funding programmes.

Guidelines

- **Format**: A4 sheets, containing between 2 and 4 pages of content (without template overheads)
- **Edition**: Coordination by Expert Group chairs, with potential contribution from experts
- **Design**: Common format, defining an attractive and professional style, including graphical material

---

1.2. White Papers

White papers are informative documents, promoting or highlighting findings about a particular product, service, technology or methodology. While brochures and other promotion materials are often oriented towards an eye-catching design, a white paper intends to provide persuasive and factual evidences that a particular research topic is a better approach or solution to a given problem or challenge rather than another. These in-depth, technical documents are designed to discuss an issue or situation in detail.

White papers offer a number of benefits:

- **Education**: A white paper educates the audience on a specific topic, such as a problem they may not be aware of;
- **Pathfinders**: By accessing the content of a particular white paper, readers may explore further about other research topics, generating leads for the Next Generation Internet and the Digital Agenda of the European Commission;
- **Leadership**: By providing the expertise on a topic in hand, the editor establish itself as an authority and thought leader within the community. This helps to position a given initiative as the solution to the problem;
- **Legitimacy**: White papers are not based on mere speculation. It’s a well-researched document, backed up by data and the experience of experts. This builds legitimacy with the target audience;

---

**Keystone Document:** The paper can act as leverage for other activities emerging from the document, such as blog posts and webinars;

---

Think NEXUS edits white papers to disseminate upon researches emerging from the Expert Groups, spreading the insights among the broader NGI community, persuading readers to realize about the need for a human-centric digital agenda and the influence of the EU-USA axis to make it possible. To this end, the papers follow a common scheme: 1) definition of the problem or issue; 2) EU vision; 3) USA vision; 4) comparison between approaches and/or the strength of a joint cooperation.

**Guidelines**

- **Format:** A4 sheets, containing between 5 and 8 pages of content (without overheads)
- **Edition:** Coordination by Expert Group chairs, with mandatory contribution from EU/ US experts
- **Design:** Common format, defining an attractive and professional style, including graphical material

---

2. State of Play

This deliverable D3.5 gathers the publications released by the ‘Policy’ Expert Group, taking as reference the research priorities identified in D1.3 and main trends identified by the consortium and out of discussions with experts.

2.1. List of Publications

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Book chapter</td>
</tr>
<tr>
<td></td>
<td>Date</td>
</tr>
<tr>
<td></td>
<td>November 2020</td>
</tr>
<tr>
<td>Experts</td>
<td>Glenn Ricart, Jose Gonzalez, Vasilis Papanikolaou, Hubert Santer, Fabrice Clari, Nikos Sarris, Peter Van Daele, Wouter Tavernier</td>
</tr>
<tr>
<td>Open access</td>
<td>Not available at the time of writing.</td>
</tr>
</tbody>
</table>

This work⁴ is part of the “ICT Policy, Research, and Innovation: Perspectives and Prospects for EU-US Collaboration” book⁵.

Digital transformation is pushing all market sectors to level up their digital capabilities to better serve customers and improve the user experience. The European Commission launched in 2016 the Next Generation Internet (NGI) initiative as part of the DSM strategy. NGI includes a number of different – but always interrelated – emerging technologies in the following focus areas: artificial intelligence and autonomous machines, blockchains and distributed ledgers, big data, Internet of Things, 5G, cybersecurity and privacy technologies, cloud and edge computing, and open data.

As for cooperation in the field of Information and Communications Technology, Europe and the United States should seek a joint framework to expand efforts in new emerging technologies, while preserving common principles around a comprehensive EU–US digital economy dialogue. The NGI Initiative is an important opportunity to radically rethink the way the Internet works today, and more human-focused narratives are needed more than ever.

Personal data privacy management across the Atlantic is among the core topics tackled by the Think NEXUS project. This document is based on a discussion between Think NEXUS and two experts from the project's working group (one from Europe, the other one from the US), and explore the impact of the latest European decision on the EU-US Privacy Shield agreement.

In the past 30 years, there has been an important globalisation of ICT infrastructures. Therefore, data flows and free flows of data have become more and more important for the European and the US economy and with it comes the importance to be able to exchange data between these two regions in a simple manner.

Nevertheless, the data protection legislations in Europe and in the US are different. In order to facilitate and to enable a simple data exchange between the two transatlantic regions, they need to build equivalent data protection laws.

Between 1998 and 2000, the Safe Harbour Agreement was elaborated, signed and has been then used to regulate data flows between the European Union and the United States. But some doubts regarding the effectiveness of this mechanism emerged and a legal case against this agreement was led by Max Schrems. Therefore, the Safe Harbour Agreement was declared invalid by the European Court of Justice (ECJ) in October 2015. This led to further discussions between the EU and the US around "a renewed and sound framework for transatlantic data flows with a higher level of protection". The Safe Harbour Agreement was then replaced by the Privacy Shield, again invalidated after a few years.

In such context, this white paper exposes consequences of the invalidation of the Privacy Shield and new challenges to be overcame, and proposes recommendations in order to move forward towards a new EU-US agreement with regards to data flows.
Table 3 – References Publication #3

<table>
<thead>
<tr>
<th>Title</th>
<th>Artificial Intelligence – Comparison of US’s and EU’s approaches</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>White paper</td>
</tr>
<tr>
<td>Date</td>
<td>November 2019</td>
</tr>
<tr>
<td>Annex</td>
<td>2</td>
</tr>
</tbody>
</table>

**Rationale**

Artificial Intelligence has been highlighted as a main topic to be tackled by Think NEXUS experts during the first workshop (July 2019), as documented in the deliverable D2.4 (1st Thematic Workshop report). As that time, it had been stated that “AI is a major technology the Next Generation Internet builds upon. As such, the development of solutions generates a new field of ruling for policy makers. However, the semantics behind AI- technologies and applications are not shared between both sides of the Atlantic (and event within each region itself). Cooperation on AI taxonomy could confer the opportunity to better tie EU and US developments and mutual understanding, thus fostering this technology’s growth.”

Based on that outcome, the team considered it was important to put approaches, both from the European Commission (starting from the EC 2018’s communication on IA) and the US, in perspective. The “Artificial Intelligence – Comparison of US’s and EU’s approaches” white paper presents both visions and compare them.
### Rationale

This report comes from a trend analysis which had been performed by GAC after an exchange with EC representatives.

As recently commented by Thierry Breton, European commissioner for Internal market, “Online platforms have taken a central place in our life, in our economy and in our democracy”. However, legal and regulatory frameworks related to digital services are governed by the “Electronic Commerce” directive of June 8, 2000, which has become obsolete and no longer allows respond effectively to new digital challenges and the difficulties posed by the emergence of web giants.

Additionally, in its Agenda for Europe, Ursula von der Leyen has given its political guidelines for the next European Commission 2019-2024. Among the six political goals the president wants for Europe over the next five years is the ambition to create “a Europe fit for the digital age” – this means being able to better regulate web giants by “upgrading the liability and safety rules for digital platforms, services and products through a new Digital Services Act”.

In such context, the new Digital Services Act is compared to a bill which had been introduced in November 2019, the Consumer Online Privacy Rights Act ‘COPRA’.

It is worth noting that since the US bill COPRA stayed in ‘draft’ mode, the project did not further develop this topic.
3. Next Steps

Think NEXUS will update the collection of publications herein contained with new releases until the project end, releasing a second version of this deliverable. The topics will take into consideration (i) the new research lines defined in D1.4; as well as (ii) the feedback and inputs provided by the European Commission and external reviewers of the project.
Annex 1 – The future of EU-US data flows
Transatlantic crossings:
the Future of EU-US Data Flows

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.
Transatlantic crossings: the future of EU-US data flows

Think NEXUS, an EC-funded project, aims at reinforcing EU-US collaboration on NGI-related topics in three focus areas: Science and Technology, Innovation and Entrepreneurship and Policy. The aim is to boost strategic research, industrial partnerships and policy compliances in order to gain socio-economic benefits in both the EU and US regions.

In the framework of this project, we are regularly publishing several short articles aiming at comparing the US and the EU approaches in different topics of NGI and providing recommendations for further collaboration. The present document is focusing on the protection of data transferred from the EU to the US.

Introduction

In the past 30 years, there has been an important globalisation of ICT infrastructures. Therefore, data flows and free flows of data have become more and more important for the European and the US economy and with it comes the importance to be able to exchange data between these two regions in a simple manner.

Nevertheless, the data protection legislations in Europe and in the US are different. In order to facilitate and to enable a simple data exchange between the two transatlantic regions, they need to build equivalent data protection laws.

Between 1998 and 2000, the Safe Harbour Agreement was elaborated and signed. This set of principles aimed at ensuring the data transfers between the EU and the US complied with the European Data Directive 1995. It was based on the following 7 principles:

- **Notice**: Individuals should be informed that their data has been collected, how it will be used and how to contact the data holder for any queries;
- **Choices**: Individuals should be able to opt out as well as forward the relevant data to another third party;
- **Onward Transfer**: the transfer of any data can only happen with a third party that meets the required data protection principles;
- **Security**: a reasonable effort must be made to keep the data safe from loss or theft;
- **Data Integrity**: the data must be relevant and reliable for its original purpose of collection;
- **Access**: individuals should be able to access, correct and delete any information held about them;
- **Enforcement**: there must be effective means of enforcing these rules.

---

Transatlantic crossings: the future of EU-US data flows

The Safe Harbour Agreement was based on a self-certification mechanism: each US company self-certified that it will respect the data protection requirements from the EU. But some doubts regarding the effectiveness of this mechanism emerged and a legal case against this agreement was started and led by Max Schrems. Therefore, the Safe Harbour Agreement was declared invalid by the European Court of Justice (ECJ) in October 2015. This led to further discussions between the EU and the US around “a renewed and sound framework for transatlantic data flows with a higher level of protection.”

The EU-US Privacy Shield and its invalidation

Result of these discussions was the adequacy decision on the EU-US Privacy Shield adopted on the 12th of July 2016 (Decision 2016/1250) which became operational on the 1st of August 2016. This new arrangement aimed at providing stronger obligations on companies in the US to protect the personal data of Europeans and at stronger monitoring and enforcement by the US Department of Commerce and Federal Trade Commission (FTC), including through increased cooperation with European Data Protection Authorities.

“The new EU-US Privacy Shield will protect the fundamental rights of Europeans when their personal data is transferred to US companies. For the first time ever, the US has given the EU binding assurances that the access of public authorities for national security purposes will be subject to clear limitations, safeguards and oversight mechanisms. Also, for the first time, EU citizens will benefit from redress mechanisms in this area. In the context of the negotiations for this agreement, the US has assured that it does not conduct mass or indiscriminate surveillance of European.” Commissioner Jourová

The Privacy Shield arrangement included the following elements:

- Strong obligations on companies handling Europeans’ personal data and robust enforcement;
- Clear safeguard and transparency obligations on US government access;
- Effective protection of EU citizens’ rights with several redress possibilities.

However, this regime was also attacked in ECJ arguing that it still not is sufficient to guarantee the security of personal data. And indeed, on the 16th of July 2020, the ECJ issued a judgment declaring as invalid the Safe Harbour Agreement.

Therefore, this facilitated framework for data transfers has been abolished and the US was put on the same level than other countries which does not have a positive adequacy, meaning that companies could still use

---

data transfer mechanisms that were available for other countries such as standard contractual closes and other corporate mechanisms.

**Consequences of the invalidation of the Privacy Shield and the new challenges**

In practices, the invalidation of the Privacy Shield is inconvenient for many companies as using standard contractual clauses implies heavy administrative overhead. Indeed, it requires companies to conduct an assessment of themselves to guarantee that their particular circumstances taking into account all the details of their data processing activities, the scope, the scale of the data and its sensitivity, the likelihood that could be targeted, etc. are adequate to protect personal data. This is currently a heavy burden for many companies and this legally complicated situation is not going to get solved until the US and the EU agree on a political arrangement that streamlines the relationship again between the EU and the US as the Safe Harbour Agreement and the Privacy Shield Agreement did. This is particularly true as more than 5 300 companies in the US relied on the Safe Harbour Agreement and most of them are small and medium-sized companies which are scrambling to find a basis under EU law for transferring personal data.

For the US, this invalidation of the Privacy Shield Agreement is much larger than just a privacy issue: it is a national security issue which is an important challenge. Indeed, this invalidation raised questions regarding the standard contractual clauses, created new obligations on data exporters and imposed certain obligations on data protection authorities. These findings have created uncertainty regarding transatlantic data flows specifically as well as data transfers from the EU to certain other countries more broadly. The gist of this invalidation is: the subject seems to be a transatlantic matter, but the implications are much broader.

In addition, since the invalidation of the Privacy Shield, the US Commerce Department and the European Commission have published press releases and have committed to try to work together to build a framework addressing the core fundamental rights expressed by the ECJ in its decision. The ECJ observed that the US surveillance program conducted under the Section 702, the US Foreign Intelligence Service Act or the Executive order 12-333 both do not grant surveilled persons actionable of redress before independent and impartial court. The ECJ also identified two ways in which US surveillance law lacks essential equivalence to EU legislation: EU safeguards and more specifically the lack of an effective and enforceable right of individual redress and the issue of proportionality.

Moreover, another challenge is that with the ECJ’s invalidation of the Privacy Shield, it is the second invalidation of data protection EU-US agreements and this has created a broader uncertainty of data protection legislation and therefore, of the future of data flows. As a consequence, it can be observed that there is a crisis in the belief of the globalisation of data flows and a resurgence of the importance of data sovereignty. Indeed, more and more countries not just within the EU but also outside the EU have become
Transatlantic crossings: the future of EU-US data flows

convinced that their data is such a strategic important asset that they cannot run the risk anymore of foreign authorities, foreign countries exercising control over these data. Several examples illustrates this trend towards dividing data back into silos: discussions in the US around the social media TikTok that has been required to be sold to a US company in order to keep the data from US citizens in the US and similarly the European Commission is examining possibilities to do the same for Facebook, requiring Facebook to sell its European activities to a European company in order to shield the data. This trend can become a challenge for future EU-US collaboration in data protection as it goes against the work done since the last 20 to 30 years in this domain.

Next steps and recommendations

On the European side, companies that used to rely on the Privacy Shield Agreement now have to rely on another mechanism, the standard contractual clauses if they want to continue to transfer data to the US. Therefore, they have to identify whether there are adequate safeguards for the transfer of personal data and to screen what the risks are for the data to be intercepted and what can be done to mitigate those risks. Moreover, this assessment needs to be done on a case-by-case basis. The existing fundamental conflicts are between the safeguards that EU data protection laws expect to have versus the competences that apply in other countries. Therefore, for most research projects or organisations, the short term solution consists in assessing which kind of data transfer activities they are engaged in, assessing which risks are to run for those data processing activities and identifying whether they have alternatives that are easily available either through technical measures to mitigate the risk by scaling down the amount of data being transferred, or by looking for alternative providers. Nevertheless, none of these options are particularly viable, none of them are sustainable and all of them seem to be harmful in terms of societal progress. But, on the short term and on the scale of an individual research organisation, these solutions seem to be the only practical resources available. Other potential solutions are much more complicated and part of a much larger picture that cannot be influenced by companies or research projects.

In order to build a new EU-US collaboration framework regarding data flows, both sides of the Atlantic are undergoing specific actions.

Indeed, in the EU, discussions on the importance of standard contractual clauses have been engaged. Moreover, in early September 2020, the European Data Protection Board has formed two different task forces aiming at revising and updating standard contractual clauses. This will be important to enhance the trust and confidence between the US and the EU. In addition, the European Commission and more specifically the DG Justice are working on revising standard contractual clauses.
Transatlantic crossings: the future of EU-US data flows

In the US, the US Department of commerce has issued a white paper specific on the issue of transferring data between the EU and the US. It explains that a case by case analysis needs to be undertaken but that part of the analysis concerns the nature of the data being transferred. Indeed, if the transferred data is not likely to be part of a national security letter request or under surveillance law in the US, the process for transferring data becomes much easier. On the other hand, if it is likely to be part of a national security letter request or under surveillance law in the US, the process is more time consuming. Through this white paper, the recommendation guidelines on the additional measures and safeguards through the standard contractual clauses have been extensively formalised and organisations can related to this white paper to learn about what needs to be done to transfer data from the EU to the US. One of the recommendations of this paper would be for the European Data Protection Board to produce a similar paper on its own expectations so companies could merge those and decide if they are able to work under those current terms, this existing legislation and these existing policies.

Even if the standard contractual clauses and other mechanisms as anonymisation and encryption techniques seem to be a solution to the privacy issues related to the transfer of data between the EU and the US, there is a crucial need for a US Federal privacy law and the perspective of building such a law seems to be very optimistic since more progress has been made to this regards in the last 2 years than in the last 20 years. The US is not going to solve the national security implications of the invalidation of the Privacy Shield, but it will get them closer to a value of privacy in a broader term. Indeed, current discussions in the US concern a higher baseline for privacy and data. Now, these discussions are also impacted by the new US President election which has been resulting in a new administration. Data privacy is still a high priority but as the administration is newly formed, the discussions and activities to this regard will probably take more time which does not enable to provide a specific timeline for a new agreement succeeding the Privacy Shield.

5 [https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF](https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF)
Annex 2 - Artificial Intelligence – Comparison of US’s and EU’s approaches
Artificial Intelligence – Comparison of US’s and EU’s regulatory approaches
Think NEXUS, an EC-funded project, aims at reinforcing EU-US collaboration on NGI-related topics in three focus areas: Science and Technology, Innovation and Entrepreneurship and Policy. The aim is to boost strategic research, industrial partnerships and policy compliances in order to gain socio-economic benefits in both the EU and US regions. In the framework of this project, we are regularly publishing several short articles aiming at comparing the US and the EU approaches in different topics of NGI. The present document is focusing on Artificial Intelligence.
THI __

___ NK

NEX __

___ US
The European Commission’s approach towards AI

The European Commission has made Artificial Intelligence (AI) one of its priority. Its goal is to “boost EU’s research and industrial capacity and to put AI at the service of European citizens and economy”¹ by dealing with technological, ethical, legal and socio-economic aspects of AI in order to stay at the forefront of this technological revolution, to ensure competitiveness and to shape the conditions for its development and use.

The European Commission’s approach towards AI is based on three pillars (according to the EC communication in April 2018)²:

**Being ahead of technological developments and encouraging uptake by the public and private sectors**

The European Commission has increased its annual investments in AI by 70% under the Horizon 2020 programme and will reach 1.5 billion € for the period 2018-2020. For the next long-term EU budget (2021-2027) the EU has proposed to invest at least €7 billion from Horizon Europe and the Digital Europe Programme in AI³. These investments will be dedicated to the following activities:

- Connect and support AI research centres
- Support the development of an “AI-on-demand platform” which aims at providing AI resources for all users
- Strengthen the development of AI applications

This investment represents only one part of the investment the European Commission hopes to reach. As the countries in Europe and the private sector seems to understand the high investment AI needs for the next decade, the European Commission is hoping to reach more than 20 billion € per year of investment over the next decade.

**Ensure an appropriate ethical and legal framework**

The European Commission aims at handling all the ethical and legal questions that will come through AI and its applications. The GDPR is one of the major first step on the subject but a step forward needs to be done in order to ensure legal clarity in AI-based applications. The following papers have been considered by the European Commission in its reflections:

The Report on liability for Artificial Intelligence and other emerging technologies by the Expert Group on Liability and new technologies

Ethics Guidelines for trustworthy Artificial Intelligence prepared by the High-level group on Artificial Intelligence

The Staff working document for emerging digital technologies

The EU guidelines on ethics in artificial intelligence: Context and implementation by the European Parliament

Prepare for socio-economic changes brought about by AI

To support the efforts of the European countries responsible for labour and education policies, the European Commission will:

- Support business-education partnerships to attract and keep the AI talents in Europe
- Create trainings for professionals
- Upstream preparation regarding the possible changes in the labour market and skills
- Strengthen the digital skills and competences in science, technology, engineering, mathematics, entrepreneurship and creativity
- Support the Member States with the modernisation of their education and training systems

The European Commission has also highlighted that the development of AI can only be achieved if the citizens trust in AI and trust can be earned through the respect of ethical standards reflecting the European values.

Moreover, the European Commission has released a “timeline for Europe’s AI strategy” as shown in the following figure. All the European Commission’s actions around AI should follow this timeline.

![A TIMELINE FOR EUROPE’S AI STRATEGY](image)

Figure 1: Timeline for Europe’s AI strategy
The US approach towards AI

The US was the first country to have implemented a comprehensive AI research and development strategic plan in May 2016 under the administration of Barack Obama. The plan established a set of objectives for federally funded AI research both occurring within the government and outside such as in academia:

- Make long-term investments in AI research
- Develop effective methods for human-AI collaboration
- Understand and address the ethical, legal, and societal implications of AI
- Ensure the safety and security of AI systems
- Develop shared public datasets and environments for AI training and testing
- Measure and evaluate AI technologies through standards and benchmarks
- Better understand the national AI research and development workforce needs.

The goal for the US government was to focus its resources on the types of AI research that the private sector will be less likely to support (e.g. public health, urban systems, environment sustainability, etc.) as the private sector is investing heavily in AI at an increasing pace.

Nevertheless, the US has been less active institutionally regarding questions of ethics, governance and regulation compared to developments in the EU, until in February 2019 when the US president Donald Trump issued an Executive Order launching the American AI initiative. It explains the importance of the role of the Federal Government with regards to the facilitation of AI R&D and is promoting trust, training people for changing workforce, and protecting national interest, security and values – similar to the European approach. Moreover, it emphasizes the country’s leadership in AI but highlights the necessity to enhance collaboration with foreign partners and allies.

The American AI Initiative is based on five pillars:

- Promote sustained AI R&D investment
- Unleash Federal AI resources
- Remove barriers to AI innovation
- Empower the American worker with AI-focused education and training opportunities
- Promote an international environment that is supportive of American AI innovation and its responsible use.

The goal of this American AI Initiative is that all executive departments and agencies that
are developing or deploying AI, providing educational grants, or regulating or guiding AI are adhering those five pillars.

Conclusions - Comparison of the different approaches

The European commission is focused on the rules that will frame the AI development. It provides clear ethical principles and a checklist to be used when developing AI systems. These principles will be tested by companies and other stakeholders in a pilot project to start in the summer of 2019. While in the US with the election of Donald Trump it took another path: “The US was on the path to really forward-thinking AI national policy under the Obama administration. Now, we’re not”, says Mark Latonero, a fellow at the USC Annenberg Center on Communication Leadership & Policy⁶.

The main difference between the United States (US) and the European Union (EU) in the matter of AI are illustrated in the following figure⁷.

![Figure 2: EU/US comparison on AI](https://www.ft.com/content/025315e8-7e4d-11e9-81d2-f7785092ab560)

Nevertheless, some similarities can be observed as the first set of intergovernmental policy guidelines on Artificial Intelligence initiated by the OECD was adopted in May 2019 and aims to

---

⁶ [https://www.ft.com/content/4fd088a4-021b-11e9-bf0f-53b8511af673](https://www.ft.com/content/4fd088a4-021b-11e9-bf0f-53b8511af673)

⁷ [https://www.ft.com/content/025315e8-7e4d-11e9-81d2-f7785092ab560](https://www.ft.com/content/025315e8-7e4d-11e9-81d2-f7785092ab560)
ensure AI systems are designed to be robust, safe, faire and trustworthy in 42 countries. Among these countries are the 36 OECD member countries (including most of the countries in the European Union and the US) and 6 other countries including Argentina, Brazil, Colombia, Costa Rica, Peru and Romania. These principles state that:

- AI should benefit people and the planet by driving inclusive growth, sustainable development and well-being
- AI systems should be designed in a way that respects the rule of law, human rights, democratic values and diversity, and they should include appropriate safeguards to ensure a fair and just society
- There should be transparency and responsible disclosure around AI systems to ensure that people understand when they are engaging with them and can challenge outcomes
- AI systems must function in a robust, secure and safe way throughout their lifetimes, and potential risks should be continually assessed and managed
- Organisations and individuals developing, deploying or operating AI systems should be held accountable for their proper functioning in line with the above principles

Consistent with those principles the OECD provided five recommendations to governments:

- Facilitate public and private investment in research & development to spur innovation in trustworthy AI
- Foster accessible AI ecosystems with digital infrastructure and technologies and mechanisms to share data and knowledge
- Ensure a policy environment that will open the way to deployment of trustworthy AI systems
- Empower people with the skills for AI and support workers for a fair transition
- Co-operate across borders and sectors to progress on responsible stewardship of trustworthy AI.

9 https://www.oecd.org/going-digital/ai/principles/
Annex 3 - Digital Services Act (EU) vs COPRA (US)
Digital Services Act (EU) vs COPRA (US)
The latest regulation initiatives: Digital services act (EU) vs COPRA (US)

Think NEXUS, an EC-funded project, aims at reinforcing EU-US collaboration on NGI-related topics in three focus areas: Science and Technology, Innovation and Entrepreneurship and Policy. The aim is to boost strategic research, industrial partnerships and policy compliances in order to gain socio-economic benefits in both the EU and US regions.

In the framework of this project, we are regularly publishing several short articles aiming at comparing the US and the EU approaches in different topics of NGI. The present document is focusing on the latest initiatives regarding the regulation of digital services in the single market in the European Union (EU) and the United States (US).

In the European Union: The Digital services act

In its Agenda for Europe, Ursula von der Leyen has given its political guidelines for the next European Commission 2019-2024. Among the six political goals the president-elect wants for Europe over the next five years is the ambition to create “a Europe fit for the digital age”.

In the same text, she specifies “I want Europe to strive for more by grasping the opportunities from the digital age within safe and ethical boundaries”.

The objectives of the president-elect on this subject are:

- To develop joint standards for the 5G networks
- To achieve technological sovereignty in some critical technology areas
- To invest in blockchain, high-performance computing, quantum computing, algorithms and tools to allow data sharing and to define standards for these technologies
- To preserve high privacy, security, safety and ethical standards
- To put forward legislation for a coordinated European approach on the human and ethical implications of Artificial Intelligence
- To upgrade the liability and safety rules for digital platforms, services and products through a new Digital Services Act
- To update the Digital Education Action Plan.

In June 2019, the “Digital Service Act note” of the DG Connect was released which is used as basis for discussions at the DSM Steering Group. The objective is to build a new act aiming at updating the regulatory framework for all digital services in the single market, encompass a REFIT of the E-Commerce Directive of 2000

The latest regulation initiatives: Digital services act (EU) vs COPRA (US)

and to set new rules for platforms. The E-Commerce Directive of 2000 is based on the “no-regulation-for regulation’s sake” principle and on the laissez faire approach which consist in regulating only where there is a specific need for it. This is why the Directive lasted long - it is flexible and revising it would generate difficulties in application. Nevertheless, in 2015, it became clear through the publication of the Digital Single Market Strategy that this Directive needed to be revised. Indeed, the European Commission indicated that “It is not always easy to define the limits on what intermediaries can do with the content that they transmit, store or host before losing the possibility to benefit from the exemptions from liability set out in the e-Commerce Directive”², highlighting that the Directive has its limits with regards to the responsibility of the publication of illegal content.

In its “Digital Service Act note”, the DG Connect identified five issues that need to be handled with:

- Divergent rules for online services across the Digital Single Market
- Outdated rules and significant regulatory gaps for today’s digital services
- Insufficient incentives to tackle online harms and protect legal content
- Ineffective public oversight
- High entry barriers for innovative services.

Moreover, it highlighted the possible objectives the initiative could have:

- To give providers of digital services a clear, uniform, and up-to-date innovation friendly regulatory framework in the Single Market
- To protect, enable, and empower users when accessing digital services
- To ensure the necessary cooperation among Member States, together with the adequate and appropriate oversight of providers of digital services in the EU.

The scope of this initiative will cover “all digital services and in particular platforms”³. The following updates to E-Commerce Directive are suggested by the DG Connect⁴:

- To keep the home country control but to extend its scope:
  - It should include consumer protection, commercial communications and contract laws across the European Union but also services established in third countries. Moreover, the establishment in the European Union should be simplified through clearer rules.
  - There are some grey areas such as ISPs, cloud services, content delivery networks, domain name services, social media services, search engines, collaborative economy platforms, online

---

The latest regulation initiatives: Digital services act (EU) vs COPRA (US)

advertising services and digital services built on electronic contracts and distributed ledgers that should be regulated. Moreover, “category of services on the basis of a large or significant market status, complementing the competition threshold of dominance” should be defined.

- To update the liability provisions of the E-Commerce Directive:
  o The “general principle of a harmonised graduated and conditional exemption […] needs to be updated and reinforced to reflect the nature of services in use today”.
  o New rules or clarifications of the principles to “collaborative economy services, cloud services, content delivery networks, domain name services, etc.” should be adopted.
  o The notions of active and passive hosts should be adapted to today’s services and be replaced by “editorial functions, actual knowledge and the degree of control”.

- To maintain the prohibition of general monitoring obligations as a foundational cornerstone of Internet regulation while considering “specific provisions governing algorithms for automated filtering technologies […] to provide the necessary transparency and accountability of automated content moderation systems”.

- To uniform rules for the removal of illegal or harmful content based on the Recommendation on illegal content: notice and action rules tailored to the types of services are suggested as well as binding transparency obligations and transparency “for algorithmic recommendation systems of public relevance”.

- To add specific obligations for cross border online advertising services.

- To facilitate data transfers and improve service interoperability when feasible accompanied by appropriate standardisation initiatives, and co-regulatory approaches.

- To include in the general framework provisions, options which “would allow controlled regulatory experimentation” facilitating the introduction of new services.

- To create a new regulatory structure that would “ensure oversight and enforcement of the rules, in particular for cross-border situations, but also partnerships and guidance for emerging issues”.
The latest regulation initiatives: Digital services act (EU) vs COPRA (US)

In the United States: The Consumer Online Privacy Rights Act ‘COPRA’

In November 2019, Senate Democrats led by the Senator Maria Cantwell of the Washington State introduced a bill that aims to provide federal privacy guarantees for American’s personal data. This bill is called the Consumer Online Privacy Rights Act (COPRA).5

“In the growing online world, consumers deserve two things: privacy rights and a strong law to enforce them.”, according to Senator Maria Cantwell6.

COPRA gives Americans control over their personal data, prohibits companies from using consumers’ data to harm or deceive them, establishes strict standards for the collection, use, sharing, and protection of consumer data, protects civil rights and penalizes companies that fail to meet data protection standards. Moreover, the Senate recognized the need to do more to protect children and young people’s online privacy and therefore, the bill tackles also teen privacy with new safeguards.

One of the main aspects of this bill, is that internet users will be able to pursue companies which are not respecting their will in terms of data protection. Indeed, former Director of the federal Trade Commission’s Bureau of Consumer Protection and Georgetown Law Professor, David Vladeck said: “The bill not only codifies privacy as a right – a measure long overdue – but it also recognizes that ‘rights’ that are unenforceable are empty gestures. For that reason, the bill not only restores control of personal information to consumers, but equally important, the bill gives consumers and the Federal Trade Commission real tools to hold companies accountable when they collect information without permission, when they fail to reasonably safeguard consumers’ information, or when they misuse that information.”.

The principal elements of this bill are as following8:

- Data privacy rights:
  - The consumers have the right to access, delete and correct inaccuracies in their data held by an entity.
  - The entities have the right to transfer data only upon request of the consumer. It cannot be transferred if the consumer does not want it to and has not consented to it.

---

8 https://www.cantwell.senate.gov/imo/media/doc/COPRA%20One-Pager.pdf
The latest regulation initiatives: Digital services act (EU) vs COPRA (US)

- The entities should not process or transfer covered data beyond what is reasonably necessary.
- The entities shall establish, implement, and maintain reasonable data security practices to protect the confidentiality, integrity, and accessibility of data.
- The processing or transferring of data on the basis of the characteristics of an individual for certain purposes or in a manner that unlawfully segregates or discriminates against is prohibited. Entities using an algorithmic decision-making have to annually conduct an impact assessment which would describe, evaluate and assess the algorithmic system.

- Oversight and responsibility:
  - Executives of large data holders shall annually certify to the Federal Trade Commission (FTC) that the entity maintains adequate internal compliance controls and reporting structures to ensure that such certifying officers are involved in and are responsible for decisions that impact the entity’s compliance with COPRA.
  - An employee who is designated by a covered entity as a privacy officer or a data security officer shall be responsible for implementing a comprehensive written data privacy and security program, for annually conducting privacy and data security risk assessments, data hygiene and other quality control practices and for facilitating the covered entity’s compliance with COPRA.
  - Whistle-blowers (people that have noticed an entity’s data abuse and that makes it public) are protected.
  - Covered entities cannot directly or indirectly discharge, demote, suspend, threaten, harass or in any other manner discriminate against a covered individual of the covered entity.

- Enforcement and pre-emption:
  - The FTC, state Attorneys General and individuals can take any entity into court if it violated COPRA.
  - A new bureau will be established within the FTC and a new Data Privacy and Security Relief Fund will be created in which the FTC and state Attorneys General would deposit recovered funds to be used to redress, compensate affected individuals, and other privacy initiatives.
  - The States’ law on consumer protection shall remain as long as there is no conflict of interest between those laws and COPRA. In any case, COPRA supersedes any State law to the extent such law directly conflicts with COPRA’s provisions\(^\text{10}\).

The latest regulation initiatives: Digital services act (EU) vs COPRA (US)

Comparison between the EU initiatives and the US initiatives

The European Union has a clear advance on the United States in terms of consumer privacy protection. Indeed, the General Data Protection Regulation (GDPR) was already written in 2012 and after four years of legislative negotiations, has been enacted in 2016. It is only seven years later, in 2019, that the United States initiated a similar law, the Consumer Online Privacy Rights Act (COPRA).

The United States’ privacy scheme has been in a race to catch up to the expansive individual consumer rights granted to individuals in the European Union and to provide oversight on companies who collect and process personal information. Many States in the US have been drafting their own privacy laws which are seen as a response to the GDPR, as for example the California Consumer Privacy Act (CCPA), effective on the 1st of January 2020. The COPRA initiative is aiming at establishing a solid and unified legislative ground for the whole country on consumer privacy protection.

Steve Durbin, managing director of the Information Security Forum, a London-based authority on cyber, information security and risk management, commented the COPRA bill by saying: “In much the same way as GDPR began a far reaching debate over the rights of the individual, so too is this piece of legislation continuing a similar conversation across America. What is clear is that privacy is becoming more of an issue in the United States and there is a very real need for a Federal law to avoid States introducing their own variations and interpretations on privacy which adds a further compliance burden to already overstretched businesses looking to understand and comply with their obligations across the various regions in which they are transacting business.”

The European Union is even going a step further and is preparing a new regulation: The Digital Service Act. This Act will provide more detailed consumer data protection rules in the scope of digital services and platforms.