The Role and Responsibility of Internet Intermediaries in the Field of Copyright and Related Rights

Lilian Edwards

Professor of E-Governance

University of Strathclyde, Glasgow

WIPO, June 22 2011

The issues

- Online intermediaries (OIs) eg ISPs, hosts play a vital role in Internet economy in providing access to, hosting and distributing content.
- Newer intermediaries providing new functionality eg search, aggregation, social networking, distribution of legitimate © and user-generated content, also have key roles
- Ease with which infringing content can be accessed and distributed seen as acute problem for content industries
- What role should OIs have here?
- In particular should they be compelled to take part in imposing sanctions on alleged infringers ("graduated response")?
- Do we need international harmonisation in this area?

Existing model global regimes for OI liability

The original policy issues

- OIs – originally ISPs - seen as the natural gatekeepers to the Internet
- Seen as most effective actors to control distribution of illegal and harmful content (obscenity and defamatory content as well as copyright)

BUT

- Lack of effective *practical* control – volume of material, dynamic nature
- Lack of *legal* control (privacy? Liability for interference?)
- *Inequity* - "shooting the messenger"
- Consequences of unlimited liability – effect on online industry and digital society?

CONSEQUENCE: development of global safe harbors or immunity regimes c 1998-2000 on

US Digital Millennium Copyright Act s 512

- Copyright only ; applies to “service providers”
- Divides OIs into mere conduits, hosts, caching intermediaries, and “linking tools” eg search engines.
- “Safe harbor” given from liability, subject for hosts to
  - Expedient take down on notice (NTD)
  - Systems to identify and remove repeat infringers
  - Hosts to accommodate TPMs
  - Not receiving direct “financial benefit” (s 512(b))
- Seen as good balance between interests of OIs, rightsholders and public interest.
- Concerns about chilling effect of NTD on free speech (cf CDA – total immunity re publication torts)
- Met partly by “put back” notices to meet take down & penalties for unfounded accusations + identifn as ©holder
- Injunctive relief remains possible

The EC Directive on E-Commerce 2000

- Applies to Information Society Service Providers (ISSPs)
- Some doubt about status of “for free” services, eg Google, now mostly allayed
- “Horizontal effect” - not just (c) content
- Immunities allocated in respect of functions: mere conduit, caching, hosting. No reference to “linking”. Some EU states have brought it in under one of existing heads.
- NTD regime re hosting, not as well worked out as DMCA. Liability can arise on actual knowledge of “illegal activity or information” OR “awareness of facts and circumstances”
- Crucially, asserted that OIs not under obligation to *monitor* for such awareness (art 15)
- Injunctive relief remains available (art 14(2))
- Tension between these two in later P2P filtering cases.

The P2P problem: going beyond NTD

- NTD was a good solution when sites *physically hosted* infringing content eg MP3.com.
- However, creation of “peer to peer” sharing removed utility of NTD
- 1st generation P2P (peer to peer) – *Napster*, 2001 – centralised database
- 2nd generation –*Grokster*, Supreme Court, 2005 – decentralised – “inducing” infringement. US courts rejected idea that safe harbors of DMCA applied to P2P clients.
- 3rd generation – BitTorrent (BT) protocol**.** Decentralised, fast, sometimes anonymised/encrypted (eg Winny P2P in Japan, Tor). Most Western P2P traffic now uses BT.

Result?

- Phyrric victory of *Grokster – why?*
  - 2nd/3rd gen networks persist even when client shut down, eg eDonkey
  - Open source protocols eg BT technology
  - Lack of *Napster*–style chokepoints and ease of moving data to different servers
  - *So eg Pirate Bay* (torrent site) lost in Swedish courts 2009 but has continued to function mostly since

=> New strategies:

- Sue users; sue torrent sites; sue ISPs to (a) block torrent sites (etc) (b) control access of their users to infringing content.

Suing users

- Sue (or threaten with suit) the filesharers not (or as well as) the intermediaries
- Unpopular with customers; apparent errors, disproportionate penal damages. Deterrent? Too random.
- RIAA said in 2008 would end volume litigation
- In EU/UK, also issues of how to obtain identity of filesharer from ISP
- Data protection law sees this as processing of personal data
- Time-consuming , costly and courts may be unhappy with extortionate approaches – see recent UK *ACS-Law* case

Sue torrent sites and/or ISPs

- Back to ISPs as “chokepoints”
- Aim: sue **ISPs** as contributing to, authorising, etc filesharing and **then** get injunction ordering them to block access to torrent etc sites (or other duties – see graduated response)
- Some big EU successes – eg Italian Supreme Court ordered Pirate bay blocked by all Italian ISPs; but cf rejected by Norway.
- *Roadshow v iiNet* – ISP found not liable in Australia
- *EMI v Eircom* – Irish ISP settled and agreed to impose “3 strikes” on users and block Pirate Bay
- But – *EMI v UPC*, 2010 - same judge said Irish copyrt law did not give power to order ISP to block site like Pirate Bay (!)
- Enormous global legal and business uncertainty, harmful to OIs, including those with novel business models eg search engines, social networking hosts
- Compliance of such actions with immunity regimes very unclear

“Graduated response”

- Seeking ISP co-operation (by legislation, by court order, by voluntary co-operation) in some or all of–
  - Identifying users from IP addresses harvested by rightsholders
  - Passing on allegations of infringement (warnings, strikes) to identified filesharers (“notice and notice”)
  - Imposing *sanctions* on identified filesharers, usually on some threshold eg “three strikes”
  - Sanctions can include traffic slowing, restricted access to certain sites, monitoring (DPI), disconnection
  - ISPs may also be asked to block access for all to certain sites eg torrent download sites, “cyber-lockers” = hosts of infringing content in non-compliant jurisdictions

“Graduated response” - advantages

- Alleged that all other approaches have failed
- Speedy and cheap for © industries compared to suing (some) users in court (esp in EU given DPD constraints)
- Better for © industries than suing own customers
- Deterrent as more chance of “being caught”
- Educational as user typically gets several warnings before sanction
- Evasion possible but doesn’t need to stop all filesharing – just enough
- Better for ISPs by removing bandwidth hogs?? They already manage traffic.

“Graduated response” - problems

- *Due process* : disconnection/sanctions without *prior* court process/independent oversight. HADOPI 2 demands supervision by judge; UK DEA does not.
- *Error:* harvesting IP addresses .and matching them to ISP subscribers both very error prone (mobile networks?)
- “*Collective punishment*” : IP address only identifies *subscriber*, not actual filesharer – should parent be liable for kids (or kids for parents??). Visitors?
- Liability of domestic users for *open wi fi* ? What “reasonable steps” can be demanded eg of the old?
- *Public open wi fi* - Libraries, universities, community? Also businesses eg hotels, cafes using open wi fi as draw. Loss of social utility.

“Graduated response” – problems - 2

Fundamental rights and graduated response

–*Privacy* - “Deep packet inspection” (DPI) might be required of ISPs to filter traffic to/from users (eg, no P2P protocol traffic) – is such blanket surveillance lawful under EU DP law? See AG opinion in *Sabam v Scarlet*.

–Implications for *net neutrality*?

–*Freedom of expression* – Right to access Net? For education/work/e-government? Depends if sanction involves blacklist for all ISPs? Proportionality of sanction?

–*Website blocking*: especially worrying; threshold of evidence required ?, “dual purpose” sites like YouTube, cloud sites, etc.

–General issue of *proportionality*.

Costs ! Division rightsholders/ISPs controversial. Will it save money?

Alternatives - 1

Levies and taxes ("alternative compensation schemes")

- Already used in some systems to compensate for private use/ "fair use"
- Compensate for private downloading? Fisher.
- Return to artists plus advantages digital distribution – choice, flexibility, format shifting
- Issue - market rate return preferred to flat rate return.
- Arrival of iTunes (enabled by DRM) thus "killed" this avenue
- DRM has since fallen out of consumer favour

Alternatives - 2

Find **alternate business models** than selling **copies?**

- Legal pay-for-downloads (iTunes etc) – not yet in all countries (also merchandise, gigs etc)
- Newer free + ads/ “freemium” model - last.fm, Spotify, YouTube, etc – streaming exceeding downloading
- Issues
  - difficulty of getting **licenses** from labels– should there be compulsory licensing, as with radio plays?“Legal P2P” eg Virgin Media, especially hampered – blanket flat rate packages resisted
  - Is ads revenue model sustainable?.
  - Will people *pay*? 80% in UK said they would if provided. Some Spotify success.
- **Bundling?** Cf iPhone/apps; Nokia Comes With Music.
- **Revenue sharing**: cf YouTube Content ID – monetising “tolerated use”rather than take down. Needs pro-active investment eg © databases, license deals, back catalogue. Some exchange of control for revenue.

Conclusions - 1

- Global consensus on NTD as sensible balance between rightsholders and intermediaries broken in copyright field
- No consensus on replacement regime
- Graduated response (GR) solutions are costly, error prone and sanction may be disproportionate; pose serious risks to fundamental rights and public interest in digital inclusion; and their effectiveness is unproven.
- Accordingly recommended that any attempt to impose GR by law should be justified by prior, independent ,empirical investigation, taking into account not just economic factors but also (i) impact on fundamental freedoms (ii) public interest in digital inclusion and promotion of innovation and (iii) state of incentives to create a market of legal alternatives to illicit filesharing.
- If GR regimes so justified, legislative regimes, subject to constitutional scrutiny , rather than voluntary or coerced measures should be adopted.

Conclusions - 2

- Solutions imposing fewer costs on user and public interests should be adopted first, eg, “notice and notice” rather than notice and disconnection, and empirically monitored to see if they prove sufficient
- International treaty should lay down rules on safeguards to be observed in any GR regime imposed by law. In particular, independent and transparent scrutiny of allegations of infringement before sanction, as well as judicial appeal after such, is vital.
- Website and content blocking and blanket monitoring in particular should both be subject to stringent scrutiny as presumptively in reach of fundamental freedoms.
- The international community should give pressing attention to what legal steps must be taken to facilitate and incentivise new business models for monetising digital content.