

Stanford Law School

Intermediary Liability: Basics and Emerging Issues

Daphne Keller

December 2019

Presentation Roadmap

- High Level Overview (Slides 3 to 13)
- Review of Specific Laws (Slides 13- 22)
- Dials and Knobs for Lawmakers Adjusting Intermediary Liability Laws (Slides 23-29)
- Emerging Questions and Ideas (Slides 31-42)

Intermediary Liability Law

High Level Overview

Intermediary Liability Law

- Defines intermediaries' legal responsibilities for content posted by users.
- Longstanding issue: responding to *illegal* content.
 - Often, but not always, "notice and takedown"
- Emerging issue: responding to *legal* content
 - Might platforms be required to carry lawful speech, even if they don't want to?
 - Might platforms be required to remove lawful but harmful speech?

Intermediary Liability Laws Trade Off Between Three Major Goals

1. Harm prevention

- IL laws can reduce harms ranging from movie piracy to child pornography. Platform gatekeeper role makes them powerful enforcers.

2. Economic growth and innovation

- Express purpose of many IL laws. At the extreme, bad IL laws would make platform businesses impossible.

3. Freedom of expression and information

- Platforms that fear liability take down legal speech to be safe. Investors that fear liability don't fund open platforms.

Intermediary Liability: Ideal Outcome?

Platforms take down bad content, and leave up good content.

Intermediary Liability: Ideal Outcome?

Platforms take down bad content, and leave up good content.

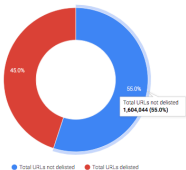
- *If only we could agree on what is good and bad...*
- *The answer might vary for a site directed to kids, a real estate site, a business review site, etc....*

Intermediary Liability: Ideal Outcome?

Platforms take down ~~bad~~ illegal content, and leave up ~~good~~ legal content.

Ratio of Valid to Invalid Notices – Right to Be Forgotten, per Google's Transparency Report

START 5/29/2014 END 10/16/2019



Potentially Illegal Content



The problem the law needs to solve is not: *“What should platforms do with illegal content?”*

It is: *“What should platforms do with this whole array of potentially illegal content?”*

Platform Motivations in Notice and Takedown Systems

- Economic incentive to over-remove.
- Multiple studies document over-removal. See Urban et al 2016, my CIS [blog post](#) listing other studies.*
 - Notification errors
 - Censorship goals: Ecuador, Retraction Watch
 - Commercial goals: takedowns targeting competitors are very, very common
- “Wrongful removal” claims against intermediaries are close to impossible in US. Globally, a few such claims succeeded beginning in 2018 (Brazil, Germany, Poland).

“Over-Removal” and Fundamental Rights

- Expression and information rights
 - Most widely discussed and addressed in cases/literature
- Privacy and data protection rights
 - Particularly in “monitoring” cases
- Fair trial and remedy or due process rights
- Equality and non-discrimination rights
 - Disparate impact of over-removal because of human bias, machine bias, sloppiness, political pressure, etc.

Case Law on Intermediaries and Rights

- European Ct of Human Rights
 - *Delfi*, 2015: OK to make news forum monitor for hate speech
 - *MTE*, 2016: NOT OK to make news forum monitor for defamation / personality rights infringement
- CJEU *SABAM* and other cases briefly discuss user rights
- *Belen Rodriguez v. Google*, S. Ct. of Argentina 2014
 - No monitoring obligation, because of threat to speech
 - Public adjudication/order standard for many removals
- *Shreya Singhal*, S. Ct. of India 2015
 - Public adjudication/order standard for all removals
- Older U.S. Cases
 - Rare Internet cases: *Zeran*, *Cubby*, *CDT v. Pappert*
 - Pre-Internet cases: *Smith*, *Bantam Books*

Intermediary Liability Law

Review of Specific Laws

Intermediary Liability Globally

- Many countries have law for just one aspect, i.e. just for copyright (Chile) or just for ISPs (Japan)
- Many have no specific law, but – as in *Belen Rodriguez* in Argentina - reason from general tort and rights principles.
- Some rely on control of local architecture (like China's "Great Firewall")
- In practice, law/politics from a few regions shape outcomes for the rest of the world
 - US – DMCA takedowns, 1st Am. Drives cultural norms of US platforms, etc.
 - EU – global compliance with hate speech code of conduct, e.g.
 - China – increasingly visible with Tiktok etc.

EU: eCommerce Directive

- eCommerce Directive
 - Art 12: Safe harbor for “mere conduit” information transmission.
 - Art 13: Safe harbor for “caching,” must be “automatic, intermediate, and temporary”
 - Art 14: Safe harbor for “hosting,” provider must remove upon obtaining knowledge of illegality
 - Art 15: “No general obligation to monitor”
- News Laws and Pending Changes include:
 - AVMSD
 - Copyright Directive
 - Terrorist Content Regulation
 - Digital Services Act

US Intermediary Liability Law

- Three Major Components:
 - CDA 230: complete immunity for leaving most content up, “good Samaritan” immunity for taking it down
 - DMCA: highly formal notice and takedown for copyright
 - Gaps between the two: non-© intellectual property, federal crimes, prostitution and trafficking claims per 2018 amendment
- Statutes largely occupy the field.
 - US courts have barely considered constitutional or fundamental rights issues, while courts in many other countries have.

Communications Decency Act 230

- Extremely broad immunity for claims that are not IP or federal criminal claims.
 - Don't have to take content down even if known to be illegal.
- Covers very broad range of technologies.
 - As long as do not contribute to creating the content.
- 1996 law with express economic goal (to promote Internet development) and free expression goal.
- Ongoing legislative attacks, including SESTA/FOSTA amendment in 2018.

Communications Decency Act 230

- Two separate immunities:
 - Immunity for *leaving up illegal content*. (230)(c)(1)
 - “Good Samaritan” immunity for *taking down legal content* based on good faith effort to weed out illegal or even “objectionable” material. (230)(c)(2)
- Pragmatic calculation about “moderator’s dilemma” – perverse incentive not to moderate.
 - Under prior law, platforms that moderated user content risked liability as editors (with *control*) or based on having *knowledge* of unlawful content.
 - To encourage moderation, Congress made platforms immune regardless of control or knowledge.

Why Change 230? Conflicting rationales would lead to very different amendments...

- To make platforms take down more racist, bullying, and otherwise ugly or harmful speech?
 - PROBLEM: Much of that is legal speech. 230 is not the reason it's online. But 230 IS the law freeing platforms to take it down.
- To make platforms stop (allegedly) silencing conservatives?
 - PROBLEM: That requires a govt agency to define political neutrality.
- To stop opioid sales?
 - PROBLEM: Federal criminal law already reaches platforms.
- To reach bad actors (Backpage, e.g.)?
- To shift business advantage between hotels/AirBnB, retailers/Amazon, news media/news aggregators?

Digital Millennium Copyright Act (DMCA)

1. Service must be listed in 512(a)-(d) (roughly: access providers, caching, hosting, and search engines).
2. Provider must satisfy some simple, logistical prerequisites (like registering an agent).
3. Most providers must properly respond to valid DMCA notices.
4. Provider must not run afoul of some known, and fiercely litigated, DMCA hot issues (like having “red flag knowledge”).

DMCA Highly Detailed Takedown Process

- Notice must provide specified info from 512(c)(3)
 - Inadequate notice cannot create knowledge and liability. (c)(3)(B)(i).
 - Inadequate notice can trigger duty to coach, or can be ignored, see (c)(3)(B)(ii).
- Intermediary must remove “expeditiously.”
- Counternotice: host “takes reasonable steps promptly to notify” the accused, who may submit counternotice as specified in 512(g).
 - Host is not *required* to do so, but gets additional immunities.
 - 10-14 days after receipt of counternotice, host reinstates content unless complainant notifies host that it is suing the accused.

Intermediary Liability Law

Dials and Knobs

Major Legal Dials and Knobs

1. Protect broader or narrower set of technologies or business models
2. Permit greater or lesser degree of platform control over content
3. Define culpable "knowledge" broadly or narrowly
4. Provide more or less detailed procedural rules for notice and takedown

1. Protecting More or Fewer Intermediaries

- By function: enumerate technologies (like caching, hosting, etc.) versus broadly protecting unforeseen technologies.
 - *Differences here may be particularly consequential for innovation.*
 - *Different rules for different network layers often make sense.*
- By size: define more stringent rules for larger, better-resourced platforms.
 - *Rules like these are hard to define. (What happens to Wikipedia? Perverse incentives for growth/corporate structure?) But in their absence lawmakers may set rules that make competition by small platforms close to impossible.*

2. Permitting More or Less “Control”

- In every intermediary liability system, platforms can lose immunity by exercising too much control.
 - *This is needed at minimum as a definitional line between platforms and content creators.*
 - *Some systems use concepts like “passivity” or “neutrality”.*
- Defining “control” can be extremely difficult
 - *Can platforms have ranking or search functionality at all?*
 - *Can they prohibit lawful but harmful content at all?*
 - *Foreseeability issues - do innovators and investors know what tools are immunized?*

3. Defining Culpable “Knowledge”

- In most intermediary liability systems, platforms lose immunity for illegal content they “know” about.
- Law’s definition (or lack of definition) has great consequences. Does platform remove when it...
 - *Knows that the content exists?*
 - *Knows that someone alleged it was illegal?*
 - *Knows that someone alleged it was illegal in formal notice, subject to penalties for misrepresentation, possibility of legal appeal, etc.?*
 - *Knows because non-lawyers can recognize it as illegal?*
 - *Knows because lawyers recognize it as illegal after researching the law? Must they seek out additional facts? Defenses from the accused?*
 - *Knows because a court/public authority has held it illegal? (This is Constitutionally mandated standard for some claims/countries)*

4. Procedural Safeguards

- Formalities for accuser.
 - *Formal requirements for information included in notice.*
 - *Penalties for bad faith notice.*
- Opportunity for accused speaker to provide “counter-notice” defending speech.
 - *As part of private process carried out by platform. **Note: data suggests this hasn't done much good so far.***
 - *As part of public opportunity before court or regulator.*
- Transparency for independent review.
 - *Like Lumen Database.*

Other Legal Dials and Knobs

- Bright-line rules versus fuzzy standards
- Private versus public user communications
- Different rules for infrastructure layers of Internet
- Due diligence or duty of care versus penalizing control and knowledge
- Public / research transparency
- Different rules for different claims (child abuse vs. defamation, e.g.)
- Legal consequences other than takedown mandates

For a lot more detail, see my *Design Principles for Intermediary Liability Laws* piece with Joris van Hoboken or *Build Your Own Intermediary Liability* piece on Balkinology

Intermediary Liability Law

Emerging Questions and Ideas

Some Big Questions

1. Limits on *state* power to pressure platforms for “voluntary” removal under Terms of Service (TOS)?
2. Limits on *platform* power to remove lawful expression under TOS?
3. Limits on national courts compelling global removal/delisting?
4. Limits on compelling intermediaries to actively police, monitor, or filter users’ activities and expression?
5. Which regulators own platform content issues? (Media regulators? DPAs? Someone else?)
6. If neither platforms nor courts are viable decision-makers, what is left?

1. States relying on platforms' TOS for content removal

- By formal agreement: Hate Speech Code of Conduct
- By state practice: Internet Referral Units
- Human rights experts and academics ask:
 - Does encouraging *private* agreements that effectively restrict Internet users' rights (re speech, surveillance, etc.) violate the *state's* positive obligations to protect fundamental rights?
 - Are states abdicating their own duty to set rules subject to judicial review to protect fundamental rights?

2. Limits on platform TOS power (1/2)

- Can users assert rights to share lawful expression on private platforms (aka “must-carry” claims)?
 - A few lower courts in Brazil (speech rights), Germany (*Drittwirkung*), and Poland say YES
 - 30-ish US cases say NO (see my *Who Do You Sue* paper)
 - Competition and platform dominance matters. See Kavanaugh analysis in *Halleck*, *USTA*, and *Pepper* (or my *Who Do You Sue?* paper)

2. Limits on platform TOS power 2/2

- Can users assert rights to fair and transparent *process* for platform TOS enforcement?
 - Santa Clara Principles: clearly stated rules, consistent enforcement, appeals, transparency reports.
 - Some EU authorities have said YES, as a matter of consumer protection law.
 - Some US proposals would vest similar powers in FTC.
- How would these principles apply to ranking or recommendation systems?

3. Global Removal

- *Equustek*: S. Ct. of Canada orders Google to de-list results globally based on trade secret claim, sees no free expression conflict
- *CNIL*: CJEU says France can't require global Google de-listing for *all* Right to Be Forgotten claims, but can for some
- *Glawischnig-Piesczek*: CJEU says Austrian law can require global Facebook takedown in some cases for defamation
- Happening Now: global removal rulings from India, etc.

4. Filtering – Practical and Policy Issues 1/4

- Filters can't reliably detect context of re-used material
 - ISIS recruitment video used by reporters or in counter-speech
 - Compare child sex abuse content, which has no lawful context
- Errors may fall disproportionately on speakers based on language, race, national origin, religion
 - [Sap et al 2019](#)
- Filters can be very expensive to implement (YouTube Content ID \$100 million at last report)

4. Filtering – Legislation 2/4

- Ecommerce Directive Art. 15 says no “general” monitoring duty
- Copyright Directive Art 17
- Draft Terrorist Content Regulation may have filtering requirement based on *police* notice (Commission & Council vs. Parliament drafts)
- EU Digital Services Act
- UK Online Harms White Paper (references monitoring)

4. Filtering - Human Rights Case Law 3/4

- CJEU 2012 *SABAM* cases: monitoring burdens users' rights to privacy and free expression, host's right to conduct business
- ECtHR *Delfi* and *MTE* rulings: Making a news site monitor user comments for defamation violates users' info/expression rights. Making it monitor for hate speech doesn't.
- CJEU 2019 *Glawischnig-Piesczek* case: approved filtering for court-specified content under Article 15
 - Without discussing fundamental rights
 - Seemingly precludes human review of filters' work

4. Filtering - Human Rights Factors 4/4

What questions would a court ask in truly reviewing a filter for fundamental rights compliance?

- Accuracy and error rate in detecting technical duplicates and discerning new context
- Resulting benefits to claimant or society
- Resulting harms to other Internet users
 - Qualitative: What is the harm – expression, information, data protection, privacy, non-discrimination, fair trial?
 - Quantitative: How many people are harmed? A .1% error rate can affect millions of people a week.
- Alternatives to achieve same benefit with less harm³⁹

5. Who Are the Platform Regulators?

- Media regulators are the natural owners if you think platforms are like broadcasters.
 - Existing model barring “harmful but legal” speech
 - UK Online Harms White Paper
 - Audio Visual Media Services Directive
 - Covers YouTube and other video hosts
- Data Protection Authorities already oversee intermediary liability issues for “Right to Be Forgotten”
- In US – FTC? FCC?

7. A Facebook Supreme Court for Everyone?

- Problem: Everyone is bad at content moderation at scale
 - Platforms mess up all the time. Even a 99.99% perfect job leaves glaring errors.
 - Courts/regulators don't have the resources, If they used platform-style adjudication shortcuts, it would violate due process guarantees.
 - Facebook Oversight Board aka "FB Supreme Court" will at best solve a tiny portion of this problem (which I am hopeful for.) At worst, it will be a politicized, mistrusted failure. We need time to watch this experiment play out before building on this model!
- No one has ever tried to regulate this much (previously ephemeral) human behavior. It was never possible. Our laws and philosophy have no real model for doing it at this scale.

Ways Forward? (1/2)

- Better takedown processes
 - Clearly needed, low-hanging fruit
 - Not enough to counteract over-removal incentives
 - May be hard for small platforms, hurt competition goals
- Two emerging ideas that are important but also IMO currently under-researched and under-theorized. We need very serious analysis and cross-field collaboration. **I'm not saying don't do these, just think a lot before acting.**
 - "Must-carry" rules limiting platform power to take content down under TOS. (See *Who Do You Sue* paper listing models)
 - Regulation of ranking and algorithms. (This is my next big research project. I believe this is incredibly, incredibly complicated and easy to mess up.)

Ways Forward? (2/2)

- *Meaningful platform takedown transparency* (not just aggregate data) is key. Lawmakers need better information to regulate wisely.
- Consider *platforms' strengths* (speed, financial resources, automation) *versus public authorities'* (applying law, protecting rights, democratic accountability). Allocate responsibilities accordingly.
- Vet proposals against, at minimum:
 - Three recurring players: *claimant, platform, accused*.
 - Three big goals: *anti-harm, expression, innovation*.

Thank You

[https://cyberlaw.stanford.edu/about/people](https://cyberlaw.stanford.edu/about/people/daphne-keller)
[/daphne-keller](#)
[@daphnehk](#)