DOI:10.1145/3722549

Brett Danaher, Jonathan Hersh, Michael D. Smith, and Rahul Telang

Opinion
Fighting Crime Online

Options, evidence, and the empirical case for judicial site blocking in the U.S.

THE INTERNET HAS been a transformative technology, facilitating the exchange of information and allowing for the decentralization of commerce. The benefits of these features have been well documented.

However, digital platforms—and the decentralization they facilitate—have also allowed illegal activities to flourish online. Internet platforms such as Craigslist have increased prostitution and sex trafficking activities by 17%,[4] dark-web drug marketplaces such as the Silk Road have facilitated the trafficking of drugs and other illegal substances,[6] and file-sharing platforms have facilitated the illegal exchange of copyrighted media.[10]

In theory, illegal activities such as these should be easier to police in digital spaces given the ability to collect and analyze large-scale data. In practice, illegal activities have flourished online due to the anonymity provided by digital platforms, the decentralized nature of Internet interactions, the low costs involved in setting up and switching to new illicit sites, and jurisdictional challenges in holding foreign websites accountable for violating domestic laws.

Here, we discuss the empirical evidence on the effectiveness of various methods of enforcement against criminal behavior on the Internet, synthesizing results from several distinct categories of crime. We then discuss why some methods are more effective than others in reducing illegal activities. We conclude by arguing that judicial website blocking, a method deployed in numerous stable, rights-respecting democracies worldwide, has been shown to have several desirable properties in fighting online criminal activities, and within the bounds of a carefully crafted framework we outline here, could be used safely and effectively in the U.S. as well.

Enforcement Against Internet Crimes

Information systems researchers have categorized online enforcement efforts into two broad areas: demand-side and supply-side. Demand-side enforcement seeks to reduce consumers' motivation to consume illegal content by targeting consumers with education, fines or other legal deterrents. In contrast, supply-side enforcement seeks to reduce consumers' ability to consume illegal content by targeting the suppliers of illegal goods and services, aiming to make it more difficult for them to provide illegal content.

Demand-side enforcement. Demand-side enforcement measures include anything that targets the users or consumers of illegal sites online, such as changes in government policy and penalties toward such users, or high-profile lawsuits against individuals using illegal sites. Several papers have found that demand-side enforcement can be effective at reducing piracy and increasing paid legal consumption of music, but that their effectiveness can wane if enforcement grows lax over time.[1,8] Enforcement of demand-side policies can be difficult to maintain due to the expense of targeting a large number of users. Demand-side policies also can be politically unpopular if they are viewed as invasive or curtailing Internet privacy. As such, demand-side enforcement in some cases has economic properties that are less desirable than those of supply-side policies.

CREDIT TK

Supply-side enforcement. Supply-side enforcement generally takes four main approaches: shutting down sites, increasing a site's legal liability for hosting infringing content, requiring sites to remove infringing content upon request from a rightsholder, and blocking access to structurally infringing sites.

Site shutdowns typically involve months of effort and can coordination across law enforcement agencies in multiple countries. For example, the FBI spent months building a case against the popular drug trafficking site The Silk Road, and many more months coordinating with authorities in the numerous countries where Silk Road mirror servers were housed before they were able to seize these servers and shut down the site. Similarly, the shutdown of the pirate site Megaupload involved months of coordination between the U.S. Department of Justice and law enforcement agencies in eight different countries.[a]

Although site shutdowns could potentially affect behavior, they are vulnerable to a phenomenon dubbed the "hydra effect." The hydra effect occurs when content on, and traffic to, the shutdown site disperses to existing or newly created substitute sites faster than those sites can be shut down.

For example, research has found that, because of the hydra effect, the shutdown of the Silk Road had little impact on the rise of online drug trafficking over time;[b] the shutdown of Backpage caused no observable decrease in the number of consumers visiting online commercial sex advertising sites;[11] and the shutdown of Kino.tv, an illegal video streaming site, caused no increase in legal consumption of motion picture content.[2]

Another supply-side approach involves increasing the legal liability for sites and individuals who knowingly facilitate criminal activity. For example, the FOSTA-SESTA law in the U.S. allows sites to be held legally liable for knowingly facilitating sex trafficking. In response, many online commercial sex advertising platforms began more actively policing their sites to remove posts and users suspected of trafficking, and one working paper found this reduced the number of transactions involving underage providers.[12] A related study found that when authorities arrested several illegal drug sellers on a major drug trafficking site, it led to a reduction in the number of sellers and drug transactions on that site.[5]

As digital technologies become more powerful, their benefits and potential harms grow, making platform regulation increasingly important in the future.

A third supply-side approach requires sites to remove infringing content after being notified by rightsholders. This "notice and takedown" approach has been effective in the context of e-book sales.[9] In a quasi-experimental research study, books that experienced targeted copyright protection via takedown notices sent to Google and Yahoo! saw a 14% increase in sales relative to a group of control titles where no notices were sent.

A notable challenge with both the increased legal liability and notice and takedown approaches is that their effectiveness is limited when websites are located internationally. For example, the FOSTA-SESTA law increases legal liability for websites located in the U.S. but has no impact on foreign sites. Similarly, under U.S. law Google and Yahoo! incur legal liability if they do not respond to notice and takedown requests from U.S. rightsholders, but international search engines would not.

With the fourth main supply-side approach, website blocking, legal authorities direct Internet service providers (ISPs) to not resolve the domain names of infringing sites and alert the user the site is being blocked. The advantage of this strategy is that it does not require the arrest of individuals, or the seizure of physical servers, located in foreign countries. Domestic ISPs simply block access to infringing sites hosted internationally, obviating the need to coordinate with foreign authorities. Thus, website blocking can scale more easily and rapidly to target many international sites than would be the case with site shutdowns, increased (domestic) legal liability, or notice and takedown requests.

Research in the piracy literature has shown that, when deployed at sufficient scale, website blocking can reduce piracy and increase legal consumption. Researchers have shown that blocking access to a single piracy site, The Pirate Bay, had little impact on legal media consumption because of the hydra effect.[7] However, several studies have demonstrated that the simultaneous blocking of multiple piracy sites can decrease total piracy and increase legal consumption.[7,c] In short, for blocking to be effective it must disrupt the ability of the hydra to regrow its heads. It is reasonable to assume that these results extend to other online crimes beyond media piracy, such as the sale of counterfeit goods, illegal drug marketplaces, and websites that facilitate sex trafficking. Moreover, the threat of website blocking may provide incentives for the platforms themselves to more effectively police illegal activities on their sites.

Website Blocking as an Enforcement Tool in the U.S.

As digital technologies become more powerful, their benefits and potential harms grow, making platform regulation increasingly important in the future. While this Opinion column discusses media piracy alongside illicit drug sales and sex trafficking, new technologies such as 3D printing and AI-based image generation will allow other illegal or harmful activities to be facilitated online. For example, today individuals can download patterns to 3D print working firearms without going through the legal process of becoming licensed to own one.[3] Similarly, in 2023 NCMEC's CyperTipline

a U.S. Department of Justice. Justice department charges leaders of Megaupload with widespread online copyright Infringement. (2012); https://bit.ly/3G1Uevo

b RAND Europe. Taking stock of the online drugs trade. (2016); https://bit.ly/3RHqqqy

c The impact of online piracy website blocking on legal media consumption. SSRN (Mar. 2024); https://bit.ly/4id8XRJ

received 4,700 reports of Child Sexual Abuse Material (CSAM) created with generative AI tools.[d] A December 2024 *60 Minutes* investigation into Clothesoff.io, one of the most popular online "nudify" services, showed the site intentionally masked its true location, listing an invalid address in Buenos Aires, Argentina.[e]

Given the limitations of existing demand-side enforcement policies, and the difficulty enforcing many supply-side policies on websites located internationally, the empirical evidence suggests that website blocking has a number of desirable properties in fighting online criminal activity.

Of course, website blocking should not be taken lightly. The ability to block domestic access to foreign websites raises significant procedural and free-speech concerns—concerns that were major reasons the SOPA-PIPA Act did not pass Congress in 2012.

That said, a lot has happened since 2012. On one hand, we have more information about the individual and societal harms caused by piracy, sex trafficking, drug trafficking, and other illicit activities facilitated by online platforms. On the other hand, there are many rights-respecting democratic governments that have enacted judicial site-blocking measures. These countries include Canada, the U.K., much of E.U., Australia, Brazil, India, and South Korea. The specifics of the laws in these countries vary, but they generally follow six main principles, which we believe are a useful framework for other democratic countries considering site-blocking legislation:

Lawful: Blocking is administered by a court, or an administrative authority overseen by the court. Prior to blocking any site, the court or administrative authority conducts a careful judicial review to verify the site in question is in violation of the blocking legislation.

Targeted: Blocks are limited to sites that are "structurally infringing" or whose "primary purpose" or "primary effect" is facilitating illicit activity (rather than sites hosting only some infringing content). Blocking is also limited to foreign-run sites outside the jurisdiction of the court.

Proportional: Website blocking is carefully calibrated to balance the demonstrated harm potential of the website against the potential impacts on free speech and lawful commerce, while also considering the overhead and expenses imposed on ISPs.

Transparent: Decisions of the court or administrative authority are transparent to site owners, site visitors, and the public at large. Where feasible, site owners are notified before the block goes into effect, and given an opportunity to appear before the court to oppose the order. Users visiting blocked sites are redirected to a landing page explaining the reason and judicial authority behind the block, and where they can direct concerns, questions, or appeals. Finally, the court or administrative authority makes its blocking decisions available for public review.

Limited: In addition to the opportunity for immediate redress discussed above, courts provide ways in which sites that are no longer structurally infringing can be removed from blocking.

Flexible: ISPs are given flexibility in the technical measures they use to implement the blocks, as long as the implementation is sufficiently effective.

As noted previously, the experience in these countries shows that, within such a framework, website blocking can be implemented in a way that is effective at reducing illicit activity without harming free speech or impeding legal commerce.

The U.S. is notably absent from the list of rights-respecting democratic governments that have adopted judicial website blocking. However, one measure of the changes that have occurred in the 12 years since SOPA-PIPA is that in March 2025 Representative Darrell Issa and Representative Zoe Lofgren, two legislators who strongly opposed SOPA-PIPA in 2012, introduced legislation and organized industry round tables toward enacting judicial site blocking in the U.S.[f,g]

Given the known and increasing harms associated with illicit activities facilitated by online websites, the limitations associated with existing demand- and supply-side measures available to U.S. authorities to fight crime, the empirical evidence of site blocking's effectiveness, and the examples from other countries that have safely enacted judicial website blocking legislation, we believe now is the right time for legislators in the U.S. to give serious consideration to incorporating judicial website blocking legislation into the U.S. laws as a way to address online illegal activities that harm U.S. citizens and businesses. C

References

1. Adermon, A. and Liang, C.Y. Piracy and music sales: The effects of an anti-piracy law. *J. Economics 122*, 2 (2014).
2. Aguiar, L., Claussen, J., and Peukert, C. Catch me if you can: Effectiveness and consequences of online copyright enforcement. *Information Systems Research 29*, 3 (2018).
3. Basra, R. The world's most popular 3D-printed gun was designed by an aspiring terrorist. *Wired* (2024); https://bit.ly/3G1UpXA
4. Chan, J., Ghose, A., and Seamans, R. The impact of Craigslist on prostitution trends. *Information Systems Research 28*, 3 (2017).
5. Chan, J. et al. Shedding light on the dark: The impact of legal enforcement on darknet transactions. *Information Systems Research 35*, 1 (2024).
6. Christin, N. Traveling the silk road: A measurement analysis of a large anonymous online marketplace. In *Proceedings of the 22nd International Conference on World Wide Web*. ACM (2013).
7. Danaher, B.et al. The effect of piracy website blocking on consumer behavior. *Management Information Systems Q. 44*, 2 (2020).
8. Danaher, B., Smith, M.D., and Telang, R. The effect of graduated response anti-piracy laws on music sales: Evidence from an event study in France. *J. Industrial Economics 62*, 3 (2014).
9. Reimers, I. Can private copyright protection be effective? Evidence from book publishing. *J. Law and Economics 59*, 2 (2016).
10. Rob, R. and Waldfogel, J. Piracy on the high C's: Music downloading, sales displacement, and social welfare in a sample of college students. *J. Law and Economics 49*, 1 (2006).
11. Zeng, H.S., Danaher, B., and Smith, M.D. Internet governance through site shutdowns: the impact of shutting down two major commercial sex advertising sites. *Management Science 68*, 11 (2022).
12. Zeng, H. *Sound of Freedom Trilogy: Responding to the Rise in Human Sex Trafficking Facilitated by Digital Platforms*. Doctoral dissertation. Heinz College, Carnegie Mellon University (2024).

Brett Danaher (danaher@chapman.edu) is an associate professor of economics and management science at Chapman University, Orange, CA, USA.

Jonathan Hersh (hersh@chapman.edu) is an associate professor of economics and management science at Chapman University, Orange, CA, USA.

Michael D. Smith (mds@cmu.edu) is the J. Erik Jonsson Professor of Information Technology and Public Policy at Carnegie Mellon University, Pittsburgh, PA, USA.

Rahul Telang (rtelang@andrew.cmu.edu) is the Trustees Professor of Information Systems at Carnegie Mellon University, Pittsburgh, PA, USA.

d National Center for Missing and Exploited Children. Generative AI CSAM is CSAM (2024); https://bit.ly/4jtvWJj

e Marks, N. et al. AI "nudify"' sites lack transparency, researcher says. (2024); https://bit.ly/3XTnNFE

f Frank, M. My chat with Rep. Darrell Issa, new Hollywood friend. (2025); https://bit.ly/4jniLtb

g Lofgren, Z. Rep. Lofgren introduces targeted legislation to combat foreign online piracy that preserves the open Internet. (2025); https://bit.ly/4lhGhts