

Regimes of Legal Liability for Online Intermediaries: an Overview – Lilian Edwards

- Types of online intermediaries

Historically law developed with Internet Service Providers (ISPs) in mind eg (then) CompuServe, AOL, Demon; goals expanded during dot-com boom to protecting hosts (Amazon, e-commerce portals, traditional media going online eg BBC, NYT etc); law troubled since by “new” types of intermediaries: eg search engines; auction sites; aggregators, comparison sites; P2P client sites, torrent sites; user generated content (UGC)sites (eg Facebook, YouTube, eBay); mobile intermediaries.

- Legal risks

Extremely diverse. Liability for content can include libel/defamation; adult material; child sexual images; terror/hate material; blasphemy; copyright infringement; fraud or false advertising; breach of privacy criminal trading standards law. Relatively little litigation globally, but enough to scare operators into demanding protection c 2000.

- Global regimes of “safe harbors” or ISP/intermediary immunities.

Best known are

- EC E-Commerce Directive 2002 arts 12-15; covers all types of civil or criminal liability except gambling and (oddly) privacy/DP; “horizontal” provision; almost total immunity for acting as mere conduit, for caching; controversy around the hosting provisions (art 14) – see below - current regime is no liability without either actual or constructive knowledge of illegality – in practice, mainly a “notice and take down (NTD)” paradigm.
 - US Digital Millennium Copyright Act – covers only intellectual property. Similar format to ECD except that
 - Explicit protection for “locational tools” ie search engines and hyperlinking sites
 - Better worked out rules on NTD eg requires proof of authenticity for sending take down letter; opportunity to object and demand “put back” (though almost never used); service provider protected from suit if they take down in good faith.
 - Many developing countries still have no rules.
- Regimes in crisis – why?
 - Transformation of intermediaries from self-professed non-culpable neutrals (pre 2000 ISPs) to sites, esp UGC ones, arguably “complicit” in various types of illegality to make profits for themselves. Most obvious problems:
 - ISPs as provider of broadband for downloading copyright files illegally; response in France, UK, heavily lobbied for in EC Telecoms Framework and ACTA, has been “three strikes” notice and disconnection schemes, making ISPs responsible for policing filesharing; clearly against spirit of ECD Arts 14 and 15.
 - eBay as obvious purveyor of counterfeit luxury-name goods. Issue dressed as trade mark law but in principle about whether “notice and take down” is now insufficient and site should be obliged to monitor and filter ex ante. Same issue re YouTube/Viacom copyright dispute in USA.

- State pressure on hosts, ISPs, search engines to act as guardians of public morality: eg filter child porn and harmful content; monitor for terror attacks.

Questions

- Do “one size fits all” regimes like ECD still have a place? Especially given the strength of the pro-IP lobby, and the anti-child pornography lobby?
- Should the law move from only requiring NTD of hosts, to demanding prior monitoring and filtering to avoid liability? Should this be connected to financial gain by site, and if so, how?
- What basic protections should a NTD or filtering regime have so as not to become a license for private censorship or abuse by rights holders? Is the DMCA a good model here?
- Do search engines (or other intermediary classes) need a special immunity regime?
- Do online intermediaries still need special protections at all in a mature online market?