DENTONS

Grow | Protect | Operate | Finance

Sovereignty, extraterritoriality and protections for digital users in the global context

Errol Mendes, Jacqueline Palumbo,
Gabriela Loredana Alexandru

Regulating the Internet – Really?
Part IV: Balancing values and economic interests
Tuesday, January 23, 2024

EU Digital Services Act

Gabriela Alexandru, Head of Political, Press and Information Section

EU Delegation to Canada

The problem (s):

- **citizens exposed to increasing risks and harms online (spread of illegal activities, risks for their fundamental rights, other societal harms)**

- **the supervision of online platforms not sufficiently coordinated and effective**

- **fragmented regulation triggered risks for the functioning of the internal market**

The solution:

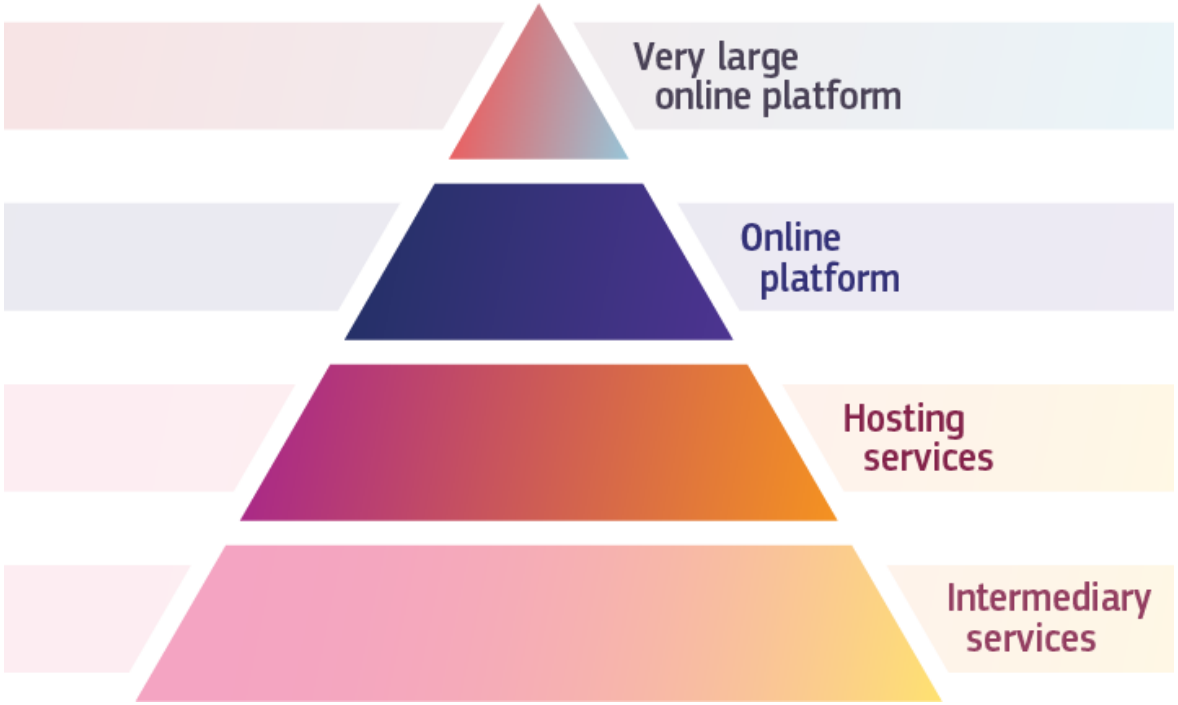
EU Digital Services Act: a single, uniform set of rules for the EU, to give users new protections and legal certainty to businesses

Objectives

- ✓ **To create a safer digital space in which the fundamental rights of all users of digital services are protected**

- ✓ **To establish a level playing field to foster innovation, growth, and competitiveness, both in the European Single Market and globally**

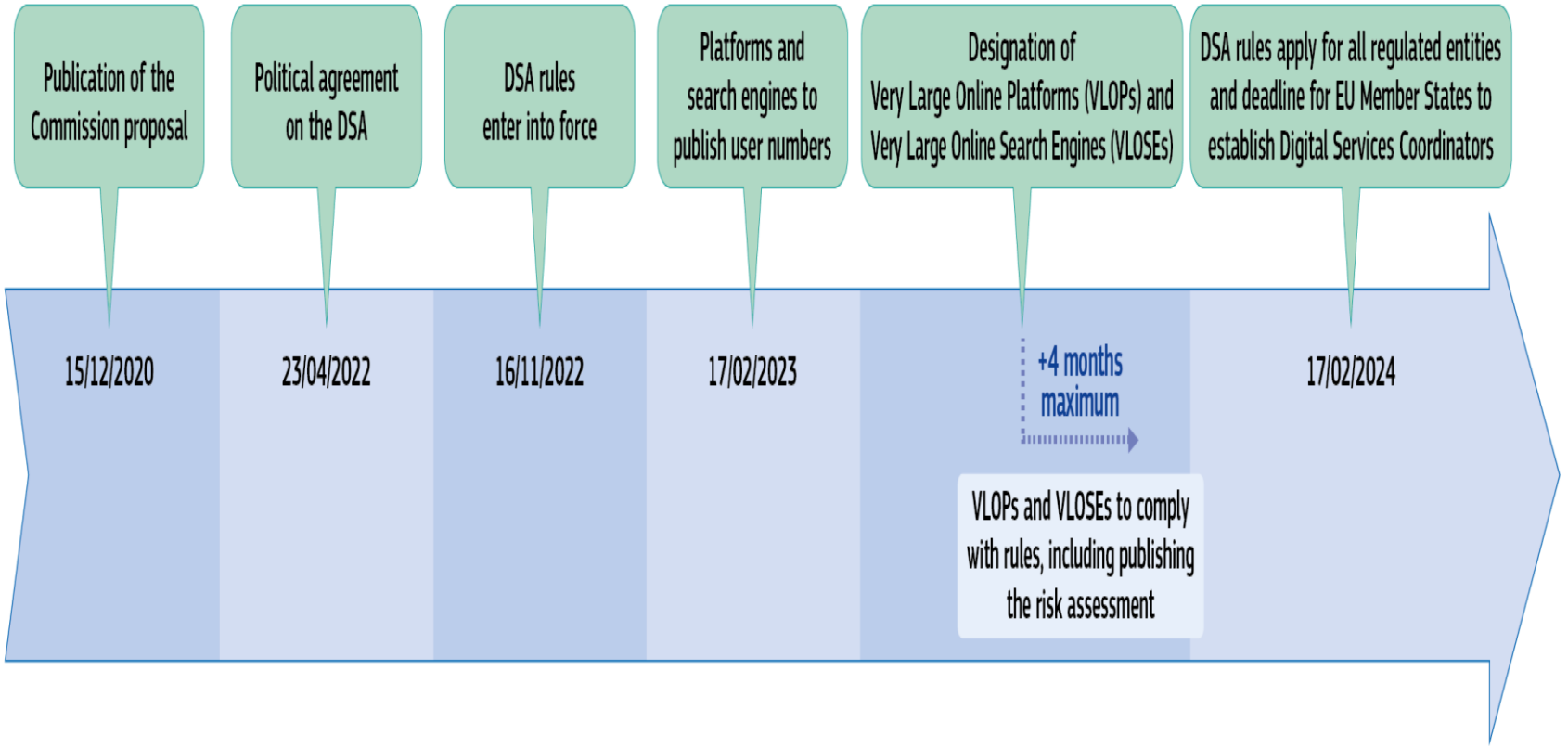
Which providers are covered?



Who has to do what?

	VERY LARGE PLATFORMS	ONLINE PLATFORMS	HOSTING SERVICES	ALL INTERMEDIARIES
Transparency reporting	●	●	●	●
T&Cs	●	●	●	●
Cooperation with national authorities	●	●	●	●
Points of contact & legal representatives	●	●	●	●
N&A	●	●	●	
Reporting criminal offences	●	●	●	
Complaint & redress mechanisms, OOC dispute settlement	●	●		
Trusted flaggers	●	●		
Prohibition of Dark Patterns	●	●		
Measures against abusive notices	●	●		
Special obligations for marketplaces (e.g. KYBC, random checks)	●	●		
Bans on targeted ads to children and based on special categories of personal data	●	●		
Accessibility	●	●		
Transparency of recommender systems	●	●		
Advertising transparency	●	●		
Risk management	●			
Independent audits	●			
User can opt out of profiling	●			
Data sharing with authorities & researchers	●			
Codes of conduct	●			
Crisis response cooperation	●			

Timeline for Digital Services Act



More information

https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package#:~:text=The%20DSA%20will%20be%20directly,users%20by%2017%20February%202023.

Accessing Digital Evidence to Fight Serious Crime: Modern Challenges Call for Modern Solutions

Panel 4: Sovereignty, Extraterritoriality & Protections for Digital Users in the Global Context

Regulating the Internet – Really? Part IV
ICJ & Dentons Canada LLP – Virtual Conference - January 23, 2024

Jacqueline Palumbo
Senior General Counsel & Head of Treaty Negotiations,
National Litigation Sector, International Assistance Group

- **The problem**… Law enforcement and prosecution authorities need more timely access to digital evidence in the possession or control of Communications Service Providers (CSPs) abroad – critical evidence needed to counter serious crimes (online child sexual exploitation, terrorism & cybercrime).

- **The solution**…. More effective measures of int'l cooperation – bilateral & multilateral – **BUT** must balance legitimate global crime fighting objectives with need to protect privacy interests and human rights.
  ****The solution hinges, in part, on forging strong partnerships with domestic and foreign CSPs***

Core principles of international cooperation in criminal matters

1. Respecting State sovereignty
2. Strong global partnerships are built on trust and good faith
3. Gathering evidence on foreign soil only with permission or by invitation
4. Reciprocity

Traditional int'l cooperation falls short on timely cross-border access to e-data

1. Mutual legal assistance (MLA) predates the rise of social media platforms and the ubiquitous use of mobile devices.
2. Ill-equipped to efficiently process immense volume of requests seeking access to cross-border electronic evidence.
3. Massive problem for MLA regime in the U.S. where most of the major CSPs are located.

Two examples of recent int'l efforts to respond to the growing problem

1. The **Second Additional Protocol** to the Council of Europe's Cybercrime Convention
2. Bilateral **Data Access Agreements** relating to the U.S. *Clarifying Lawful Overseas Use of Data Act* (CLOUD Act)

2nd Additional Protocol

- Council of Europe instrument – Supplements Cybercrime Convention (a.k.a. Budapest Convention)
- Most unique features:
  - Provisions on direct cooperation between practitioners and private entities in the jurisdiction of another Party to obtain:
    - **domain name registration info** (“WHOIS” article);
    - **subscriber information**
  - **Giving effect to foreign data production orders -** Expedited form of cooperation for the disclosure of subscriber information and (possibly) traffic data

Other features of 2nd Additional Protocol

- Comprehensive **Data Protection** and **Rule of Law** safeguards

- Obtaining Evidence in Emergency Cases (imminent risk to life/safety):
  - **Expedited disclosure of stored computer data** – leverages the 24/7 Network POC in the *Budapest Convention*
  - **Emergency Mutual Legal Assistance** – available for a wide range of assistance in urgent cases (not only e-evidence)

- **Videoconferencing** of experts and witnesses and **Joint Investigation Teams** – particularly useful where no other international agreement is in place for this type of assistance

Second Additional Protocol

Public consultations are under way

We welcome your views!

https://www.justice.gc.ca/eng/cj-jp/cyber/index.html

Data Access Agreement – *CLOUD Act*

- More direct access to e-information in the possession or control of a foreign CSP to fight serious crime.
- Requesting country transmits domestic order directly to the foreign CSP – eliminates some bureaucratic steps.
- The Parties agree to recognize the foreign legal process ….however, not legally enforceable extraterritorially.
- Can be used to obtain content-data, as well as subscriber information and transmission data.

Data Access Agreement – Safeguards

Examples of some of the protections:

- Serious crime scope.
- Targeting and Minimization requirements, e.g. orders must not target citizens, PRs or persons located on the territory of the country from which data is sought.
- Privacy interests are protected through strict data management procedures.
- Essential interests are protected, e.g. use limitations in death penalty cases, non-discrimination clause

The support of industry is key to success….

- Need to understand current challenges (legal, procedural, operational) faced by CSPs in responding to foreign requests for digital evidence
- Need to develop an implementation model that works for them
- Ongoing consultation with CSPs to ensure solid partnerships are forged

DENTONS

Grow | Protect | Operate | Finance

Thank you!