

Santa Clara University

47 USC 230(c)(2) and Immunity for Online Filtering

Prof. Eric Goldman

Director, High Tech Law Institute

<http://www.ericgoldman.org> • <http://hightechlaw.scu.edu>
egoldman@gmail.com

Overview

- 230(c)(1) protects online actors from liability for third party content
- 230(c)(2) protects filtering decisions, even first party decisions
- 230(c)(2) doesn't get much love
 - No specific reference in (scanty) legislative history
 - Dispositive in less than a dozen cases
 - Numerous courts have confused the two provisions or made unhelpful cross-references
 - Effectively ignored in academic literature

47 USC 230(c)(2)

- No provider or user of an interactive computer service shall be held liable on account of—
 - (A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or
 - (B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).

Prima Facie Defense

- **230(c)(2)(A) = first party filtering**
 - Provider or user of an interactive computer service
 - Voluntary action taken in good faith
 - Restrict access or availability of objectionable material
- **230(c)(2)(B) = providing filtering instructions to third parties**
 - Provider or user of an interactive computer service
 - Action to enable or make available the technical means to restrict access to objectionable material
- **Statutory exclusions**
 - Federal criminal enforcements
 - IP laws
 - ECPA

Provider/User of Interactive Computer Service

- **Interactive computer service =**
 - any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions
- **Access software provider =**
 - a provider of software (including client or server software), or enabling tools that do any one or more of the following:
 - (A) filter, screen, allow, or disallow content;
 - (B) pick, choose, analyze, or digest content; or
 - (C) transmit, receive, display, forward, cache, search, subset, organize, reorganize, or translate content.

First Party Filtering

- **230(c)(2) Immunity Upheld**

- Green v. AOL (3d Cir. 2003) (failure to prevent virus in chatroom)
- Langdon v. Google (D. Del. 2007) (rejection of ad)
- e360Insight v. Comcast (N.D. Ill. 2008) (spam filtering)
- Some dicta suggests this is the primary/only purpose of 230(c)(2)

- **Immunity Denied**

- Goddard v. Google (N.D. Cal. 2008). 230(c)(2) unavailable when filtering policy for 3rd party ads related “to business norms of fair play and transparency” [huh?]
- National Numismatic Certification v. eBay (M.D. Fla. 2008). Auctions of counterfeit goods do not qualify as “objectionable” content

Third Party Filtering

- **Publishing filtering instructions to third parties**

- Zango v. Kaspersky (9th Cir. 2009)
- Pallorium v. Jared (Cal. App. Ct. 2007) (distribution of blocklist protected by 230(c)(2)(B))
- Compare MAPS v. Black Ice (CA Superior Ct. 2000).
 - 230(c)(2)(A) available for good faith blocking, even if misapplied
 - 230(c)(2)(A) denied when allegations of bad faith blocking
 - 230(c)(2)(B) applied to distribution of blocklist
 - 230(c)(2)(B) denied for publicly announcing blocklist

- **Implementing filtering instructions provided by third parties**

- Usually covered by 230(c)(1). Ex: Kathleen R. v. Livermore (Cal. App. Ct. 2001)
- But Mainstream Loudon v. Board of Trustees (E.D. Va. 1998). Public library's decision to implement 3rd party filtering software not insulated from review by 230(c)(2)

Statutory Ambiguities

- **Must filtering determinations be made in good faith?**
 - 230(c)(2)(A) = yes, but several cases have said good faith is subjective, not objective
 - 230(c)(2)(B) = ?
- **How do access software providers “provide[] or enable[] computer access by multiple users to a computer server”?**
- **What filtered material is protected?**
 - Reading #1: ejusdem generis interpretation of “objectionable” [“material [that is] obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable”]
 - Reading #2: subjectively objectionable content
 - Reading #3: subjectively objectionable content, software, etc.

What Happens if 230(c)(2) Isn't Available?

- 230(c)(1)
 - Ex: Optionrealbig.com v. Ironport Systems (N.D. Cal. 2004)
- Other statutes
 - 15 USC 7707(c) (no CAN-SPAM liability for email filtering). Ex: White Buffalo v. UT Austin (5th Cir. 2005)
 - Utah §[13-40-202](#) (immunity for spyware identification and removal)
- Constitutional/Public Policy Limits
 - Truth as a defense
 - Opinion as a defense
 - Matter of public interest. Ex: New.net v. Lavasoft (C.D. Cal. 2004) (in context of anti-SLAPP motion)
 - Freedom of the press. Ex: Miami Herald v. Tornillo (US Sup. Ct. 1974) (newspapers do not have must-carry obligation)
- Failed elements of prima facie case
 - Ex: Zango v. PC Tools (W.D. Wash. 2007)

Suggested Practices

- Accurately describe every characterization
- Provide error-correction and dispute resolution processes
- Explain filtering criteria to consumers
- Support a federal anti-SLAPP law