

# INTERNET INTERMEDIARY LIABILITY: A PRIMER

Nicolo Zingales, 10 February 2014

## Basic Outline

Who

What

Why

When

How

# Who is an intermediary?

- Any provider of a service that is necessary to engage in networked communication

## **A tentative list**

- Network operators, mobile telecommunications providers, and access providers (ISPs in a narrow sense)
- Website hosting companies, including portals, dedicated server space and domain name registrars
- Information location tools and content aggregators
- E-commerce platforms and online marketplaces
- Providers of online services, such as email and cloud computing, which allow user-to-user communications or host user-generated content
- Network-related hardware manufacturers, such as computer and mobile manufacturers
- Network-related software and applications developers, such as companies designing anti-virus programs and filtering technologies.
- Payment intermediaries, such as companies offering credit cards and other online payment system?

# What is intermediary liability

- Usually indirect, or “secondary” liability for content created by others
- However, some legislations expand the notion of prohibited acts to hold intermediaries directly liable (example, “inactivity or indifference” may be sufficient to infer the existence of authorization or permission),
- Criminal and civil liability
- Damages and injunctive relief

# What activities are covered?

- Conduit: transmitting, routing, or providing connections for material through a system or network or by reason of the intermediate and transient storage of that material in the course of such transmitting, routing, or providing connections
- Caching: intermediate and temporary storage of material on a system or network undertaken for the purpose of enabling subsequent users to access material made available by one particular use
- Hosting: storing of information on systems or networks at the direction of a user
- Information location tools: services allowing location of information on the web, such as a directory, index, reference, pointer, or hypertext link
- Non-profit education (US-specific): institutions acting as service providers for their staff, such as faculty members and graduate students performing teaching or research.

# Why does it matter?

- Increasing importance of digital rights in knowledge-based economy
- Risk of abuses for political or commercial purposes
- Increasing tendency towards the creation of “private regimes” operating independently from the substantive law of the country concerned
- >>>need for uniformity, principles and safeguards

# When did IIL safe harbors develop?

- Context: development of digital technologies, strong US “copyright industry” lobbying and international agreement on copyright protection (WIPO Copyright Treaty of 1996)
- First model (1996): US Communication and Decency Act, Section 230
  - Provides complete immunity for *good faith* editorial choices to any provider and user of an interactive computer service for information created or developed by another person or entity.
  - broad understanding of “interactive computer service provider”: not only the provider, but any user of such services who exercises technical or editorial control over the content created or developed by others.

# How is protection from liability established?

US first to embrace a detailed model for intermediary (non)liability for copyright protection with the DMCA (1998) setting several conditions:

- Conduit: (1) such activity is *initiated by the user* and directed to the designated recipient (2) through *automated process* without any modification or selection of the content or of the recipient, and (3) with *no copy* of the material made available in a manner ordinarily accessible to anyone other than anticipated recipients, or maintained for longer than necessary.
- Caching: 1-3 above, + “upon notification (...) the service provider must expeditiously remove or disable access to the material claimed to be infringing, provided that the notification includes the acknowledgement that the material has previously been removed from the originating site or access to it has been disabled, or a court has ordered it removed”.

# How...(cont.)

- Hosting: (1) Does not have actual *knowledge* of the infringing nature of the material, and is not aware of facts or circumstances from which infringing activity is apparent; or upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material. (2) Does not receive a *financial benefit* directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity; (3) upon notification of claimed infringement, *responds expeditiously* to remove, or disable access; and (4) has a designated agent for the notification of claims of infringements and *follows the special procedure* of notice and take-down indicated by section 512(g).
- Information location tools: 1-4 of ©
- Nonprofit education: the institution must provide to all users of its system or network informational materials that accurately describe, and promote compliance with US copyright law



# How ...(cont.): The takedown procedure

- Expeditiously remove content
- Take reasonable steps promptly to notify the subscriber that it has removed or disabled access to the material.
- Upon receipt of a counter notification (under oath), promptly provide the person who provided the notification with a copy of the counter notification, and inform that person that it will replace the removed material or cease disabling access to it in 10 business days.
- Replace the removed material not less than 10, no more than 14, business days following receipt of the counter notice, unless the complainant has filed an action seeking a court order.
- + damage liability for any knowing misrepresentation of the infringing nature of the activity or of the mistaken nature of the removal or disablement of content

# How do IIL regimes around the world depart from this model? (1) the EU

- Information society service” is defined as “any service normally provided *for remuneration, at a distance*, by means of electronic equipment for the processing (including digital compression) and storage of data, and *at the individual request* of a recipient of a service”.
- Communication conduits have similar obligations as DMCA, but removal for caching can be ordered by an administrative authority in addition to a court
- Hosting: same conditions as the DMCA, but (1) constructive knowledge counts only for civil purposes, (2) must have no authority or control over the recipient (no matter the financial benefit) and (3) no specific NTD procedure
- Issues: no uniformity on “knowledge”, criminal liability and injunctions, and on information location tools.

## (2) Finland

- Court-based procedure
- But, NTD procedure not needed for “manifestly illegal” material.
- Both the service provider and the content provider have the right to appeal against the court order within 14 days from its notification.
- Specific provision establishing liability of the content producer for false information given in his defense.

## (3) India

- Intermediary,” is defined as:  
“any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes”.
- General safe harbor, if the provider “proves that the offence or contravention was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence or contravention”

## (4) Japan

- Intermediary defined as provider of a service whose purpose is to communicate third party information to other parties
- General safe harbor based on the actual or constructive knowledge of illegal activity *and the necessity of the measure* in order to prevent infringements
- “Notice and notice” procedure, and takedown occurs automatically once a week has passed from the forwarding of the notification to the alleged infringer without counternotice
- However, adjudication is done exclusively by private body.

## (5) UK (Notice and Notice + Notice and Disconnect)

- Digital Economy Act requires ISPs to provide copyright owners (upon request) with anonymised reports showing numbers of notices received by each subscriber, and allows copyright owners to apply for a court order to reveal the names and addresses of subscribers on the list.
- ISPs have by contract with subscribers established a system of penalties ranging from educational videos to disconnection

# A word on filtering and injunctions

- Both the DMCA and the ECD specify that general monitoring obligations should not be imposed
- However, both contain language that could be read as requiring the installation of filters for illegal content:
  - section 512(m) of the DMCA specifies that standard technical measures developed in accordance with industry can legitimately derogate to this prohibition
  - in EU, the ECD indicates in article 12.3 that it does not prevent the possibility for a court to require the ISP to prevent an infringement, although the European Court of Justice has held that imposing the installation of filters for all copyrighted content licensed by complainant would be disproportionate
- In addition, the European Court of justice has held that injunctions must be available against an ISP to impose the release of information necessary for identifying users operating in the course of trade .

# The African context

- African Charter, art. 27 “the rights and freedoms of each individual shall be exercised with *due regard* to the rights of others, collective security, morality and common interest.”
- No protection of privacy, but freedom of expression in art. 9
- Declaration of Principles on Freedom of Expression in Africa, favor for self-regulation of media
- Presumption of innocence applies also in civil proceedings