The DMCA & ACTA vs. Academic & Professional Research: How Misuse of this Intellectual Property Legislation Chills Research, Disclosure and Innovation

Authors

Tiffany Rad

and

Christopher Mooney

Introduction

Fair use, reverse engineering and public discussion of research encourage innovation and self-regulate industries. However, these principles, which define our vibrant and creative marketplace, are fading. If professionals cannot constructively critique another's research online without being burdened with takedown notices until the critique is obscured or functionally removed for long periods of time, we do not have a society from which we can learn from others' mistakes and improve our professions. The Digital Millennium Copyright Act (DMCA) is increasingly being used in ways that chill free speech, disclosure of security vulnerabilities and innovative research. If the ACTA (Anti-Counterfeiting Trade Agreement) is passed, many countries will experience similar intellectual discourse chilling effects as we have in the United States.

Three hypothetical situations presented (below) are examples of how multiple and repetitive DMCA take down notices can be used in a similar way in which a DoS (denial of service) attack paralyzes an online service.

The Unfair Corporate Advantage:

You run a software company. You and a competitor are about to launch similar products in the marketplace. If your company is quick, you will have the advantage of being first to market. However, your intellectual property is similar to, but not the same, as your competitor's. Your ISP (Internet Service Provider) is flooded with DMCA takedown notices regarding your new software's source code. Most, if not all, of your company's site is removed by your ISP. The day planned for launch, you have no online presence. You miss being first to market.

Silencing Discussion of Security Vulnerabilities:

You are a security researcher. You are _$B!G_ and are racing another researcher with a similar vulnerability disclosure. Because you are all about the 0-day, to slow down the other researcher, you file multiple DMCA take down notices to his ISP. You decide to let the ISP sort through whether or not the take down notices are legitimate; you are not a lawyer, right? As a result, his blog, social networking accounts and his company's site are down. You post your 0-day.

Chilling Online Critique:

You have been injured by the scientific and medical techniques implemented by a physician. This doctor has written numerous books and has appeared on television shows advocating this medical technique. You would like for other doctors and patients to know that something went wrong with your treatment and encourage scientists to figure out why. On your blog, you and other medical professionals discuss the application of the technique and whether or not it is safe. Utilizing proper fair use techniques, you take short snippets of the doctor's books, properly attributed, and post them on your blog for critique. Your blog -- and all critique mentioning this doctor's name -- is offline because your ISP has received multiple and repetitive DMCA take down notices. As a result, no one can discuss online anything negative about this doctor or his techniques.

Are these hypothetical situations fact or fiction? Christopher Mooney, Director and co-founder of Project DoD and Tiffany Rad, pro bono attorney for Project DoD, posit that these hypothetical situations are based upon actual experiences by Project DoD and our clients. As a result of the takedown notice issues for predominately non-infringing online speech, we will discuss why data havens -- some in anticipation of enactment of the ACTA -- are becoming more popular and what ISPs, companies with an online presence and the legal profession can do to mitigate the chilling effects of the DMCA's over-broad take down notice provisions.

Who is Project DoD?

Project DoD has been running a censorship resistant hosting project for twelve years. Project DoD is a volunteer managed open source project with a handful of developers. All volunteers participate in their spare time and DoD.net pays the bills entirely with 501(c)(3) donations.

In today's hosting environment, the more controversial the content, the more likely it will be silenced as a result of Internet censorship. Project DoD resembles a censorship-resistant service provider because it cares more about the principle that all members of society deserve just and equal access to speak their minds than it does about profit margins.

Background of Project DoD v. Federici:

A little over a year ago Project DoD, one of its users, and one of its upstream providers started receiving DMCA takedown notices from a group of individuals bent on silencing Advocates for Children in Therapy (ACT), an organization composed of activists and psychologists trying to stop the practice of attachment therapy. As it turned out, ACT had allegedly been chased around the Internet by Ronald S. Federici et al. based on a claim that ACT was violating his copyright and the copyright of his colleagues. ACT was bounced from both small and major hosting providers because of these DMCA 512 infringement notifications, and the organization was never once given the option to file a counter notice.

Other ISPs' decisions to drop hosting of ACT's website presumably originate from the fact that the DMCA seeks to tie the ISP's liability to the content upon notification of infringement. Takedown notifications are not simply a cease and desist against the user, but an implicit threat on behalf of the notifier that the ISP may be sued for its user's content. If a user files a counter notice, the ISP must continue to keep the content down for about ten days but may suffer further liability on behalf of its user if the content is not restored within fifteen days.

If the ISP follows all of these legal procedures, which require time taken away from their employees' core competencies, they may still suffer baseless threats from either party. Remember, there is no judicial oversight of this entire process. In order for either party to have their day in court, the DMCA has forced the ISP into the position of arbitrating this legal dance, which is at best time-consuming, and at worst a total blunder that leaves the ISP liable for damages to one party or both. We have made blog postings about this problem and its implications on free speech before, but that is minimal analysis compared to what one might find on sites like the EFF (Electronic Frontier Foundation), Public Knowledge, Chilling Effects, or simply by following **#DMCA** or **#ACTA** on Twitter.

As if to add insult to injury, the tool to prevent abuse by either party is section 512(f), which allows the ISP to collect damages and attorney fees if either the notice or counter notice was misrepresented. This provision amounts to more lawyers, more time, more money, and as we are finding out, it is often a huge battle simply to choose jurisdiction (which is likely to be a nightmare with the ACTA).

The Details

The violation about which our analysis is based was a page with a list of properly cited quotes, that were/are quite clearly fair use. What's more, our friends at the EFF, with their work on Lenz vs. Universal, recently got a judge to state that fair use must be considered before takedown notices are sent. These findings go a long way to giving provision 512(f) teeth for any ISP willing to stand up against abusive takedown notices, but do not guarantee that an ISP is willing to go through the process of defending its users. In fact, the deck is stacked so far against the ISP and its users that there have only been a handful of 512(f) claims filed in the last ten years despite rampant abuse.

Project DoD's involvement with this case started when Mr. Ronald S. Federici sent an incomplete takedown notice for a list of properly cited quotes from his book. Project DoD honored the initial takedown notice, but realized it was incomplete when ACT expressed their intention to file a counter notice. DoD.net apologized to all parties and requested clarification on the elements of notification from Federici and restored ACT's content.

We now strongly recommend that all ISPs possess a full understanding of what elements of notification are required by a takedown notice, and request clarification for incomplete notices. While Mr. Federici insisted that DoD.net shut down their entire website, the elements of notification define the exact content that is claimed to be infringing. What is more, it provides key conditions that may be contested by either the user or the ISP in a counter notice or 512(f) claim.

At this point, Mr. Federici put together the proper elements of notification and we forwarded that to ACT. The content was removed from advocatesforchildrenintherapy.org, and ACT filed a counter notice maintaining that their use of the content was fair. In order for Project DoD to comply with the safe-harbor conditions of the DMCA, we were then statutorily required to keep the content down for ten days.

This is one of the worse possible requirements of the DMCA. Without any judicial oversight, someone can send a takedown notice to an ISP, and in order for the ISP to not be liable — even if the user contests the notification — they must keep the content down for ten days. In the computer security world, we call this a Denial of Service (DoS) attack.

After DoSing ACT's content for ten days, Project DoD started to receive takedown notices from other people listed on ACT's site that followed the same template as the Federici notices. It is clear to us that there was collusion behind the scenes, and after all was said and done, we received six other takedown notices from individuals listed on the childrenintherapy.org homepage. Similar to the Federici takedown notice, we requested clarification on the elements of notification where necessary and took ACT's content down for each 512 notice received. For over a full month there was some part of the ACT site that had the word "REDACTED" written all over it because of this abuse.

While the content was down, Project DoD and its upstream provider, Silicon Valley Web Host, received harassing communications threatening further legal action if the content was restored as required by the statute. The process of dealing with every complaint was time consuming, to say the least, and these individuals were sending additional complaints via email on a daily basis that we needed to forward to our counsel for review. What is more, they severely strained our relationship with our upstream provider and nearly had every site we host go dark as a result.

We cannot demonstrate with more clarity what it means to be a member of a hosting collective that puts its mission and members above profit. In the end, we survived the assault and moved on to pursue technological solutions that would help prevent attacks on free speech in the future.

Unfortunately, about six months later, we received another takedown notice from Mr. Federici for the same exact content, but this time the communication came through his attorney. Again, both Project DoD and our upstream provider were assaulted and again the content was exactly the same despite the consolidation of the domain name, from **advocatesforchildrenintherapy.org** to **childrenintherapy.org**. ACT, controls both domains, but they had put in a redirect for the advocates domain to the shorter childrenintherapy domain.

Enough was enough! Project DoD's members consulted with the EFF to discussed what options we had at our disposal, and the conclusion was obvious: provision 512(f). The EFF backed our upstream provider, while Project DoD's attorneys Tiffany Rad and Craig Dorais found additional attorneys, Robert Mittel and Rufus Brown, to assist with the case.

Common Abuses for DMCA Takedown Provisions

The following provisions constitute, at very least, protocol failings in DMCA-takedown style laws. We will be using the U.S. DMCA as the use case to demonstrate both the abuse theory and some real world examples of abuse. Taken together, it should be made clear that, whether intentional or not, the takedown provisions of the DMCA favor the alleged right holder over the alleged infringer.

Fair Use is Not a Magic Bullet

Up until the summer of 2008 when Lenz v. Universal addressed fair use in DMCA takedowns, it was nearly impossible for one to mount a defense against fraudulent DMCA takedown notices for failing to consider fair use.

A counter notice must make the assertion that the original takedown is a not the alleged right holder's copyright, and Lenz v. Universal gave an alleged infringer a direct path to resist DMCA abuse by stating that fair use must be considered as a necessary pre-condition to comply with the elements of takedown notification. This finding has proven not to be the magic bullet one would think.

The problem here is that fair use is complicated, and is often handled on a case-by-case basis, since the details vary from case to case. This difficulty to prove fair use means abusers may still send takedown notices with little legal risk, especially since having a case go to court to make a determination of fair use is exceedingly rare. Under the U.S. DMCA, the person filing a counter notice, or the ISP, may file a 512(f) claim stating that the alleged right-holder is misrepresenting his or her copyright by failing to consider fair use. Additionally, both in our experience and statistically, 512(f) is exceedingly difficult to use.

There is a major jurisdictional problem with 512(f). If an alleged infringer or an ISP wants to employ 512(f) as a defense against takedown abuse, it is looking more like they will not get to choose a home venue. For example, if Alice wants to sue Mallory, her home venue likely does not have personal jurisdiction over Mallory, which means Alice has no choice but to challenge abuse in Mallory's home venue. This unfortunate situation is problematic for the alleged infringer because she must now find representation in an unfamiliar jurisdiction and bear the burden of fighting a case over a great geographic distance. For this reason, the authors have first hand experience with Maine throwing out Project DoD v. Federici for lack of jurisdiction.

It should be noted, however, that Maine's decision in Project DoD v. Federici might not hold in every jurisdiction. There is a theory, espoused by Eric Goldman, Associate Professor at Santa Clara University School of Law and Director of the High Tech Law Institute, that if the alleged right holder engages in a campaign of harassment against that this "should easily qualify under the Calder v. Jones 'Effects Test' of expressly targeting harms towards the victim." [1] While we believe the Project DoD v. Federici case to be an excellent example of how hard it is to mount a 512(f) defense using fair use, even after the Lenz v. Universal finding, it is far from being the only time we have seen fair use violated with DMCA takedown notices.

In April of 2005, two of Project DoD's users, Daniel Papsian and an anonymous user, made a parody sites of Walmart Foundation's website and the 700 Club website called walmart-foundation.org and the700-club.com respectively. These sites were not only a clear parody -- which anyone could see from reading the sites' articles -- they were produced as part of a subversive media class at Carnegie Mellon University as a satirical commentary on the two organizations.

Both sites were only up for about two weeks before Project DoD received DMCA takedown notices; first for the Walmart Foundation parody, and then for The 700 Club parody. These incidents are a prime example of how the DMCA has effectively put a great deal of power into the hands of the alleged rights holder and how this can have disastrous consequences on censorship. In both cases, Project DoD's users struggled with the option to file a counter notice since their work was clearly fair use. On the other hand, there is no way to prove this until one has entered the court system which would mean, if litigated, these users needed to argue this point in court against all the legal might of Walmart and The 700 Club.

The state of fair use protection in the U.S. has been reduced to having enough money to defend one's fair use of a work in the court systems. Additionally, similar to Project DoD v. Federici, one must fight this in the alleged right holder's venue; in order for the ISP to maintain its Safe Harbor protection, it must still take the content down unless a counter notice is filed. Even in the highly unlikely event that a counter notice is filed, the content must stay down for the statutory waiting period of ten days.

Statutory Waiting Period, or Statutory Denial of Service Attack

The next abuse case should support our supposition that the DMCA was framed to favor the alleged rights holders rather than the alleged infringer. Upon receipt of a counter notice, in order for the ISP to maintain its Safe Harbor, the content must stay down for a statutorily required ten business days.

In effect, when combined with the Safe Harbor incentives for the ISP to make no judgments on the user's content, this provision amounts to a statutorily required denial of service attack against the user. It is not hard to surmise what happens if an attacker takes advantage of this abuse vector and, likewise, what happens when a mass of anonymous attackers abuse this same vector.

This paper began with three hypothetical situations regarding how easy it would be to knock a competitor's website offline. However, there are other examples one can think of including taking down a protest organizer's page before an event or even silencing political decent before an election. This provision is arguably the smoking gun of the DMCA.

While other economic conditions incentivize ISPs to avoid the counter-notice process by simply kicking the user off their service, this provision explicitly denies a just and balanced outcome if the ISP allows the user to file that counter notice.

But that is not all this provision has in store. It also requires that the user's content be restored within fifteen days of the counter notice. This begs the question: is the ISP also liable to the user if the content is not restored before that time? If that is combined with a requirement to keep the content down for ten days, and we are left with a five day window for the content to be restored after the ten day denial of service. It is no wonder ISPs are simply removing users from their service.

Project DoD saw one additional tactic when dealing with the Advocates for Children in Therapy site that we believe was intended to leverage the ten day statute to DoS ACT and induce fatigue for Project DoD in hopes that we would abandon our user. After Mr. Federici filed his takedown against ACT and was informed of the counter notice, there was a consorted effort on behalf of Mr. Federici and his colleagues to send six more takedown notices -- each censoring different portions of the ACT site -- over a period of about two months. This is the DoS attack.

Back Door Takedowns

This is a topic with which Project DoD has a long history of handling: back door takedowns and their negative consequences. Project DoD has been around for twelve years which means we have had plenty of opportunities to hop from provider to provider. The most common reason we have switched providers is because of back door takedowns.

Despite the fact that Project DoD provides a designated agent to deal with DMCA takedown requests as required by the statute and the content resides on our servers, the de facto process for sending an ISP a takedown notice is to contact the registered netblock owner in ARIN. This process often leads to our upstream provider receiving the takedown notice and usually results in that provider erroneously handling the DMCA notice despite our objections. The end result is that, even with service providers that are willing to stand up for a user's rights, control is slowly migrating up the chain to a smaller and smaller number of providers.

This migration, however, is not necessary. So long as the content simply passes through the Providers network, this helps all upstream providers enjoy the common carrier ISP classification. Likewise, this means that they need not comply with the takedown and counter notice dance. Project DoD strongly encourages small and large ISPs to take the following steps in order to prevent back door takedowns:

1) Make sure to file every ISP's copyright agent with the copyright office;

2) (Applicable if you are a small ISP do not host sensitive content on virtual private servers) There is an indication that responsibility for DMCA takedown notifications falls to – among other things – the organization in control of the hardware where the alleged infringing material resides;

3) Due to the fact that the de facto standard to find the controlling ISP has become a whois lookup against ARIN, try to get a proper CIDR netblock and register smaller ISP's organizational information with ARIN;

4) Lastly, if you're an upstream ISP and you receive a takedown notice for content hosted on a clients server that has gone through steps one, two, and three (above), maintain your common carrier status with the alleged rights holder and encourage them to send the notice to the designated agent for your client's server.

These steps should reduce the types of conflicts that Project DoD has run into with its upstream providers over the years, but still may not protect you against a determined abuser.

Project DoD has had too many cases of backdoor takedowns, DMCA and otherwise, to discuss them all here. In one of our more interesting cases, one of DoD.net's original users, HackBloc.org, had posted email communications about a man's scheme to entrap collective members. This man sent the takedown to Above.net, who was two hops up from dod.net at the time. Above.net insisted Project DoD remove the material and sent that demand to our collocation provider, who then forwarded it on to us.

Above.net is a large backbone provider. Having them arbitrate the takedown process is almost equivalently as dangerous to free speech as media consolidation in the news industry. Project DoD was left no choice but to comply with Above.net demands and asked HackBloc.org to remove the related section of their zine. HackBloc replaced the section with a small bit of information about what had happened and the DMCA takedown notice itself.

Above.net then received another takedown notice for the original DMCA takedown notice, but rather than recognize this second notice as abusive, they threatened to shut our service off, and by transitivity the service of all our users, if we allowed our user to continue "this game of wack-a-mole". More importantly, Project DoD would have stood up for the user on this second notice, but Above.net chose to exercise control over our statutory right to arbitrate the DMCA on behalf of our user.

Today, Dod.net has a more functional relationship with our upstream provider in San Jose. In Project DoD v. Federici, Mr. Federici attempted to employ back door takedown techniques after dod.net had successfully gone through the takedown and counter notice process. Mr. Federici sent the same DMCA takedown notice to Silicon Valley Web Host (SVWH), Project DoD's San Jose upstream provider, and through the four steps outlined above, and the support from the EFF, SVWH was able to assert their status as a common carrier.

The Endless Chain Attack

One would assume that if the entire takedown notice and counter notice process was followed to completion, that there is no reason or need to comply with another DMCA takedown notice for the same exact content. This conclusion may be drawn from the ten-day statutory waiting period.–One only has to imagine what would happen if a takedown notice were periodically sent every ten days for the same exact content; this would mean perpetual downtime for something the framers of the DMCA clearly intended to come back up.

As it turns out, this is another time-consuming vector for abuse. Since the ISP shares liability with the user for the content, it is up to the ISP to rigorously inspect each additional takedown notice to make sure it does not contain a potentially new violation. If one adds this to the mounds of work ISPs already have to go through to deal with DMCA takedown requests, it should slowly become more and more obvious why most for-profit ISPs opt to remove their users rather than support the counter notice process.

Project DoD was blindsided by this attack the first time Mr. Federici sent us a repeat takedown notice. In fact, it was our disdain with this abuse of process that motivated us to file the lawsuit, Project DoD v. Federici. Nevertheless, the tactic required us both on the second repeat notice, and the third repeat notice, to spend a bunch of time making sure each element of notification in the new DMCA takedowns was exactly what it was in the first one.

Leveraging a 512(g) Counter Notice to Identify a User

Part of the elements of notification requires the alleged rights holder provide:

> v) A statement that the complaining party has a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law.
>
> (vi) A statement that the information in the notification is accurate, and under penalty of perjury, that the complaining party is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed. [2]

This statement means that the alleged rights holder may hide behind an agent working on his or her behalf. Also, the same sort of language is used in section 512(h), which covers subpoena requests to the ISP from the alleged rights holder. In fact, this section clearly states that:

> (1) **Request.—** A copyright owner or a person authorized to act on the owner's behalf may request the clerk of any United States district court to issue a subpoena to a service provider for identification of an alleged infringer in accordance with this subsection. [2]

The wording that the owner may request "the clerk or any United States district court to issue a subpoena" should demonstrate an intention to require court intervention before releasing personally identifying information about the alleged infringer. However, any such wording to allow an agent to act on behalf of the alleged infringer, or to protect the alleged infringer's personally identifying information is conspicuously absent from subsection 512(g), which is required if the alleged infringer wants to restore access to his or her content. This detail is not lost on those who would leverage the DMCA to side-step court intervention for a subpoena.

In a separate case on Project DoD, a user exists who, coincidentally, also criticizes the practice of attachment therapy. This user has specifically requested that their personally

identifying information remain private for fear of retribution. This user displayed an NBC video demonstrating some of Mr. Federici's holding techniques to compare them with a practice called "face-down take-down", which has been shown to be potentially lethal.

Mr. Federici filed a DMCA takedown notice for the fair-use of his illustrations, and added that the "Author of [the] blog can write [a] counter-notification, with actual name and address in order for us to respond legally". Project DoD's user, for fear of retribution, chose not to file a counter notice that would potentially release this identity. To this day, that particular criticism of a proposed method of therapy remains censored in the United States for this reason. The user chose to instead put the video up on a service called Video Weed, which is not hosted in the United States.

The Primary Chilling Effect

The largest failing of the DMCA takedown provisions is that the entire subsection is intended to tie the ISPs liability to the content that it hosts with no court intervention. If one analyzes disputes between two parties (the alleged rights holder and the alleged infringer), these parties are the ones that are going to be able to make the most passionate arguments about the publication of that content.

Instead, as we have shown so far, the takedown provisions show that the balance is tipped, on almost every subsection, towards the alleged rights holder. This injustice holds true at the highest level of the takedown statute by making a disinterested third party -- most of which are motivated by profit -- primarily responsible for the content by tying that third party's liability to the content as a contributory infringer.

The problem here is that profit motivated online service providers, in a market with very thin margins, are possibly the worst candidates one could choose to arbitrate such disputes. One only has to consider the time and effort it takes to comply with all statutes, the additional time to deal with the abuse cases listed above, and the ISPs exposure to financial liability to understand why most ISPs choose to censor their users upon receipt of a takedown notice.

Project DoD has users that have been kicked off of Network Solutions, GoDaddy, Bluehost, WordPress, and a whole set of small providers that, for brevity, we are unable to enumerate here. Remember, Advocates for Children in Therapy was kicked off multiple hosts, including Network Solutions, before landing on Project DoD.

While the censorship of the users above is awful, they were all able to find a new home with Project DoD. This convenience, however, does not exist for some of the most popular content distribution mechanisms on the Internet. Today's social networks exist under one company and have a resilience against decentralization for two reasons.

First, there is not, at the time of this writing, a production ready decentralized social network. Second, even if that network were to exist, the success of a social network is

heavily tied to the number of users one can connect with. For this reason, our current social networks are likely to remain under the control of a small number of companies for the immediate future. One must ask: what happens when a user of one these services receives a DMCA takedown?

These services are no different from other online service providers. They make the same calculations about profit and they have also chosen to censor their users. The major problem is that when these users are censored, there is no other hosting option for the user. The content is taken down, and without a responsible counter notice policy, it will remain unavailable on such networks.

A Project DoD user was able to host with Project DoD when kicked off of Bluehost, but when he was kicked off of Twitter and Facebook, he had no other options. The combination of DMCA-style takedowns, and a lack of consumer choice results in disastrous consequences for free speech, while creating a whole new classification of censorship.

Fixing the DMCA

So what can be done to resolve the DMCA's take down abuses? We can take one of two approaches: We can solve it through the courts and the legislative system or we can try to solve it through direct action. Arguably, the former requires we work within the system, and the later leverages technology to bring about change in that system.

Suggestions for amendments to the Act include:
1) remove provisions like the ten day denial of service attack;
2) include privacy protection for a counter notice;
3) establish consequences for back door takedowns;
4) explicitly declare that fair-use must be considered as part of the elements of notification;
5) remove ISP responsibility for repeat DMCA notices or for and notice received from a bad-faith actor, or;
6) remove ISP liability for the content which would reduce copyright infringement to the same status of every other law in the U.S.

In short, we simply need to restore the balance between the alleged infringer and the alleged rights holder.

Technology will set us Free

There are two broad ways that technology may be leveraged to defend against censorship or initiate copyright reform. One technical solution will show how to protect the anonymity of a service provider so that they cannot be leveraged as tools to censor society and the other solution is a hybrid approach that will show how to resist censorship using the most common protocols for providing access to information while addressing jurisdiction hopping.

Censorship Resistance Through Technology

There is a very interesting use case of Tor that can provide non-standard Internet Service Providers a way to protect their anonymity while providing a service. Tor has the ability to provide hidden services to other Tor users, and while the protocol details are beyond the scope of this white paper, it is worth noting. The major limitations of such a service are that it will only be fast for small burst of traffic, the user must get service information out-of-band from a directory, and both the service provider and Tor user much have software capable of routing traffic through the Tor network.

So what if users cannot be expected to use Tor? First, let us say that we are unaware of any service protection model -- like Tor hidden services -- that address the problem of providing society with a service platform that is both censorship resistant and accessible by standard users over standard protocols. That is to say, most users lack the technical sophistication to connect to a Tor Onion router, access a directory service (x.y.onion), and request that service, let alone abandon their fast Internet services for something encumbered by the relay and rendezvous dance.

We need to clarify that we are impressed by the Tor hidden service protocol and can think of countless applications that make it a worthwhile project to support. If a protocol you are thinking of implementing or deploying has low bandwidth requirements and the details of the onion network and directory service can be hidden from the end user of your application, then we would strongly recommend using the Tor hidden service protocol. On the other hand, Project DoD is trying to solve the specific issues illustrated by our takedown censorship examples earlier. This means we are expecting to have users that lack the technical sophistication, or patients, to use Tor to access content over standard protocols.

Project DoD's problem is a hard one to solve considering service nodes are almost always tied to a specific location. We are dependant upon DNS resolution for name lookup and people expect access to any service to be equally as fast as comparable services.
To limit the scope of this discussion, we are simply trying to solve the problem of providing society (for free) with quality access to censorship-resistant hosting. While the principles may extent to many different services, it is easy to talk about the details in specific terms and apply those principals more generally later. So why not just move all content to Sweden (or some similar data haven) and be done with trying to solve the problem? The short answer is, because that is not completely satisfactory.

The real problem is that every country has a different set of rules and regulations that affect an individual's liberty in spectacularly beneficial and detrimental ways. Those laws that infringe on one's freedoms should have their equal right to disgust the population, jolting people out of apathy and into action. In addition, there is a real technical reason to want to provide services that are geographically closer to the population using them.

As demonstrated, the DMCA takedown provisions in the US have a statutory ten-day denial of service clause. When people get served a DMCA takedown notice, and then file a counter notice, it would be nice if their content automatically shifted to another country, and the site would just come back up in the US after a configured amount of time.

Consider the following. In specific terms, we have user content being provided through some service (http) and we believe that content should remain up through both technical and legal assault. As a side-note, while there is plenty of content that is decidedly illegal in most countries, we are aware of a huge set of content that has become a casualty of other laws. This is the content that suffers as a side-effect of copyright law or other such laws that abusers employ to censor content.

Before assumptions are made regarding Project DoD attempting to create an infrastructure that could be used to host pirated copies of the latest blockbuster movie, please understand that this is not the intent. The asset we are trying to protect looks a lot more like the content in Project DoD v. Federici than pirated movies or music.

Distribution of Responsibility and Isolation of Control

Organizations and individuals are governed by their country's laws. While no government or court should order an organization to censor content that is out of its jurisdiction, sometimes they do. No single organization should be the vanguard of these ideas nor have the last say in content provided by a censorship resistant infrastructure. In short, we are proposing that no single organization or individual is in control of the infrastructure.

An elegant solution would be to have a group of individuals, organizations, or companies, each with a different set of driving ideals, each subject to different laws, but all committed to being part of a world that is free of censorship. Furthermore, we think it's clear that no single organization or individual should have it within their power to censor content outside of their control. This begs the question of what such organizations or individuals are in control of. For now, let's call this physical asset a server "cell." We chose the word "cell," because, just like in guerilla resistance, we believe there should be no single strategic asset to attack.

Redundancy of Data

In general terms, it is ideal to prevent the loss of any one physical server or cell from causing downtime. The risk is clear: either through confiscation, attack, or hardware failure, the content should stay up. For these purposes, this again reminds us of the principal that there should be no strategic asset to attack in order to silence content. If one were to confiscate a single server, and that server had the only copy of a user's data, it is a failure of the infrastructure to protect the user. This creates a need for an infrastructure to have data replication over geographic boundaries, while, at the same time, be resilient enough not to suffer downtime from a single server loss.

Horizontal scalability in both server and software design is a hard and sometimes impossible problem to solve for certain data sets. Normally horizontal scalability is something desired by high volume environments, but the principals behind the concept may also gain high availability over geographic regions, and thus censorship resistance. The software engineering communities working on cloud computing and databases have been trying to move everything into this elastic paradigm for a few years now. What this means is that there is no longer a master slave model for data access and replication, and at very least if there is still a need for the master slave paradigm to accommodate the data model, that slaves should exist in different jurisdictions. Additionally, failover from master to slave should be trivial.

If you add the additional constraint that this horizontal scalability replicates over jurisdictional boundaries, we have a system that can scale with popularity and usage but that is also resilient to failure of any single node or server. It should be noted that this design requirement is ideal for a censorship resistant infrastructure but that the details of implementation are very different for each data set. One only has to look at the CAP theorem, which states that it is impossible for a distributed system to simultaneously provide Consistency, Availability, and Partition tolerance at the same time in order to understand that some constraints (like consistency) may need to be relaxed for certain data sets. In short, we can summarize this requirement simply saying the following: in order to make the data resilient against downtime, one should try to make applications that access such data scale horizontally over large geographic distances.

A Resource Should have Jurisdictional Resilience

Building upon the principal that Project DoD has redundancy of data and distribution of responsibility as well as isolation of control, because we are still trying to protect a user from experiencing downtime, it is important to also consider the risk that a singular jurisdiction imposes on the user or the "cell" operator.

There may be multiple organizations or individuals controlling distinct cells under one jurisdiction. This is true for Project DoD's development platform, which controls nodes in both San Jose and Oakland, California. Considering this fact, what are the risks and solutions at the granularity of someone who controls a server cell or a user that wants to self-censor content in a particular jurisdiction?

To answer this question, imagine we have a resource, foobar.com, and that a DMCA-style takedown law causes the cell operator to have to deny access to the content permanently or for some configurable amount of time. The operator needs the ability to disallow service to a particular resource in order to comply with certain jurisdictional restrictions. Taking such an action would prevent the content from being served from that particular server cell, and if that server cell happened to be the master data node for a user, that master access would be transitioned to another cell. Progressing one step further, none of that user's data should reside on that particular node any longer. This additional stipulation creates a disincentive for law enforcement to disrupt other users by

issuing a subpoena for the content or simply confiscating the servers. Why limit this control to just the Administrator?

As it turns out, there are plenty of reasons to provide the user with this level of control, too. For example, perhaps the user wants to release information in a hostile jurisdiction but does not want to be at risk of subpoena, and he knows that this information will likely put the cell or its operator at risk. Clearly, the user should also have the ability to choose which server cells he or she would like to provide service from.

In summary, this requirement means that at any given time, either the cell administrator or the user can choose not to provide access to content at any given time. For the administrator, this means any cell that he has control over and, for the user, this means any possible cell that is part of the infrastructure. One can also derive from this requirement that, because there is a risk of server cells going down without prior warning, content must always be in more than one jurisdiction at a time. At very least, this provides a mechanism for manual intervention to restore a user's content.

There are certainly many more vectors for exploit, but the above requirements are a necessary starting point for a censorship resistant infrastructure. Additionally, limiting the scope of development puts us closer to a censorship resistant infrastructure that can be used and improved upon.

Conclusion

Fair use and reverse engineering have been the stalwarts of innovation, but these are becoming increasingly difficult to do without facing litigation under the DMCA. Additionally, fair use associated with critiquing professional, scientific and technical procedures/processes is integral to self-regulating professional industries. If you cannot discuss these topics using fair use of copyrighted material without your upstream ISP being overburdened with copious takedown notices, innovation will be stifled.

More often than not, ISPs eagerly remove content challenged by takedown notices because the risk of making a mistake is costly; they have a tendency to err on the side of caution and remove the material promptly to avoid losing their valuable DMCA Safe Harbor protection. As a result, information such as disclosures -- including those related to security vulnerabilities -- may become extremely difficult to share.

Sharing ideas is the basis for innovation and a way in which society may correct logical, scientific, and societal errors and document the requisite changes. A delicate balance exists between granting limited protection with intellectual property laws while, at the same time, being sure that access to the work is achieved. However, it is often forgotten that the purpose of intellectual property protection is to share information, not to lock it down forever.

The DMCA was not intended for the purpose of chilling online speech, but it is. Similarly, it is being used for business market advantages as well as to silence critique.

As a result, there is an increasing appeal for online anonymizers that technologically mask identity and geographic location. Where do you file takedown notices if the country in which the content resides does not have similar intellectual property laws? It is predicted that international data havens in locations where the DMCA and/or ACTA are not laws and content-specific jurisdiction hopping will increase financial revenue and Internet traffic through those more liberal countries, principalities or sovereign nations.

Just short of legislation allowing for government mandated Internet filtering and censorship, the DMCA and the ACTA are -- or will be -- used for those purposes. If the DMCA is not redacted or amended and/or the ACTA is passed, online free speech and critique will, most likely, still find a way to be heard, but through technological hacks instead of through easily-accessible public forums. Even today in the U.S., webhosting organizations like Project DoD cannot exist without a tireless Director and pro bono attorneys who are mavens for the 1st Amendment.

When you add the equation of for-profit service providers to the ease with which content may be removed permanently with lack of court intervention even in some of the most abusive cases, society is ripe for censorship abuse at the hands of corporations, powerful interest groups and every troll with a laptop connected to their local coffee shop wifi.

References:

1. http://blog.ericgoldman.org/archives/2009/12/512f_claim_dism.htm
2. http://www.law.cornell.edu/uscode/html/uscode17/usc_sec_17_00000512----000-.html