Purpose of the visit:

- [Facebook's position:]

Facebook's oversight board

- Facebook had announced in November 2018 a new Oversight board, along with a commitment to more proactively detecting illegal content (or harmful content, as defined in Facebook's terms of service), automatically identifying ‘borderline’ content such as click bait and misinformation and demoting it, allow some enhanced level of enhanced control of the user over the content they see, address algorithmic bias in the technologies used by Facebook in content moderation, building an appeals process and enhancing transparency through public reporting on actions taken by the platform and partnerships with policy-makers and researchers.

- Facebook has just announced the Director of its Oversight Board Trust and LLC for Article 19. The Board is designed to oversee complaints made by users whose content was removed by Facebook or Instagram (within 15 days), after other internal complaint mechanisms are exhausted, and to issue opinions within 90 days, which Facebook commits to follow.

Broader content policy

- Facebook also made a plea for ‘right regulation’, clarifying that ‘services must respect local content and laws’, but that legislation needs to clarify certain parameters: clear definitions of content, rates of acceptable content, accepted lines between free expression and safety, and obligations for transparency reporting on content detected. He declared his hope to work with legislators, starting with France, on regulation, and other governments ‘including hopefully with the European Commission to create a framework for Europe in the next couple of years’.

- Facebook is part of most of the voluntary cooperation mechanisms set up by the Commission to tackle illegal and harmful content, including the EU Internet Forum

---

against terrorist content, the Code of Conduct against hate speech online, or the Code of Practice against Disinformation.

‘Vision for internet regulation’

- Facebook’s met VP Jourova and Dombrivskis in December last year. delivered a speech in January this year in Rome, setting Facebook’s main lines for ‘a vision’ of the Internet. made a plea for responsibilities of platforms and visionary policies in Europe and for regulation at EU level (which Facebook is ‘keen to co-operate’ on). specifically mentioned: “GDPR was the first serious attempt anywhere to create a set of principles and rules around private data in a way that is practical in the digital age. And those principles are at the heart of a vision for the internet that I believe is shared among all open societies: that it is accessible to all: transparent and accountable: that you own your own data: and that competition and innovation should be encouraged.

Geopolitical context

- positioned the policy agenda and the values carried out by the ‘internet of the West’ against the Chinese tech giants.

- At the same time, the discussions in the US on the broader liability exemption set in Section 230 of the Communication Decency Act (CDA) is increasingly brought up in the context of the Presidential campaigns, with leadership in the Democrat Party challenging the legal status quo. In trade discussions, however, the US makes a strong plea for the CDA model of the liability exemption (which is significantly broader than the European conditional liability set in the E-Commerce Directive).

The Commission’s position

- The Digital Services Act should ensure that platforms act responsibly in protecting the safety and the freedom of expression of European citizens: by clarifying the responsibilities of online platforms, and making sure that they are appropriately supervised by authorities.

- The Act will “reinforce the single market for digital services and help provide smaller businesses with the legal clarity and level playing field they need”.

- The Commission is also reflecting on rules to ensure contestability of the markets around online platforms: this is not as much about ‘breaking up’ platforms, but providing for the robust set of rules that large platforms need to follow when they reach a certain impact, and the mechanisms which allow for effective remedies when harm appears.

- Concerning Facebook’s oversight body: take note of the effort to provide independent judgement and appeals over content removals. We appreciate that the project is at its beginnings, and note that appropriate expertise and capacity will be key in the development. Also note that the existence of an independent board cannot supersede obligations related to the illegal nature of certain types of content.

Main messages

-
Background

Digital Services Act

- The Digital Services Act was announced by the President in her political guidelines and the Commission Work Programme for 2020 committed to a proposal by the end of the year.

- Services are currently working on the scoping of the issues to be covered in the legal proposal(s). The current working hypothesis is that this could include a package of measures, including: (1) rules on the responsibilities of digital services, and online platforms in particular, drawing on or revising the E-Commerce Directive of 2020, with clear procedural obligations with regards to goods sold or content disseminated through their intermediation, and establishing clear supervisory capabilities at national and possibly EU level and (2) an instrument to address the contestability of platform markets and establish rules for ‘mega-platforms’ to act responsibly on the market. The first instrument could also address emerging issues around the transparency and accountability of certain algorithmic processes (e.g. recommender systems, content moderation tools), and transparency in online advertising.

- A public consultation will be likely launched mid-March this year, and a/several legal instrument(s) could be released in December 2020.

- The legal framework for digital services is currently set by the e-Commerce Directive which includes the legal incentives for platforms to take measures against the dissemination of illegal goods or content through their services: the liability regime for ‘hosting services’ obliges them to expeditiously remove such content when they become aware of its presence. To avoid undue surveillance and to protect freedom of expression online, the Directive also prohibits Member States from imposing general monitoring obligations on service providers. In the past mandate, the Commission issued guidance on the specific responsibilities it expected from platforms (Recommendation of 2018) including a functioning notification system for users to report content, appropriate capacity for assessing notices, and due process to inform users when their content is removed and allow them to contest it, etc. The Commission also legislated to tackle specific types of content, such as terrorist propaganda, copyrighted content, or audiovisual content.

Code of Practice on disinformation – Next steps:

- The Commission published the self-assessments together with its own, factual analysis on 29 October 2019. We are now carrying out its comprehensive assessment of the effectiveness of the Code of Practice.

- In addition to the self-assessments by the signatories, we will take into account:
  - Input from the European Regulators Group for Audiovisual Media Services (ERGA),
  - An assessment from an independent consultant engaged by the Commission.
On this basis, the Commission will present its comprehensive assessment in spring 2020. Should the results under the Code prove unsatisfactory, we stand ready to propose further measures, including of a regulatory nature.

Facebook Partnership with Social Science One

In April 2018, Social Science One and Facebook launched a project on “the effects of social media on democracy and elections,” offering researchers privacy-preserving access to Facebook’s data. This project includes a new type of peer pre-review feedback service designed to speed scientific progress and shorten time-to-publication.

The partnership should enable academics to analyse the increasingly rich troves of information amassed by private industry in responsible and socially beneficial ways. It ensures the public maintains privacy while gaining societal value from scholarly research. And it enables firms to enlist the scientific community to improve their business and produce social good, while protecting their competitive positions. Social Science One is being incubated at Harvard’s Institute for Quantitative Social Science.

However, it is alleged that Facebook refuses to give significant access to data to researchers based on privacy concerns. In particular, Facebook has still not provided academics under the Social Science One with adequate data access. The European Advisory Committee Social Science One has recently repeated its concerns that digital platforms have made independent scientific research into potentially consequential phenomena such as online disinformation, polarization, and echo chambers virtually impossible by restricting scholars’ access to the platforms’ application programming interfaces (APIs).

European Digital Media Observatory:

The Commission will deploy, with an investment of EUR 2.5 million financed by the Connecting Europe facility 2019 programme, the necessary digital infrastructure for the creation of the European Digital Media Observatory (EDMO). A tender evaluation is currently ongoing to select the contractor, which will build digital infrastructure and will establish the governance of EDMO. During 2020, additional EUR 9 million will support the creation and activities of national/regional hubs activities and their interconnection to the central infrastructure.

The main objective of EDMO will be to create and support the work of a multidisciplinary community of fact-checkers, academic researchers and relevant stakeholders actively engaged in tackling the phenomenon of disinformation. To do so, EDMO will provide tools and services to improve the detection of and analysis of disinformation campaigns and malicious behaviours and increase societal awareness. Interconnected national/regional research hubs will provide the necessary knowledge of local information environment to capillary monitor information spaces and build impactful responses. Furthermore, EDMO will also support national and EU public authorities in the monitoring of the policies put in place by the online platforms (e.g. signatories of the Code of Practice) to tackle disinformation.

In order to fulfil the request from the academic community and carry-out a meaningful monitoring, EDMO will seek to design, together with relevant online platforms, a framework enabling a secure access to platforms’ data for organisations, upholding the necessary ethical and professional standards, which pursue research dedicated to better understand the disinformation phenomenon.

3 Signatories of the Code of Practice on disinformation have committed to “support good faith independent efforts to track disinformation and understand its impact, including the independent network of fact-checkers facilitated by the European Commission upon its establishment. This will include sharing privacy protected datasets, undertaking joint research, or otherwise partnering with academics and civil society organizations if relevant and possible.”

4 Access to online platform data must be compliant with national and European laws on privacy and data protection.
Facebook’s position

- Facebook’s approach to giving access to the ad library has been criticised by researchers, not least those joining the Mozilla Foundation’s efforts to define the specific requirements for an effective API5 for sharing data for research purposes. As opposed to static information published by the platform, researchers express a set of requirements on structured data access which would allow for meaningful supervision and analysis.

- Facebook recently announced updates to its Ad Library to increase the level of transparency it provides for its users and giving them more control over the ads they see. This includes in particular further information on the targeted audience, better Ad Library search and filtering, control over Custom Audiences from a list and the option for users to see fewer political ads.

- At the same time, as opposed to Twitter, it announced that the platform would not to limit targeting of political ads, and reiterated its calls for regulation across the industry. In preparatory discussions, Facebook representatives clarified that Facebook would welcome ‘clear rules on who should be allowed to advertise where and when’.

Commission’s position

- The President announced in her political guidelines a European Democracy Action plan including, amongst other, further measures for transparency of political ads.

- Under the Code of Practice on Disinformation, the signatories have taken some measures to further transparency of political advertising.

Main messages

---

5 https://blog.mozilla.org/blog/2019/04/29/facebook-ad-archive-api-is-inadequate/
Data sharing and portability

Scene setter:

- The Commission is preparing a broad strategy on data to be adopted on 19 February 2020. The strategy will set out the actions the Commission plans to undertake during the course of the mandate.

- Issues related to platforms’ data access and data sharing practices are being analysed in the context of the Digital Services Act package, both in what concerns to the economic importance and key role in the platform’s business model and economic power, and potential reporting obligations to authorities and ensuring accountability of online platforms.

- The General Data Protection Regulation already establishes a right for data subjects to port their data. Facebook offers such a functionality to its users.

Facebook’s main position

- Data portability features among the top headers of Facebook’s possible future strategy. The company has also portrayed itself as ‘entrusted entity’ for the individuals who share their data on the social media.

- In March 2019, called for laws that guarantee portability.

- As part of the broader Data Transfer Protocol (established by Facebook, Twitter, Microsoft and Apple) Facebook released a new photo transfer product allowing users to ‘move’ Facebook photos into Google products.

Commission’s position:

- For the specific point of platform-held data, the Commission has set up transparency rules on the data sharing and access policies of platforms, in particular with regards to their business users, as well as to their data sharing practices with third parties – this is regulated under the Platform-to-Business Regulation which will enter into force in July this year.

- The Commission continues to analyse the economic impact of platforms’ data collection and data sharing practices as part of the Digital Services Act preliminary fact finding, including a reflection on data sharing and access conditions, possible role of data portability and models of interoperability in particular for those very large players. The reflection also includes concerns around reporting obligations to competent authorities tasked to supervise online platforms or in the context of e.g. collaborative economy, where platforms are best placed to cooperate with authorities in the supervision of the underlying service (e.g. car sharing, accommodation rentals).

- More broadly, in order to support European citizens and companies to benefit fully from the emerging data economy, the European Commission plans to further promote a favourable policy and legislative environment with respect to the availability and exploitation of data. This is a key factor to increase and defend competitiveness of EU industries at large.

- In full compliance with the European data protection legislation in force, the EC intends to further empower citizens across Europe to control and port their data and choose the service providers that can offer them the most beneficial services that fit their needs best.

- The European Commission is now preparing a new strategy on data in order to further define governance of this important resource as an enabler of multiple technological innovations.
On the Data Transfer Protocol: while the initiative shows positive developments in establishing technical interoperability for porting data and provides for open source protocols, it only involves a very small number of very large market players in the specific applications developed. This would likely reinforce user lock-in for the well-circumscribed circle of market players. Some criticism in this direction is emerging. Independent efforts for interoperability standards are important to counterbalance this trend.

Main messages

Background

Data economy – Past and ongoing actions

In the last few years, the Commission initiated several horizontal measures relating to data. The GDPR reinforced the protection of personal data. The Regulation on the free flow of non-personal data tackles unjustified data localisation restrictions. The new Directive on open data facilitates the re-use of public sector data. The Regulation on ‘Platform to Business’ contains transparency obligations of large digital platforms with regard to their data sharing policies towards their business users and third parties.

Under the Data Economy strategy, the Commission has worked along several strands in order to make at least some data flow more easily in the economy. The 2018 Communication ‘Towards a common European data space’ sought to address re-usability of data from different origin in a holistic way: on public sector information with the Open Data Directive, on data stemming from scientific research with the review of the Recommendation on access to Scientific Information, and on Business to Business and Business to Government data sharing principles with guidelines.

The Commission also created a Support Centre for Data Sharing. Through a dedicated website, it develops and disseminates tools and technical expertise and provides practical support for data sharing. It was launched in October 2019, and the first reactions from industry are very positive.

The Commission set up an Expert Group on Business to Government data sharing to bring the policy forward. Its report will be published in February 2020.
On **common European data spaces**: One of the elements of the “Data for AI” specific objective in the **Digital Europe programme** is the development of common European data spaces, the aim of which is precisely to ensure data access in specific sectors. Through policy measures and with the support of the Digital Europe programme and the Connecting Europe Facility 2, these common European data spaces should ensure enhanced access to public and privately held data, via industrial and personal platforms and governance measures and agreed frameworks for the organisation of the data sharing. Support for measures giving individuals control over their data is also foreseen.

**Data strategy (to be launched on February 19th, 2019)**

This data strategy for Europe serves to realise the vision for a common European data space and tackles the problems identified through policy measures and funding. The actions are based on four pillars:

- **Regulation & rules**: Cross-sectoral measures for data access and use;
- **Enablers**: Investments in data and strengthening Europe’s standards, tools and infrastructures for hosting, processing and using data;
- **Competences**: Investments in general data literacy, addressing lack of skilled labour, up/reskilling of our work forces as well as dedicated capacity building for SMEs.
- The roll-out of common European data spaces in crucial economic sectors.

**Data Transfer Project**

It is a collaborative effort between Facebook, Apple, Google, Microsoft, and Twitter to build a common way for people to transfer their data between online services. The mission of the project is to create an open source, service-to-service data portability platform so that all individuals across the web can easily move their data between online service providers whenever they want. The project does this by providing an open source library that any service can use to run and manage direct transfers on behalf of users.
Global dimension of data protection and GDPR

Main Messages

- 

- 

- 

- 

- 

Background

International Data flows and protection

As the Facebook - Cambridge Analytica scandal confirmed, the respect of data protection and privacy is becoming key to ensure good political and democratic governance. Privacy as an individual human right, a democratic imperative and an economic necessity (if you want a flourishing and sustainable digital economy, you need the consumer's trust in the way their data is collected and used).

If there is one positive thing coming out of this scandal, it is the global awareness about the importance of personal data protection that has been generated among ordinary citizens around the world who want to see their privacy protected and their data to be safe. Their questions are increasingly answered in a convergent way.

A growing number of countries around the world, including from the developing world/Africa, are adopting new privacy laws that tend to be based on common elements which they share with the GDPR: a comprehensive legislation that applies across industries and sectors (rather than sectorial rules), a core set of enforceable rights and enforcement by an independent supervisory authority.

This is a global trend. Today more than 120 countries have privacy laws in place. Many more are considering adopting new laws/modernizing their privacy legislation. For example, India, Thailand, Indonesia, Brazil, Argentina, Kenya, Tunisia, Morocco and Chile recently took initiatives to strengthen their data protection regime, following the path opened by Japan and Korea some time ago.

This growing convergence is also reflected in the unceasingly international membership of Council of Europe's Convention 108, the only multilateral data protection instrument (with already more than 51 countries, recent accessions include Mexico, Argentina, Senegal, Tunisia, Cabo Verde etc.). No longer "just" a European Instrument.
The EU encourages these developments, including by offering technical assistance to developing countries.
Ongoing debate on U.S. federal privacy legislation

Already during the legislative process and upon entry into application of the General Data Protection Regulation (GDPR) in May 2018, the U.S. authorities expressed strong criticism of the new rules, claiming they would penalise U.S. tech firms, burden companies with huge compliance costs and excessive financial sanctions, stifle innovation, etc. Most of these concerns were unsubstantiated and/or speculative, and over time, U.S. authorities adopted a lower profile, and a less negative tone. Moreover, recent calls for federal privacy legislation (including by industry, civil society and Members of Congress) have led to a more genuine, "neutral" interest in the EU's approach in this area.

In the past two years, there been an ongoing debate on possible federal privacy legislation in the U.S. While the upcoming election campaigns might have a negative impact, so far the real initiative on federal privacy rules seems to come from Congress (rather than from the US administration). A number of hearings on consumer privacy have taken place in the past months and several bills have been introduced, in both Houses. Some bills cover specific areas (such as the use of personal data by internet platforms or social media services), while others adopt a more comprehensive approach. Most bills focus on providing individuals with increased transparency and rights (e.g. possibility to opt-out/opt-in of processing, as well as access, correction and deletion). With respect to companies, most of the bills seem to focus on security requirements, while leaving (broad) flexibility to companies on how they collect, use and share data.

A recurring argument in favour of federal privacy rules is the need to avoid fragmentation of the regulatory framework through diverging State laws. Another aspect on which there seems to be broad agreement is the need to strengthen the powers and authority of the
Federal Trade Commission, the independent enforcement authority dealing with unfair, deceptive or fraudulent practices in the market, which in this capacity also enforces consumer privacy. Finally, a key concern shaping the debate is the possible negative effect of privacy legislation on SMEs and on innovation (including e.g. the development of new technologies and AI).

Privacy developments at State level

In parallel to the ongoing debate at federal level, and in the absence of concrete action by Congress, several States have in the meantime developed their own privacy legislation. The most well-known is the California Consumer Privacy Act (CCPA), which entered into effect on 1 January 2020. The scope of the Act is limited to a certain extent as it excludes personal information that is publicly available from its protections, and applies only to businesses that reach a certain threshold in terms of revenue or consumers. It provides consumers with a right to opt out, a right of information and access, a right of deletion and a right not to be discriminated against for exercising their privacy rights. However, these are subject to strict conditions and (broad) exemptions. Moreover, certain key aspects, such as storage limitation, purpose limitation, data minimisation and right of correction do not exist.

While the CCPA has now entered into force, it is not excluded that it might be amended further. For example, Alastair Mactaggart, the leading force behind the CCPA, has announced at the end of last year that he will propose a new draft in 2020 to further strengthen the CCPA (including by creating a Californian data protection authority with enforcement powers).

In addition, privacy laws have been adopted in Nevada and Maine, while privacy bills are currently being debated in parliament in a number of other States, including Illinois, Minnesota, New York and Washington. A common feature in these laws/proposals is that they provide for certain consumer rights (in particular the possibility to opt-out of certain processing, as well as rights of access, correction and deletion). At the same time, key principles and obligations (e.g. purpose limitation, proportionality, data retention, limitations on sharing/selling of data, etc.) are generally missing.