

# Least-Cost Avoiders in Online Fraud and Abuse

**O**n 19 April 1995, the world watched in horror as the militia movement sympathizer Timothy McVeigh destroyed the US Federal Building in Oklahoma City, the largest act of terrorism on US soil until 9/11. An unexpected aftershock

persed across a large area, no single community has incentive to take action.

Furthermore, many perpetrators are small or even judgment-proof. A company fighting counterfeits might face hundreds of sellers; pursuing them all would be a mammoth task. Similarly, even if Zeran had managed to find his defamer, that person probably wouldn't have been able to pay for the damage he or she caused.

As pursuing individual perpetrators proves fruitless, victims naturally seek recourse from intermediaries, such as the operators of an online message board or advertising service. This approach has ample precedent—the 1968 Fair Housing Act, for example, not only prohibits discrimination in the sale and rental of housing, but also bans discriminatory text in advertisements. Print publications have decades of experience screening housing ads, and we might expect similar compliance online. The same is true for other controversial behaviors, such as defamation and false advertising, where intermediaries' obligations are also well-established.

Although intermediaries are compelled to take action online, things look different on the Web. The online Wild West doesn't just reflect cops asleep at the beat: online misbehavior reflects conscious decisions embedded in distinctive legal rules, little-known beyond specialists, which narrow system operators' obligations and liability. The balance of this piece presents and assesses these rules.

Although applicable rules are

BENJAMIN  
EDELMAN  
*Harvard  
Business  
School*

came in a posting on an AOL bulletin board the next week: a prank message promoted offensive and tasteless T-shirts with slogans drawing on the Oklahoma City attack. The message included the home phone number of Kenneth Zeran, who was listed as the putative seller—though, in fact, Zeran had no involvement whatsoever with the T-shirts or the posting (he didn't even have an AOL account). Soon, Zeran's phone was ringing off the hook, and he received multiple death threats and other violent calls. These problems worsened after an Oklahoma City radio station read the sales pitch on the air, complete with Zeran's phone number. AOL removed the offending message, but several more appeared, adding even more offensive slogans and always featuring Zeran's name and number. Shocked and angry, Zeran sued AOL, alleging that the company was negligent in failing to exercise reasonable care to prevent these bogus postings, particularly after Zeran had notified AOL of the problem.

Although Zeran's experience is an outlier, its essence is far from unique. Across the Web, users face all manner of malfeasance that system operators could prevent or

at least mitigate. Request "ring-tones" on a search engine, and advertisements will often promise "free" ringtones that actually cost US\$10 or more per month. Browse apartment listings on Craigslist, and some indicate that tenants of specified races are unwelcome. Search for handbags on eBay, and many are counterfeit.

As these examples show, networked computers can cause substantial harm. The legal system can respond, and has, but with mixed effectiveness. Here, I identify the applicable legal rules that constrain online fraud; I examine the economic underpinnings to identify whether rules assign responsibility to the parties best positioned to take action.

### **Challenges in Pursuing Online Fraud**

Surely, much online misbehavior stems from the mitigating effects of distance. Classic retail fraud hurts local customers, so taxpayers and voters predictably demand government action. In contrast, online fraud can easily target victims half a world away. Will Florida police pursue a perpetrator whose victims are largely in New York? How about Russian police? If an attacker chooses victims dis-

embodied in laws and legal doctrines, the underlying assignment of responsibility is grounded in economics and incentives. For one, assigning liability affects economic efficiency: if an online platform operator isn't required to prevent malfeasance, other ways to fix the problem might entail far higher costs. (For example, outside investigators might lack the searching, filtering, and blocking tools a platform operator would enjoy; where a platform operator can simply remove harmful materials, an outsider would need to take more complicated and more costly steps to get the material removed.) Furthermore, assigning liability affects ultimate outcomes—if fighting malfeasance becomes more difficult, more malfeasance is likely to occur.

### ***The Communications Decency Act: Limiting “Publisher” Liability***

Consider Zeran's lawsuit against AOL after its users repeatedly posted defamatory messages. Had Zeran's attackers circulated their message through a local newspaper—taking out an ad or writing a letter to the editor—his case would have been an easy win under settled precedent. But online, some think the story has a different feel. If Zeran prevailed in his lawsuit against AOL, online publishers argued, the company would have to hire censors to review every message. Or perhaps it would just shut its online forums, making the Internet that much less useful.

Online service providers took their complaint to the US Congress. Their pleas were well-received: no congressman wanted to stand by while, in one view of the situation, a few thin-skinned complainers “broke” the Internet. In the 1996 Communications Decency Act (CDA),<sup>1</sup> a brief appendix instructed that

No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.

At first glance, this single sentence seems both simple and sensible. If AOL didn't write the text that harmed Zeran, it ought not be liable as publisher or speaker. But the CDA extends further than its plain language suggests. Suppose an online service provider shows a defamatory posting, presents a deceptive ad, or distributes a racially discriminatory housing listing. Each such posting, ad, or listing comes from an independent user, and the CDA has been interpreted to hold that the service provider therefore isn't liable. Even if the service provider knew of the problem with the offending message, and even if it reaped large profits from the offense, courts have found that the CDA extinguishes service provider liability. This contradicts typical intuition about service providers' responsibilities; most people assume providers must take action when they've been notified of a problem or when they profit from a disputed activity. But the CDA relieves online services from any such obligation.<sup>2</sup> So, not only does the CDA's liability rule change incentives for those who use the Internet to defraud, but the act also sways platform operators' behavior.

### ***Who's Responsible for Enforcing Copyright?***

Online services also create controversy when they distribute copyrighted content. From a user's perspective, watching the Daily Show or Southpark on YouTube is easy, convenient, and free. But to the companies that made these shows, unauthorized distribution is a real threat. If consumers can watch for free on YouTube, paid iTunes downloads become a poor

value. Same for high-priced ads on broadcast television. Without these payments, producing new shows could become unsustainable, threatening copyright's central purpose.

Content owners hesitate to pursue users who upload infringing materials to the many websites that redistribute them. Such users are numerous, hard to find, and can rarely pay even a fraction of the compensation that owners seek. Rather, content owners prefer to target the large distributors who store, index, and redistribute infringing material. At first glance, content owners might seem to have an open-and-shut case against these distributors. Sites such as YouTube and Dailymotion host thousands of infringements, often listing infringing clips as their “most popular” or “top” material. Infringements yield profits: popular infringing material attracts users who receive ads as they search and browse, ultimately yielding lucrative sales to investors and acquirers.

Here, too, a legal rule offers protection to sites even when their services facilitate infringement, affecting their incentives. The 1998 Digital Millennium Copyright Act (DMCA)<sup>3</sup> provides that an online service provider isn't liable for copyright infringement if the files at issue were placed on the system at independent users' direction, and if the service provider, on receiving knowledge of infringing activity, acts expeditiously to remove infringing files and doesn't receive a financial benefit directly attributable to the infringing activity.

DMCA protection's scope remains a subject of considerable dispute. Consider the requirement that a service provider remove infringing files it learns about. The DMCA's plain language is ambiguous as to what level of knowledge obliges a provider to take action. It instructs that a provider remove

specific files when it receives a complaint from an authorized copyright holder. But suppose the complaint comes from an ordinary

cently ruled in Google's favor on precisely this question,<sup>5</sup> though an appeal is ongoing, and other similar cases remain undecided.

### A reasonableness standard allows flexibility to consider the myriad facts that might indicate a service provider is more or less culpable.

member of the public? What if the service knows generally that its site offers infringing files? What if the service intends to host infringing files because infringement best speeds the service's growth?

These questions are more than hypothetical. Recently unsealed litigation documents provide a behind-the-scenes look at copyrighted content on YouTube. In 2005, for instance, YouTube co-founder Steve Chen urged colleagues to "concentrate all of our efforts in building up our numbers as aggressively as we can through whatever tactics, however evil"—indicating a willingness to tolerate copyright infringement. Steve's plan succeeded: when YouTube staff in 2006 examined "all the most viewed/most discussed/top favorite [videos] to try and figure out what percentage is or has copyrighted material, it was over 70%."<sup>4</sup> Before acquiring YouTube, Google harshly critiqued its approach. One manager commented that "YouTube's business model is completely sustained by pirated content," while another called YouTube a "rogue enabler of content theft."<sup>4</sup> It seems improper that YouTube might enjoy the DMCA's protection from copyright infringement, even when its staff intended to host infringing material, and even when Google acquired YouTube with full knowledge of YouTube's infringements. But in ongoing litigation, Google argues that it satisfies each of the DMCA's requirements and therefore must receive DMCA protection. A district court re-

#### Toward a "Reasonable" Approach

The CDA and DMCA both reflect a congressional attempt to apportion an economic burden between online service providers, users, and rights-holders. Place too much responsibility on service providers, and useful services become unprofitable. Ask too little of them, and the Internet devolves into chaos to the detriment of both users and rights-holders. Striking the right balance is no easy feat. But should Congress attempt this task at all?

I envision an alternative approach: online service providers should take action that is *reasonable under the circumstances*. I doubt that responsibility can be distilled to a single sentence, as the CDA attempts, but perhaps that's for the best. Legislation can't anticipate the unending variety of online service providers or the many variations in their uses and disputes.

To a layperson, the suggestion to require "reasonable" action might seem hopelessly vague. But courts have ample experience assessing the reasonableness of parties' actions. For example, courts evaluate reasonableness in every claim of negligence.

In most cases, a reasonableness standard would reach the same result as the CDA and DMCA. No reasonable approach could prevent a single libelous message on an online discussion forum, and a user seeking to hold a forum operator liable on those facts would fail on a reasonableness test just as under CDA. So, too, for run-

of-the-mill DMCA claims. Occasionally, users upload infringing files despite a service provider's reasonable efforts, and neither reasonableness nor the DMCA would hold the provider liable on those facts alone.

Some might object that service providers will respond by closing services. I disagree. For one, a stray harmful posting wouldn't create liability for a service provider; far more would be required to establish lack of reasonable care. Furthermore, a savvy service would add defenses—"report a bad post"—to identify harmful content with modest effort. Meanwhile, for the service distributing widespread harmful material without appropriate precautions, liability is the appropriate result; such a service *should* be liable.

Crucially, a reasonableness standard allows flexibility to consider the myriad facts that might indicate a service provider is more or less culpable. Consider the deceptive ad mentioned earlier that promises free ringtones but charges \$10 per month—a fact disclosed in print so small that few users would notice. The CDA seems to indicate that a user can't sue the search engine that distributes such an ad.<sup>6</sup> But a reasonableness standard would probably hold the contrary. After all, search engines already review the ads they show. Although a full examination might be expensive and unreasonable, a partial review could focus on categories such as "ringtones," where deceptive ads are widespread. Known-trustworthy advertisers could be exempt from unnecessary delays. Conversely, in light of the deception so prevalent in "free" offers, the provider could flag any advertiser promising free service for heightened review.

Ultimately, the prevailing understanding of reasonable care is that the costs exceed the benefits. This approach rings true in online malfeasance. Suppose a

search engine hires one full-time scam-hunting employee, at a fully loaded cost of perhaps \$100,000 per year. If that employee's first year of effort protects consumers from \$150,000 of scams—and I suspect the true benefit would be far larger—the employee's contribution was positive and highly desirable. More generally, whenever a service provider can, at modest cost, protect its users from a genuine and substantial harm, that's an effort we should ask the provider to accept.

And what of Zeran's experience? I doubt any reasonable AOL filter would have prevented the first libelous message that began his plight. But after AOL removed the first message, a reasonable filter might have noticed the striking similarity with the messages that followed. Suppose experts reported that automated software can easily find such similarities, that other services run such software, and that AOL could have installed such software at little expense. If so, a court might conclude that AOL's distribution of the subsequent messages fell short of reasonable care. In my view, that's an appropriate outcome: it puts responsibility on a party in a position to take action, protects would-be victims from unnecessary harm, and brings a modicum of law and order to an online environment that otherwise knows few bounds.

**W**hen browsing online, consumers deserve at least as much protection as when reading the newspaper or visiting a retail store. Existing statutes favor simplicity over fairness—gutting longstanding legal protections, favoring online businesses over their offline counterparts, and discouraging online services from offering protections even where benefits exceed costs. My focus on reasonableness would restore an

appropriate balance, encouraging service providers to protect their users and ensuring a healthy and safe online ecosystem. □

#### References

1. *Communications Decency Act*, US Code, Title 47, section 230, 1996.
2. *Zeran v. America Online*, *Federal Supplement*, 3rd Series, vol. 129, 1997, p. 327 (US Court of Appeals for the 4th Circuit).
3. *Digital Millennium Copyright Act*, US Code, Title 17, section 512(c), 1998.
4. *Viacom et al. v. YouTube et al.*, US District Court, Southern District of New York, Case No. 1:07-cv-02103, Viacom's Reply to Defendants' Counterstatement to Viacom's Statement of Undisputed Facts in Support of its Motion for Partial Summary Judgment, 4 June 2010, paragraph 95.
5. *Viacom et al. v. YouTube et al.*, US District Court, Southern District of New York, Case No. 1:07-cv-02103, Opinion and Order, 23 June 2010.
6. *Goddard v. Google*, US District Court, Northern District of California, Case No. 5:08-cv-02738-JF.

**Benjamin Edelman** is an assistant professor at Harvard Business School, where his research and teaching explore online businesses. Although he serves as an expert or attorney in some cases raising questions of intermediary liability, Edelman had no role in any of the cases discussed here. Contact him via [www.benedelman.org/mail](http://www.benedelman.org/mail).

**cn** Selected CS articles and columns are also available for free at <http://ComputingNow.computer.org>.



**LISTEN TO GRADY BOOCH**  
**"On Architecture"**

podcast available at **cn** <http://computingnow.computer.org>