White Paper

Digital Services Act (EU) vs COPRA (US)

July 2021

Authors:

Think NEXUS Policy Expert Group

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 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*"[1].

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 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.

1 https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf (page 13)

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 Connect[4] :

- 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 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:
  - 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".
  - New rules or clarifications of the principles to "collaborative economy services, cloud services, content delivery networks, domain name services, etc." should be adopted.

2 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0192&from=EN (page 12)
3 https://cdn.netzpolitik.org/wp-upload/2019/07/Digital-Services-Act-note-DG-Connect-June-2019.pdf
4 https://cdn.netzpolitik.org/wp-upload/2019/07/Digital-Services-Act-note-DG-Connect-June-2019.pdf

  - 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".

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 Cantwell[6].

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.***

5 https://www.fastcompany.com/90436605/americas-answer-to-gdpr-heres-what-to-know-about-the-consumer-online-privacy-rights-act
6 https://gdpr.report/news/2019/11/29/privacy-u-s-senators-introduce-the-consumer-online-privacy-act/

***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."*[7].**

The principal elements of this bill are as following[8 9]:

- 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.
  - 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.

7 https://www.cantwell.senate.gov/news/press-releases/cantwell-senate-democrats-unveil-strong-online-privacy-rights
8 https://www.cantwell.senate.gov/imo/media/doc/COPRA%20One-Pager.pdf
9 https://www.dataguidance.com/wp-content/uploads/2019/11/the_proposed_consumer_privacy_online_act-_what_you_need_to_know_final-1.pdf

- 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[10].

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[11]. 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.

10 https://www.dataguidance.com/wp-content/uploads/2019/11/the_proposed_consumer_privacy_online_act-_what_you_need_to_know_ final-1.pdf
11 https://www.nixonpeabody.com/en/ideas/articles/2019/11/27/consumer-online-privacy-rights-act
12 https://gdpr.report/news/2019/11/29/privacy-u-s-senators-introduce-the-consumer-online-privacy-act/

NGI THINK NEXUS

thinknexus.ngi.eu @ThinkNEXUS_NGI

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