INTERNET LAW SESSION 2

PROF ANGELA DALY

18 OCTOBER 2019

PART I

ISSUES FOR INTERNET LAW: JURISDICTION AND PRIVATE INTERMEDIARIES

WHY JURISDICTION AND PRIVATE INTERMEDARIES

Two cross-cutting issues for substantive areas of Transnational Internet Law

On the one hand, the Internet is transnational and so inevitably crosses nation states' territorial boundaries – questions arise of which nation-state's laws apply to a particular issue

On the other hand, much of the Internet's physical and virtual infrastructure is provided by private companies: networks, equipment, services, software, many of which are also transnational – how should they be regulated? By which jurisdictions' laws?

GLOBALISATION OF COMMUNICATIONS

- The Internet has presented a much more globalised communications medium than previous TV, radio, telecoms
- We have seen the rise of transnational technology companies, especially from the United States, providing a lot of Internet services (especially outside of China)
- But – communications regulation mainly happens at a national level; sometimes at the regional level (e.g. European Union)
- This is a challenge for national regulators and national communications policy
- We have different policies in different countries – but services which are globalised

JURISDICTION

- Ability/legitimacy of institutions to exercise legal power in a particular, usually geographic area
- More specifically: the authority of a court to decide a matter
- Easy example: a nation-state exercising legal power over its geographical territory and those within in (people, companies, etc) – a court in that nation state adjudicating a dispute between 2 nationals of that country; re a house located in that territory
- More difficult examples: transnational issues – either via tech (like Internet); people of different nationalities; whether a particular subject matter falls within that court's jurisdiction e.g. place in the hierarchy
- Related concepts: (1) choice of law, (2) choice of forum and (3) recognition and enforcement of foreign judgments -> Private International Law

DE LA CHAPELLE & FEHLINGER

Cross-border disputes arise 'between users, the services they use, public authorities and any combination thereof'

'At least four territorial factors can play a role in determining applicable law:

1. the location of the Internet user(s);
2. the location of the servers that store the actual data;
3. the locus of incorporation of the Internet companies that run the service(s) in question; and,
4. potentially, the registrars or registries through which a domain name was registered.'

CHALLENGES FOR DIFFERENT ACTORS

Governments, in upholding and enforcing their national laws

Global Internet platform corporations, in interpreting and complying with the laws of up to 200 countries where they are accessible

Technical operators, worrying that the separation between technical internet layers and their role in each becomes blurred

Civil society groups, which fear a 'race to the bottom' on privacy and free expression standards

Normal users, 'confused by the legal uncertainty about what rules apply to their online activities and feel powerless to obtain predictable and affordable redress when harmed, as multi-national litigation is beyond their reach'

International organisations, 'struggle because of overlapping thematic scopes, or a geographical remit that is not universal'; lack of consensus among members; primarily intergovernmental, not multistakeholder

EXTRATERRITORIALITY

Extraterritorial extension of national jurisdiction, through 3 main methods:

1. Gov with Internet platform based in its jurisdiction can impose national laws on that company which may have global effects e.g. US surveillance (revealed by Snowden); Microsoft Ireland case ('sorted' by the US CLOUD Act)
2. Legislation with an extra-territorial reach e.g. EU's General Data Protection Regulation
3. Litigation e.g. after EU's Right to be Forgotten case (*Costeja*), French DP authority demanded Google de-index results globally – CJEU in very recent decision has said Google only has to remove results in 29 EU Member States, not beyond EU

DIGITAL SOVEREIGNTY OR RE-NATIONALISATION

1. Through technical means e.g. Great Firewall of China blocking some IP addresses etc
2. Data localization: data of national citizens processed by foreign companies needs to be stored within the national jurisdiction e.g. Russia, Vietnam's new Cybersecurity Law – but not easily scalable globally esp for small countries
3. See also: 'strong national intermediary liability regimes, requirements to open local offices (e.g. Vietnam), demanding back doors to encryption technologies (e.g. Australia) or the imposition of full-fledged licensing regimes (e.g. China?)

But these measures places on transnational operators may have impacts on other jurisdictions – and not respect the digital sovereignty of other countries?

REGIONAL INTERNET REGULATION?

Large and rich countries or regions can ensure their laws, regulations and policies are enforced against transnational Internet companies

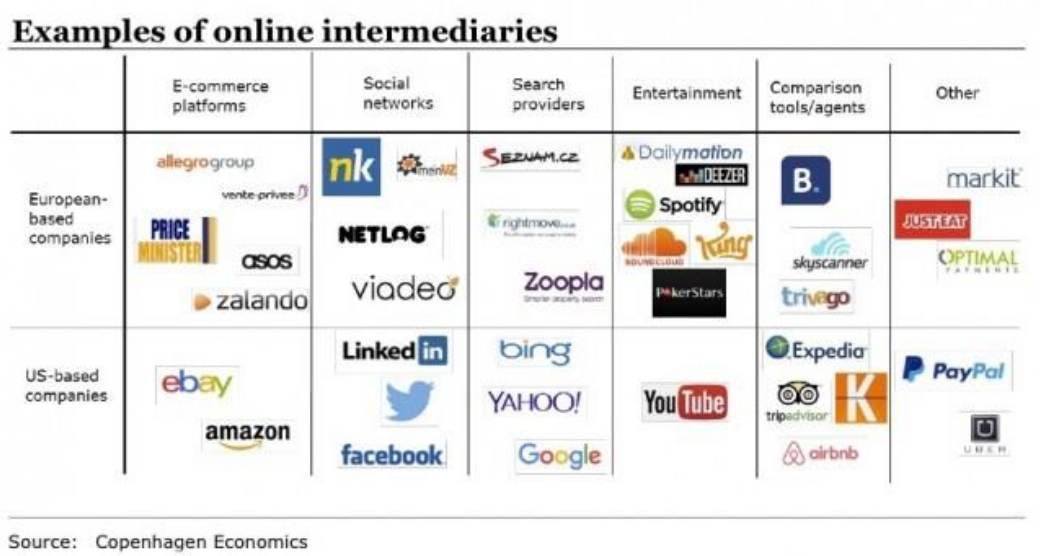
The United States, European Union, China, India and Russia have, to varying degrees, managed to do this

But – smaller countries may have more problems in getting large transnational companies to respect their laws

INTERNATIONAL COOPERATION?

- No Internet Treaty
- Mutual Legal Assistance Treaties – usually designed for criminal investigations in pre-Internet days – not well adapted for Internet environment
- Instead we increasingly see public authorities making these kinds of requests to private companies located in other jurisdictions:
  - Domain seizures: Removal of the entire domain of an allegedly infringing website.
  - Content takedown: Removal or withholding of a specific piece of infringing content.
  - User data access: Access to user information related to who posted infringing content, or other investigations.

PRIVATE INTERMEDIARIES



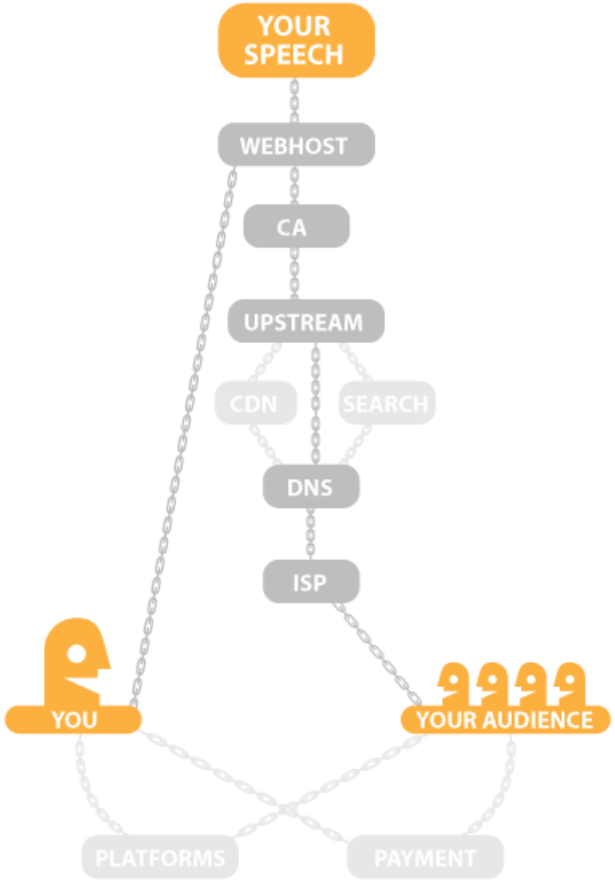
- Different kinds at different 'layers' of the Internet, e.g.:
  - Internet Service Providers
  - Other physical infrastructure providers (computers, equipment, data centres etc)
  - Software providers
  - **Platform operators** – mediating between different users/networks e.g. social media, messaging apps, search engines

PLATFORM OPERATORS - GILLESPIE

'What unites them all is their central offer: to host and organize user content for public circulation, without having produced or commissioned it. They don't make the content, but they make important choices about that content: what they will distribute and to whom, how they will connect users and broker their interactions, and what they will refuse.'

ALSO: a lot of platforms operate for free by collecting and monetizing user data.

Gives rise to both free expression and privacy concerns re content moderation and data access, use and transfer.



GOVERNANCE OF PLATFORMS

- Mostly they are private for-profit corporations
- Characterised as 'intermediaries'
- 'Social media platforms are not only in the middle between user and user, and user and public, but between citizens and law enforcement, policymakers, and regulators charged with governing their behavior.' (Gillespie)

SECTION 230 OF THE US COMMUNICATIONS DECENCY ACT

(1) Treatment of publisher or speaker

No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.

(2) Civil liability

No provider or user of an interactive computer service shall be held liable on account of—

(A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or

(B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).

- Known as a 'safe harbor' for internet intermediaries

'In other words, online intermediaries that host or republish speech are protected against a range of laws that might otherwise be used to hold them legally responsible for what others say and do.' (EFF)

SAFE HARBORS GLOBALLY

'BROAD IMMUNITY' – US POSITION

'CONDITIONAL IMMUNITY' – EU, RUSSIA, SOUTH AMERICA – NOT LIABLE IF NO ACTUAL KNOWLEDGE OF ILLEGAL MATERIAL AND THE PLATFORM RESPONDS TO TAKEDOWN REQUESTS FROM THE STATE OR COURTS TO REMOVE CONTENT

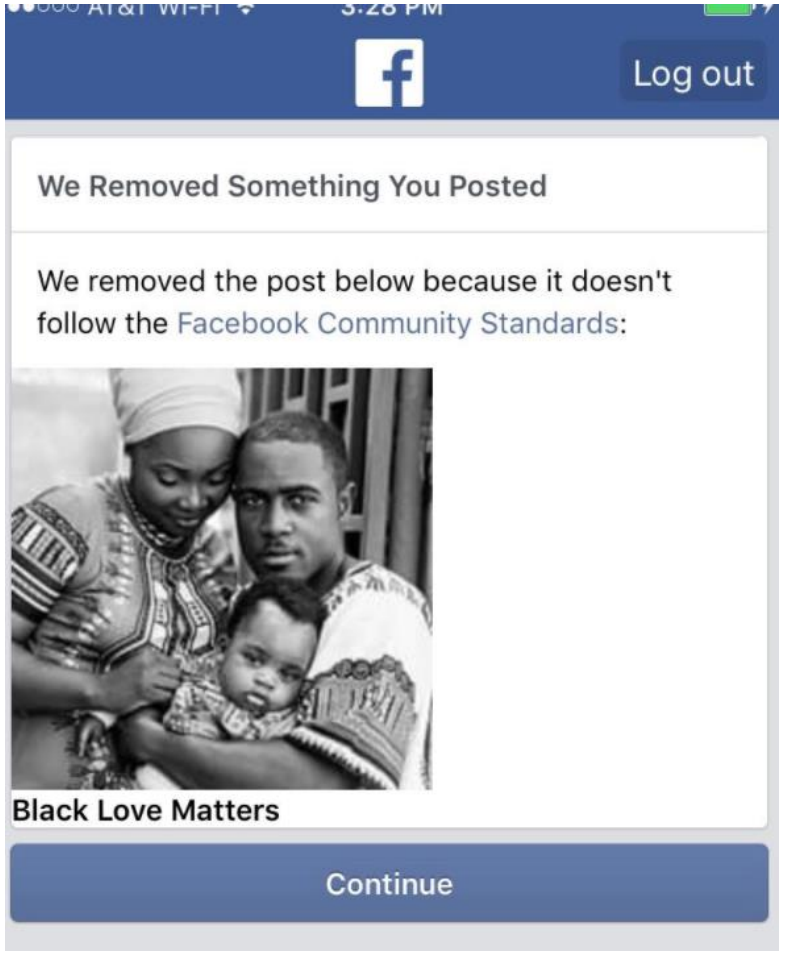
STRICT LIABILITY – MIDDLE EAST, CHINA – INTERNET INTERMEDIARIES MUST PREVENT CIRCULATION OF ILLEGAL/ILLICIT CONTENT – OFTEN PROACTIVE CENSORING/REMOVAL OF CONTENT

CHALLENGES FROM SOCIAL MEDIA

- Safe harbors were not designed with contemporary social media sites and other platforms in mind
- Intermediary liability is usually nation-specific, but platforms are usually not – many platforms are based in the US and enjoy the broad immunity of s 230 CDA but operate in jurisdictions with conditional immunity and strict liability
- Terrorism, hate speech and racial discrimination, cybercrime, protecting children online etc have challenged platforms' safe harbors re content they host in both liberal democracies and more authoritarian regimes

GOVERNANCE BY PLATFORMS - GILLESPIE

- ‘nearly all platforms impose their own rules, and police their sites for offending content and behavior. In fact, their ceaseless and systematic interventions cut much deeper than the law requires’
- Most have some rule prohibiting or limiting the following:
  - sexual content and pornography
  - representations of violence and obscenity
  - harassment of other users
  - hate speech
  - representations of or promotion of self-harm
  - representations of or promotion of illegal activity, particularly drug use
- Lots of issues with ‘false positives’ i.e. content being removed which is legitimate



PRACTICAL PROBLEMS

BUSINESS | gallery | magazine-22.11

The Laborers Who Keep Dick Pics and Beheadings Out of Your Facebook Feed

BY ADRIAN CHEN 10.23.14 | 6:30 AM | PERMALINK

Share 256 Tweet 496 +1 47 Share 10 Pin it 2

A contractor at the Manila office of TaskUs, a firm that provides content moderation services to U.S. tech companies. MOISES SAMAN/MAGNUM

- Limits of community moderation with huge platforms
- Too much content and activity to review before it is posted/made available (Apple ‘s app store is an exception)
- Labour of content moderation – outsourced to the Global South by US companies esp Facebook to Philippines
- To remove content or to filter it (help users avoid it)

BIGGER QUESTIONS AROUND LEGITIMACY OF GOVERNANCE OF AND BY PLATFORMS

- Quasi-public role – but not often subject to constitutional/administrative law constraints unlike public bodies?
- Adjudicative role – but does this accord with due process, procedural fairness, rule of law, protection of rights?
- Or – since platforms are usually private companies – should they just be governed by normal laws that private companies are subject to?

- See Nic Suzor's work on Digital Constitutionalism
- See the current discussions on the Cybersecurity Tech Accord

QUESTIONS?

PART II

DISCUSSION AND RESEARCH EXERCISES

CASES IN ITALY

Do you know of any Internet law cases in Italy which have involved questions of jurisdiction?

LEGISLATION AND INTERNET POLICY IN ITALY

1. Can you identify any policy or legislative initiatives the Italian government is planning for the Internet?
2. How does the Italian government plan to implement the new Digital Copyright Directive?

THANK YOU

ANGELA.DALY@STRATH.AC.UK