



Institute For Policy Innovation

ISSUE BRIEF

PROTECTING PROPERTY RIGHTS ON THE WEB:

THOUGHTS ON THE PROTECT IP ACT

by Tom Giovanetti

Because intellectual property protection is critical to the U.S. economy and serves the interests of a secure and content rich Internet ecosystem, it is reasonable and within the realm of sound policy to discretely target rogue websites through a Protect IP Act that preserves due process and other legal protections while not creating undue compliance burdens and legal liability for third parties.

Synopsis

Over the centuries, civilized societies have learned that certain behaviors are harmful and destructive, and so societies have set up structures and institutions, both voluntary and compulsory, in order to encourage behavior that is beneficial to society, and especially to discourage behavior that is harmful to society.

Introduction

Civilized societies don't tolerate theft, abuse, predation and violence, and so society has developed rules and institutions to restrain such negative behavior to the degree possible. There is a range of opinions about the degree to which society should attempt to restrain or influence the behavior of its citizens. Statists think government should have a large role in manipulating behavior, while libertarians think government should only maintain the basic structures necessary for the protection of liberty and the facilitation of commerce. But relatively few people argue for anarchy. Almost everyone recognizes that basic levels of protection for life and property must exist for civilized society to survive and flourish.

The Internet has changed a lot of things, but it hasn't changed human nature. Indeed, the Internet seems to have "turbocharged" human nature, facilitating dramatically increased levels of human connection, to largely beneficial but occasionally harmful ends. In addition to the Internet's remarkable ability to connect people with people, products, services, and ideas, the anonymity afforded by the Internet has served to particularly facilitate the activities of those with more nefarious intentions.

Given our understanding of how necessary basic protections are for civil society to flourish in the analog world, it would be very strange to argue that the best way for on-line society to flourish is to carve out the Internet as a zone free of such basic protections in the digital world.

Nefarious Behavior On-Line

We are all acquainted with the problem of nefarious behavior on the Internet. Viruses and other malware cause financial and productivity losses to individuals and businesses. People's lives are damaged by financial scams, phishing, and identity theft. Anonymity and digital distribution facilitate harassment and bullying to a degree never before possible. Unfortunately, bad actors are also able to find support, community and opportunity on the Internet.

Almost everyone recognizes that it would be better if we could limit these harmful online practices through a combination of technological solutions and legal structures that carefully target the harm without causing a host of unintended consequences. No one wants the myriad benefits of the Internet to get unintentionally caught up in a wave of enforcement, but of course that's no different than in the analog world where, ideally, law enforcement targets illegal behavior without unnecessarily inconveniencing the vast majority of law-abiding citizens.

If someone sets up a website intended to facilitate identity theft, an illegal scam operation, or the proliferation of harmful malware, it does not seem unreasonable that structures should exist that help eliminate that threat while maintaining all the due process protections that characterize our legal system.

The Threat of Piracy and Counterfeiting Online

In addition to all of these other harmful and destructive threats in the digital world, sometimes people set up websites specifically intended to distribute illegal pirated or counterfeit products.

In the analog world, we don't tolerate piracy or counterfeiting. Imagine how long you'd stay in business if you set up a brick and mortar storefront and hung a banner outside that said "Get all your illegal goods here!" Odds are your store would be shut down in relatively short order.

Similarly, in cities where certain streets are known as havens of "bargain goods," law enforcement sweeps through as often as their resources allow, sending the purveyors of counterfeit goods skittering into the shadows, or to another street corner.

At our borders, customs officials are constantly inspecting, interdicting and seizing shipping containers full of counterfeit goods. And federal law enforcement is constantly prosecuting large scale counterfeiting networks.

There's a reason for all this attention—piracy and counterfeiting are NOT "victimless crimes." The victims include the owners, manufacturers, distributors and retailers of legitimate goods who lose out on legitimate sales, and the employees of such industries who lose their jobs and economic prospects as a result of counterfeits.

Indeed, the economic costs of copyright piracy alone are staggering. According to IPI research, copyright piracy costs the U.S. economy annually more than 373,000 jobs, \$16 billion in lost earnings, and \$3 billion in lost state, federal and local tax revenue.¹

1. Stephen E. Siwek, "The True Cost of Copyright Industry Piracy to the U.S. Economy," Institute for Policy Innovation, Policy Report #189, October 2007.

But the victim is also the purchaser. You may not care that the heavily discounted purse or watch you've just bargained for is actually counterfeit, but what if your prescription drug or electrical breaker box or brake pads for your car are counterfeit? All of these products are *commonly* counterfeited, and if you're the unfortunate consumer of such goods, you're likely to experience loss, harm, or even death at the hands of the counterfeiters.

Legitimate Role of Government in Protecting Property Online

Much of what the federal government does today is in excess of its original Constitutional limitations, or is at least in excess of that which was envisioned by the Founders. But it's clearly the job of government to facilitate the protection of life and property, and to prosecute illegal activity.

The protection of property rights is essential because property rights are the foundation of a just society and of a functioning market economy. You can't have a just society without property rights, because without property rights, there is nothing stopping the powerful from trampling the weak, or the rich from trampling the poor. The property right gives power to the poor and to the weak.

And you can't have a functioning market economy without property rights. You certainly can't have contracts if no one can be certain who has the right to contract for the disposition of specific goods and services. Without property rights, markets just don't work.

Intellectual property rights are equally important, for all the same reasons that tangible property rights are important. Intellectual property is specifically protected in the U.S. Constitution (Article I, Section 8) because of the Founders' recognition of its importance in driving creativity and innovation. Additionally, IP rights help to ensure quality and safety through trademark brand protection, reputation, and accountability. Behind IP goods stand owners who are identifiable and can be held liable, while criminals lurk anonymously in the shadows behind pirated and counterfeit goods.

So, if we recognize the threat to our economy, to our health, and to our overall well-being posed by pirated and counterfeit goods, and if we recognize that it is a legitimate role for government to facilitate the protection of property rights, why should the Internet be set aside as a zone safe for the marketing and distribution of pirated and counterfeit goods? Is there something in the essential nature of the Internet that demands that there be no attempt to impose basic legal protections for those who participate in the online world?

To our benefit, the Internet has disintermediated business models that existed because of "analog friction," and has exposed other unnecessary and outdated government restrictions, such as laws against alcohol being sold across state lines. Additionally, the Internet has made possible entirely new models that can only exist because of the broad reach of digital distribution and the low marginal cost of setting up a business. We have benefited from these innovations brought about by the Internet revolution, and we assume that the Internet will continue to play a constructive role in a better future for the world.

But the Internet also makes it easier and cheaper than in the analog world to commit certain types of crime like counterfeiting and piracy. A "storefront" can be set up on the Internet in a matter of hours and with relatively little investment, which is obviously very different than the analog world. In the anonymous world of the Internet, it's easier to hide, or to do business with a false identity. In the analog world, law enforcement can literally padlock your front door, but in the Internet world, it's easy to pick up and move your Internet storefront to another server, or even to another country.

Our “analog” public policy should be influenced by what we have learned from the streamlined, disintermediated gains of the Internet. Policy lessons learned from the Internet should, for instance, convince us that there should not be laws and regulations that prohibit sales of insurance products across state lines or the practicing of medicine across state lines. But shouldn’t our digital public policy also be informed by what we have learned from the basic legal protections of civil society?

On this issue of preventing the harm of piracy and counterfeiting over the Internet, the question is whether a legal structure can be set up that narrowly targets these “rogue websites” distributing pirated and counterfeit content without otherwise inhibiting existing Internet functionality and continued Internet innovation. If so, that would seem a worthy pursuit.

The Protect IP Act

In recognition of the problem of piracy and counterfeiting in the digital environment, several pieces of legislation have enhanced the ability of law enforcement agencies to combat these illegal activities.

The very successful Digital Millennium Copyright Act of 1998 (DMCA) and the recent PRO-IP Act of 2008 have given lawmakers tools to combat online piracy and counterfeiting for websites hosted within the reach of U.S. law. The track records of both laws demonstrate that they have succeeded in carefully targeting illegal behavior without creating hardships or unintended consequences for the Internet ecosystem. So U.S. law enforcement officials already have tools to deal with rogue websites hosted domestically. But, of course, rogue websites residing on offshore servers or otherwise hosted by overseas companies remain safely outside the reach of these U.S. laws. And we’re all familiar with how easy it is to move a website to an offshore server in order to escape the reach of domestic law.

Figure 1

Visitors to websites whose domain names have been seized under existing U.S. law see this notice. Go to <http://dvdorderonline.com> to see it live.



But while U.S. law cannot compel compliance for websites hosted offshore, U.S. law could compel domestic Internet Service Providers (ISPs) to block access to such websites, and could further cut such websites off from payment processing services, search engines and advertising networks, if such a law existed.

Ideally, such a law would:

- narrowly target websites that exist solely or primarily to distribute illegal content,
- preserve due process legal protections for website registrants,
- ensure the application of safe harbor provisions for ISPs and others as modeled by the DMCA,
- not create burdensome compliance obligations for ISPs or others,
- preserve an appeal process for targeted website registrants.

That's the intent of the Protect IP Act, which is currently working its way through the legislative process. While no one believes that any law can entirely eliminate online distribution of pirated and counterfeit goods, the Protect IP Act would at least create a legal structure for blocking access to websites determined to be dealing in counterfeit medicines and consumer goods, pirated books, movies, music and software.

The Protect IP Act as introduced in the Senate has been refined from a previous version introduced in 2010. Additionally, a House version is anticipated which will differ in some substantive ways from the Senate version. Then, of course, the two bills will have to be reconciled.

Our analysis, therefore, consists of the aforementioned arguments in favor of protecting IP online and the goals of such legislation, and attempts to answer criticisms that have been lodged against not only the Senate legislation but also the overall intention of the Act.

Issues Related to the Protect IP Act

As one might expect, a broad coalition of companies and associations representing the content industries support the Act, as does the U.S. Chamber of Commerce, which represents more than three million businesses of various sizes across the United States.

But of course, some objections have been raised to the Act.

There is an aggressive movement most often described as the “free culture” movement that is skeptical of the entire intellectual property legal and economic framework. While some proponents argue that there should be no legal concept of intellectual property, most give begrudging assent to some idealized version of intellectual property but almost always find themselves opposed to any specific implementation of IP protection.

Free Culture Movement

It is therefore unsurprising that the free culture movement and its sympathizers would oppose the Protect IP Act, and this explains the opposition of such groups as Free Press, Public Knowledge, Electronic Frontier Foundation, Free Software Foundation, and others. IPI has often characterized the free culture movement as a belief in communism for knowledge goods. While this may seem to some as red-baiting, in this case it isn't, as the founder of Free Press, Robert McChesney, is an avowed and unapologetic Marxist.²

Political conservatives are rightly suspicious about giving the federal government additional powers of any type, and the specter of giving the federal government the power to “shut down websites” has animated some conservatives' opposition. Essentially their concern is that somehow powers granted through the Protect IP Act would be extended such

Conservative Suspicions

2. Many sources reflect McChesney's avowal of socialism and Marxism. See John Fund, “The Net Neutrality Coup,” *The Wall Street Journal*, December 21, 2010.

that the federal government would shut down websites because of political speech or content that the federal government found objectionable. Some have expressed the sentiment that the Protect IP Act is a “power grab” that would give the Obama administration a tool to shut down the websites of political opponents.

Associated with this concern is the idea that if the United States reserves the right to block websites proven to distribute illegal content, this will make us “just like China and Iran.” But this is a rather shallow and cynical analysis. The Protect IP Act is designed to *protect* property rights, to *enhance* commercial markets, and *will protect due process and free speech rights*. That is not “like China or Iran” in any way.

It’s important to remember that the federal government already has the legal tools to shut down websites hosted within the United States that have been proven to exist for the purpose of distributing illegal content. These legal tools are narrowly tailored to focus on websites solely or primarily existing to distribute pirated or counterfeit goods, and preserve the due process protections afforded American citizens. We are not aware of any instance where websites have been shut down by federal action because of political speech under the existing legal framework.

Under the Protect IP Act, the Justice Department would be required to obtain a court order in order to proceed. The Justice Department must demonstrate that the site is directed at U.S. consumers and harms holders of U.S. intellectual property. And the Department would be required to serve notice of the action promptly.

The current iterations of the Protect IP Act are at least as narrowly targeted as existing legislation and preserve the right of due process. We see no potential within the Protect IP Act that it could be used as a tool to stifle political speech.

Private Right of Action

The Senate version of the Protect IP Act contains a private right of action that has concerned many observers. Typically a private right of action is a boon to trial lawyers and the cause of an avalanche of lawsuits, so such suspicions are not without merit. In the Protect IP Act, it seems unlikely that the private right of action would stimulate a rash of trial lawyer-driven lawsuits because there is no pot of money at the end of the rainbow, since the Protect IP Act is about blocking access to websites rather than monetary damages.

Protect IP only allows rights holders to seek injunctive relief against rogue sites that evade U.S. jurisdiction. There are no damage awards, only the ability to ask that a U.S. court direct advertisers, search engines and/or payment processors to not service rogue sites.

Nonetheless, given the concerns that have been expressed over the private right of action, we expect the language in the bill related to the private right of action will be modified to allay those concerns. We are unconvinced that the private right of action as implemented in the Senate version is critical to accomplishing the goals of the Protect IP Act.

“Breaking the Internet”

A group of venture capitalists has expressed concern about the Protect IP Act,³ claiming that it “endangers the security and integrity of the Internet,” among other things. They mention their concern about the private right of action, as discussed above, and mention the Digital Millennium Copyright Act (DMCA) as a balanced (“though flawed”) approach to dealing with infringing content. Similar arguments have been made by a group of Internet engineers along more technical lines.

3. <http://www.usv.com/2011/06/the-protect-ip-act-will-slow-start-up-innovation.php>

It's safe to say that technologists have generally been unsympathetic to the concerns of IP rights holders in the history of such disputes. Indeed, Paul Vixie, one of the Internet engineers who has objected to the Protect IP Act, has said, "Most new domain names are malicious. Everyday lots of new names are added to the global DNS, and most of them belong to scammers, spammers, e-criminals and speculators." This led Mr. Vixie to design a system for blocking malicious websites through the DNS system. But Mr. Vixie opposes the Protect IP Act not because he thinks it will "break the Internet," but because "I simply cannot agree that this level of perturbation is warranted for the protection of intellectual property." In other words, he doesn't think IP protection is important enough to warrant intervention.⁴

Similarly, venture capital investors will always be inclined toward fewer restrictions, rather than more restrictions, on possible business models. On this concern we are generally sympathetic but not specifically sympathetic in the case of the Protect IP Act. The restrictions in the Protect IP Act exist only to aid in the prosecution of activity already defined as illegal within U.S. law.

It's also fair to point out that, in 2005, the National Venture Capital Association made similar arguments to the Supreme Court arguing in support of Grokster in the important *MGM vs. Grokster* case. The result of the *Grokster* decision has been an explosion in new and profitable business models related to the distribution of legal content (much to the benefit of venture capitalists) and not the harmful results predicted by the VC community.⁵

It seems that technologists and venture capitalists are easily activated to oppose copyright protections, while they conversely are almost entirely dependent on patent protection for their livelihoods and for mitigating the risks of their venture investments. Nonetheless, as policymakers draft the final versions of the Protect IP Act, it's important that they consider valid technical concerns in order to avoid harmful unintended consequences.

Internet service providers (ISPs), payment processors (VISA, Mastercard, etc.), search engines and advertising networks all have concerns that the Protect IP Act will create harmful legal liabilities for them and will otherwise expose them to unreasonable compliance costs and enforcement burdens.

In general, these are not illegitimate concerns. For a vital and functioning Internet ecosystem, it is important that the entire Internet community work together to ensure that the Internet ecosystem works to the benefit of those who participate responsibly in it. One part of the ecosystem cannot simply shift its problems onto the backs of others.

Content owners and rights holders must work with rather than against ISPs, payment processors, advertising networks, and search providers to ensure that Internet users are not victimized by those who would take online advantage of them, including purveyors of pirated and counterfeit goods.

But specifically, in the case of websites demonstrated to exist for the purpose of profiting from the distribution of illegal content, it is also not unreasonable to expect those who facilitate access to and commerce with these sites to play a role in limiting their reach.

Because the final text of the legislation is not yet available, or indeed has yet to be introduced in the House, we can only say that we think the Protect IP Act is on its way to becoming an agreement that accomplishes the important goals outlined earlier while not burdening third parties with unnecessary liability and compliance costs, and we urge all stakeholders to work toward that end.

4. George Ou, "DNS Filtering is Essential to the Internet," High Tech Forum, June 24, 2011. <http://www.hightechforum.org/dns-filtering-is-essential-to-the-internet/>

5. <https://www.eff.org/deeplinks/2005/03/mgm-v-grokster-venture-capital-speaks>

Conclusion

Too many people today are still afraid to do business over the Internet. For some, the Internet is still a digital “back alley” where they fear to tread. Unfortunately, with nefarious behavior such as phishing scams, viruses and malware, credit card hacking theft and the abundance of pirated content online, there is more to be done in order to attain an Internet ecosystem that is as reliable as possible.

Along these lines, we are encouraged by the newly announced Copyright Alert System, designed in conjunction with the major copyright content companies and trade associations, as well as with five of the U.S.’s largest Internet service providers. This voluntary system is designed to identify illegal content and to provide notification to consumers that their accounts are being used to access illegal content without creating new liability for ISPs.

This same cooperation can work toward the construction of a Protect IP Act that accomplishes its important goals. We believe that such an Act would benefit both producers and consumers of IP goods and thus benefit the U.S. economy. Further, we believe that the more securely we are able to protect creative goods online, the more we facilitate new and exciting business models for the creation and distribution of creative goods.

Everyone has an interest in an Internet that is secure, safe, and rich with content that is easily created, and easily and legitimately accessible—everyone except criminals who profit from theft and gaps in law. A Protect IP Act, carefully crafted and appropriately targeted at illegal activity, will be a useful tool that enhances rather than harms Internet engagement and commerce, to the benefit of all Internet users.

About the Author

Tom Giovanetti is president of the Institute for Policy Innovation (IPI), a public policy research organization based in Dallas, Texas. Mr. Giovanetti represents IPI at the World Intellectual Property Organization (WIPO), where IPI is an accredited NGO, and at the UN’s Internet Governance Forum (IGF). Tom has published numerous op/eds and policy studies on a wide variety of topics including tax reform, intellectual property, Social Security personal accounts, telecom reform, Internet governance, the broadband revolution, and out-of-control government spending, and testifies often before state and federal legislative committees.

About IPI

The Institute for Policy Innovation (IPI) is a nonprofit, non-partisan educational organization founded in 1987. IPI’s purposes are to conduct research, aid development, and widely promote innovative and nonpartisan solutions to today’s public policy problems. IPI’s focus is on developing new approaches to governing that harness the strengths of individual choice, limited government, and free markets. IPI is a public foundation, and is supported wholly by contributions from individuals, businesses, and other non-profit foundations.

© 2011 Institute for Policy Innovation

IPI Issue Brief is published by the Institute for Policy Innovation (IPI), a non-profit public policy organization.

NOTE: Nothing written here should be construed as an attempt to influence the passage of any legislation before Congress. The views expressed in this publication are the opinions of the authors, and do not necessarily reflect the view of the Institute for Policy Innovation or its directors.

Direct all inquires to: Institute for Policy Innovation,
1660 S. Stemmons Freeway, Suite 245
Lewisville, TX 75067
972.874.5139 (voice) 972.874.5144 (fax)
email: ipi@ipi.org