
# Web Hosting Provider Liability for Malicious content

## Introduction

StopBadware has recognized that malware poses a threat to the open Internet, and that a large and growing share of malware is distributed via websites, often without the knowledge or consent of site owners. In response to this problem, StopBadware developed a set of best practices to guide web hosting providers in responding effectively to reports of malware websites on their networks. This whitepaper serves as a complement to the best practices. It uses U.S. case law to explore web hosting provider liability for hosting malicious content managed by customers, legal protection for restricting access to such content, and whether providers have an obligation to act when such content is reported.

## Disclaimer

Information in this paper is based on general principles of law in the United States and is intended for information purposes only; StopBadware makes no claim as to the comprehensiveness or accuracy of the information. Because the law can change quickly, portions of the paper may be out of date. In addition, the information may be accurate in one jurisdiction, but not accurate in another. You should use this paper as a starting point for further research. It is not offered for the purpose of providing individualized legal advice.

StopBadware is not your lawyer. Use of this paper does not create an attorney-client or any other relationship between the user and StopBadware or the Berkman Center for Internet & Society.

## The Communications Decency Act

In the United States, companies that offer web hosting services are shielded from liability for most content that customers or malicious users place on the websites they host. Section 230 of the Communications Decency Act, 47 U.S.C. § 230 ("Section 230"). protects hosting providers from liability for content placed on these websites by their customers or other parties. The statute states that "[n]o 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." Most courts find that a web hosting provider qualifies as a "provider" of an "interactive computer service."

Although this protection is usually applied to defamatory remarks, most federal circuits have interpreted Section 230 broadly, providing "federal immunity to any cause of action that would make service providers liable for information originating with a third-party user of the service."

*Zeran v. America Online, Inc.*, 129 F.3d 327, 331 (4th Cir. 1997). This protection exists only if the web hosting provider had nothing to do with the specific content. However, web hosting providers are in a unique position to address the problems presented by malicious content on hosted websites, created either by the customer running the site or by third parties who have infected the site owned by a customer. Many web hosting providers receive reports about malware residing on, or made available from, the websites of their customers. This paper discusses the legal obligations, under the federal laws of the United States, of a web hosting provider that receives notification about malware residing on a customer's hosted website.

## What a Web Host Likely *Can* Do

Under federal law, web hosting providers can take action to address such malware reports without legal liability (absent a contract with a customer that prevents interfering with the site). Section 230 states that a web hosting provider may take action "to restrict access" to a hosted site if it contains material that is "objectionable." In *Langdon v. Google, Inc.*, 474 F.Supp.2d 622 (D.Del. 2007), the court ruled that no providers should be held liable when taking action, in good faith, to restrict access to objectionable material under 230(c)(2)(A). We can therefore conclude that web hosting providers *can* act to address malware. But are providers liable if malware placed on their customers' sites by others ends up infecting other computers and doing damage?

## What about Malware?

Whether the Communication Decency Act's ("C.D.A.") protections extend to damage caused by malware is still largely an open question of law. One case appears to partially address this issue — *Green v. America Online*, 318 F.3d 465 (3d Cir. 2003). The court held that "information provided by another" as described in C.D.A. section 230 included "signals" sent by a computer program. The court concluded that the service provider couldn't be held responsible for the victim's computer receiving a "signal or program," from their service if it was sent by a third party and the hosting company had nothing do to with the program — it "would run afoul of the intention of section 230." 318 F.3d 465, 472–73. In the Third Circuit, then, web hosts are protected from liability if their hosted sites are a source of malware without the host's knowledge. No other case has confronted this question. Further, no other Circuit has found the term "information" to include a computer program under the C.D.A, but this ruling is the best indication of how future courts are likely to rule. *Green* reflects the current trend of legal thinking in this area. A web hosting company cannot be held liable for third party malware on a hosted website under this interpretation of the law. But what if the web hosting company receives a report about malware on one of their hosted sites? Are web hosts obligated to act on this information?

## No Obligation to Act

If an Internet service provider is notified of possible malware on a hosted site, that provider likely has no obligation to act upon this information. Section 230 does not require the removal of offending content when a provider is notified. In *Zeran v. America Online*, 129 F.3d 327, 333 (4th Cir.

1997), the Fourth Circuit determined that Section 230 immunizes a provider even if that provider has been notified of the defamatory material. The plaintiff in *Zeran* notified America Online ("AOL") about false postings on one of AOL's bulletin boards that resulted in hundreds of telephone calls to his home and place of business. The plaintiff alleged that AOL was liable for delaying removal of the postings and for failing to screen future posts. The Fourth Circuit noted that Section 230 was enacted, in part, to allow providers of web services to block and screen offensive material without fear of liability. The court found that imposing liability on a provider upon notice of objectionable material was contrary to Section 230. The result? AOL was protected by Section 230 and was not held liable. Like the *Green* ruling, this is a specific case from a single Circuit; therefore, this reasoning has not been confirmed in other jurisdictions.

## Conclusion… with a Caveat

The *Green* case indicated that malware is "information" under Section 230, and under the *Zeran* case, providers are under no obligation to remove allegedly harmful information. By the reasoning of these courts, a hosting provider is not likely to be found liable for failing to act if they are notified of malware on a site within their control. However, if a web host *promises* to act, then a web host can be held liable if the problem remains unaddressed.

In *Barnes v. Yahoo!, Inc.*, 570 F.3d 1096 (9th Cir. 2009), the court held that a host can be held liable for a breach of promise under Section 230. The defendant's employee in *Barnes* allegedly told the plaintiff that she would "personally walk the statements over to the division responsible for stopping unauthorized profiles and they would take care of it," but no action was taken to remove the allegedly false profile. *Barnes*, 570 F.3d at 1099. So if a provider informs an individual that content was to be taken down, that provider could be held liable if the content is not removed. Such a promise must be made very clear in order to be binding.

The Ninth Circuit indicated that such a promise should not be construed from a general monitoring policy from a provider, or even from specific attempts from a provider to assist an individual. Rather, such liability can be avoided, the court maintained, by disclaiming any intent to be bound by any such promise. So if a web hosting provider wishes to avoid the appearance of making any promises regarding reports of malware on sites it hosts, it should include a disclaimer in any response to reports of malware, clarifying that it is not promising to take any particular action. This is a good idea in any event, since someone who reports malware is probably not a customer of the web hosting provider, and may not be aware of any applicable Terms of Service conditions or the limits of the web hosting provider's liability.