

Intermediary Liability & Gatekeeping

Protecting Platforms for Freedom of Expression

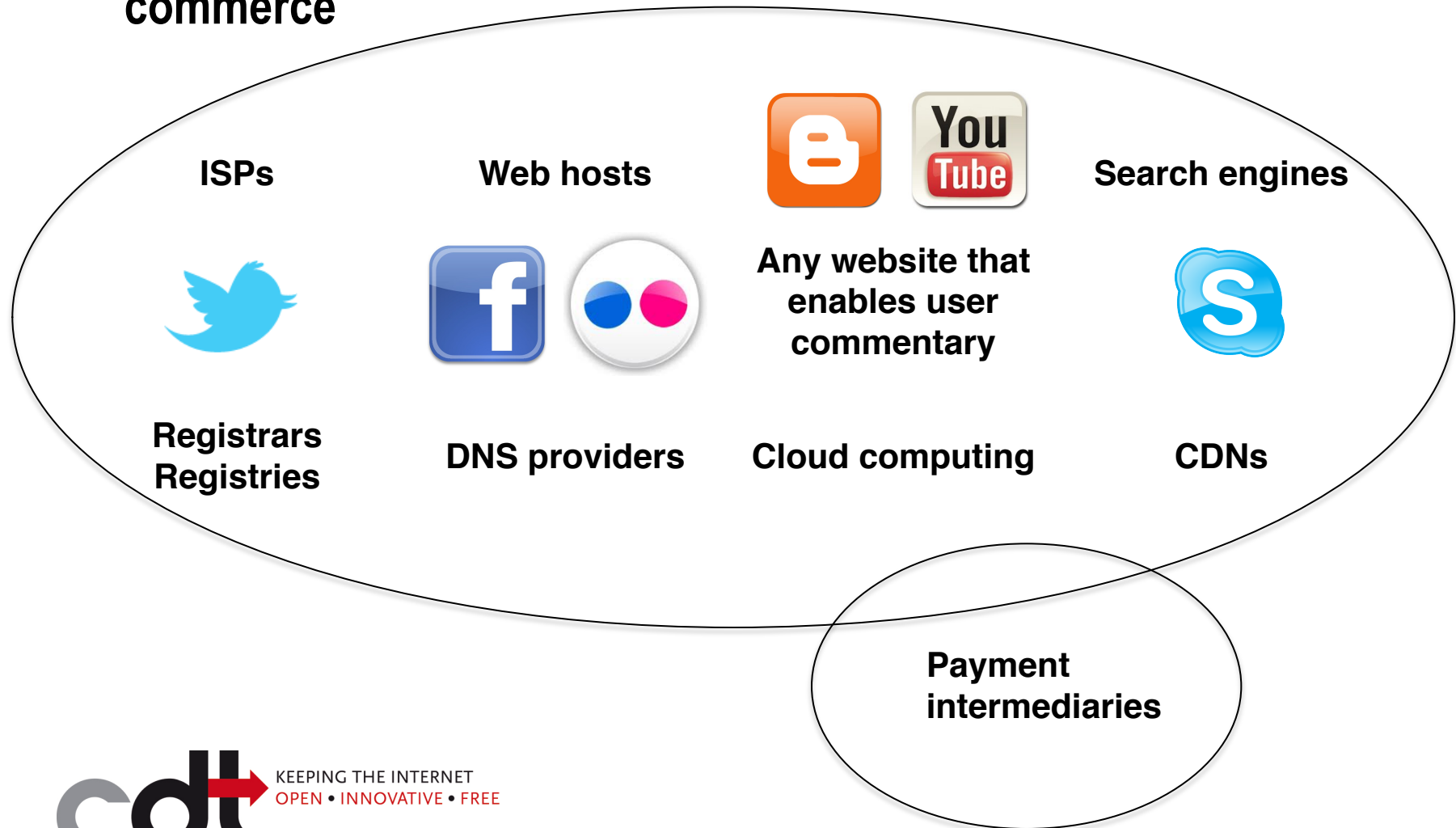
These slides were compiled by CDT in December 2012.

They may be freely used or copied, with or without attribution, so long as their substantive content is not modified.

They may also be used or copied in modified form, but versions with substantive modifications may not be attributed to CDT.

➔ Defining “Internet intermediaries”

- Platforms and conduits for expression, A2K, association, and commerce



Defining “Internet intermediaries”

- Platforms and conduits for expression, A2K, association, and commerce
- Essential for all Internet communication
- Focal point for content regulation, social policy questions

Policy questions

- What role should intermediaries play in advancing public policy goals?
- What is the scope of their liability for user activity?
- Should they take a more active role in policing user activity?

Example policy areas: copyright enforcement, safeguarding national security, defamation & hate speech, protecting children, addressing illegal content

➡ Why intermediaries?

- Global trend – governments and private entities want to enlist intermediaries to solve problems, address unlawful content
 - Direct liability *and* gatekeeping obligations
 - For legitimate purposes or as a pretext for censorship
- But Internet and its intermediaries are general purpose; facilitate both:






AND



FOE flourishes where intermediary gatekeeping is minimized

- Intermediaries are risk-averse; fear of liability limits willingness to create platforms, allow user content
- Self-censorship impacts controversial topics most
- Many platforms would cease to exist if faced with too much liability risk or burdensome monitoring obligations

	In 60 seconds, over:
	200,000 photos source
	72 hours of video source
	275,000 tweets source

FOE flourishes where intermediary gatekeeping is minimized

- **Privacy - Intermediaries may monitor and collect user data**
 - Chilling effect on FOE
- **Can become a powerful and often nontransparent tool for censorship**

FOE flourishes where intermediary gatekeeping is minimized

- “No one should be liable for content on the Internet of which they are not the author, unless they have either adopted that content as their own or refused to obey a court order to remove that content.”
2005 Special Rapporteurs’ Joint Declaration on Int’l Mechanisms for Promoting Freedom of Expression [source](#)
- “(a) No one who simply provides technical Internet services such as providing access, or searching for, or transmission or caching of information, should be liable for content generated by others, which is disseminated using those services, as long as they do not specifically intervene in that content or refuse to obey a court order to remove that content, where they have the capacity to do so (‘mere conduit principle’).

(b) Consideration should be given to insulating fully other intermediaries, including those mentioned in the preamble, from liability for content generated by others under the same conditions as in paragraph 2(a). At a minimum, intermediaries should not be required to monitor user-generated content and should not be subject to extrajudicial content takedown rules which fail to provide sufficient protection for freedom of expression (which is the case with many of the ‘notice and takedown’ rules currently being applied).”
2011 Special Rapporteurs’ Joint Declaration on Freedom of Expression and the Internet [source](#)

Economic case for intermediary protections

- Legal risk discourages innovation in new user-generated content models
- Legal risk entrenches existing market players
- Legal risk slows development of domestic Internet industries
- Creates bad environment for investment

Slows development of a country's Internet economy

Models for Protecting Intermediaries

- **Broad immunity**
 - e.g., US's "Section 230" – immunity for wide range of content-based claims
- **Conditional safe harbor from liability**
 - e.g., US DMCA for copyright; EU E-Commerce Directive for broader range
 - Limits liability as long as intermediary lacks specific knowledge and meets certain requirements
 - Requirements can vary by type of intermediary – “mere conduit,” data cache, content host, search engine

Other National Approaches

■ Chile & Canada

- Intermediaries are held liable for third-party copyright infringement if they do not comply with a takedown order issued by a court. Notice-forwarding requirement.

■ India

- Modeled on E-Commerce Directive, but 2012 regulations cast doubt on effectiveness of protections

■ Thailand

- Computer Crimes Act – extends liability for unlawful activities to service providers that intentionally “support” or “consent” to them. Data-retention requirement.

■ China

- Imposes liability and self-monitoring requirements for 3rd party content at nearly every layer – content creator, content host, access provider

Principles for “Notice and Action”

- **Clear guidance about what is valid “notice”**
 - Must be highly specific to ensure targeted response
 - Sufficient evidence or legal attestations of illegality
- **Required actions must be narrowly tailored and proportionate**
- **Safeguards are necessary to mitigate risk of abuse**
 - Penalties for unjustified notice
 - Transparency
 - Appeals system and due process
 - Flexibility for service providers

Principles for “Notice and Action”

- Required actions should not create an ongoing duty to monitor
 - No “notice and stay down”
- Required “actions” must be appropriate for type of service
 - For example, notice-and-block for ISPs raises much more serious issues of proportionality
- Actions that result in content takedown should be limited to contexts where illegality is straightforward
 - Compare defamation to copyright

Direct Gatekeeping Obligations

- Governments may seek to impose direct requirements to prevent or punish illegal content
- Believe intermediaries are well-positioned to take action
- But obligations can impose severe costs on FOE and privacy, and undermine the certainty and benefits of liability protections

Direct Gatekeeping Obligations

- **Website blocking**
 - Technical approaches vary and can have very overbroad impacts
 - Can be costly
- **Domain seizures**
 - Can be overbroad; raises difficult jurisdictional questions
 - In US, concerns about due process
- **Licensing and Content Regulation**
 - Carry-over from mass media regulation; limits opportunities for online expression
- **Warning or Punishing individual users**
 - E.g. “graduated response” or notice-forwarding requirements
 - Can provide educational function, but punitive actions raise due process concerns

Key questions for analyzing national law I

- Does the law protect intermediaries from criminal or civil liability for third-party activity?
- If yes:
 - What kinds of intermediaries qualify for protection?
 - What kinds of legal claims does the law apply to?
 - How does the intermediary qualify for protection? For example:
 - By transmitting without modification or selection of content (“mere conduit”)?
 - No direct financial benefit? ■ No actual knowledge?
 - Take “action” upon notice – remove or block content, pass on notice, retain data, suspend user?

Key questions for analyzing national law II

- Does the law make clear that intermediaries may not be compelled to actively monitor and police user activity?
- Does the law place affirmative obligations on intermediaries?
 - How burdensome? What will be the effect on investment?
 - How will users' FOE and A2K rights be affected?
 - Are there procedural protections for FOE? Recourse in case of mistakes?
 - Is there risk of overbroad impact?

Key questions for analyzing national law III

If the law takes a “notice and takedown” approach:

- Who can provide notice? For what kinds of alleged offenses?
- What form must notice take?
- How quickly must content be taken down?
- Are there safeguards against abuse?
 - Transparency
 - Appeals and due process
 - Penalties for unjustified notice

Alternatives: How to address illegal content?

- **User-empowerment tools – users control their content choices**
 - Key is user control, not central mandates
- **Increased coordination and enforcement against posters of illegal content (rather than intermediaries)**
 - Requires strong rule-of-law and due process to protect right to anonymity

Alternatives: How to address illegal content?

- **Voluntary actions by intermediaries**
 - More flexible than gov't mandates, but vulnerable to procedural abuses
 - Must avoid “end run” around limits on state action
 - Must be transparent and inclusive in development
- **“Follow the money”**
 - Focus on business relationships behind illegal content, rather than unaffiliated Internet intermediaries
 - Avoids technical problems of approaches focused on communications intermediaries
 - Powerful tool, but pose risk to FOE if used against controversial but lawful sites

Additional resources

- CDT, Shielding the Messengers: Protecting Platforms for Expression and Innovation, December 2012
 - In-depth examination of intermediary liability protections and alternatives
- CDT Advocacy Toolkit with additional papers and resources