



The Best and Worst Internet Laws

Date: Apr 20, 2007 By [Eric Goldman](#).

Over the past dozen years, the lure of regulating the Internet has proven irresistible to legislators. For example, in the 109th Congress, almost 1,100 introduced bills referenced the word Internet, and hundreds of Internet laws have been passed by Congress and the states. This legislative activity is now large enough to identify some winners and losers. In the spirit of good fun, Eric Goldman offers an opinionated list of personal votes for the best and worst Internet statutes in the United States.

Over the past dozen years, the lure of regulating the Internet has proven irresistible to legislators. For example, in the 109th Congress, almost 1,100 introduced bills referenced the word "Internet." Although this legislative activity doesn't always come to fruition, hundreds of Internet laws have been passed by Congress and the states. This body of work is now large enough that we can identify some winners and losers. So in the spirit of good fun, I offer an opinionated list of my personal votes for the best and worst Internet statutes in the United States.

Best Internet Laws

With my libertarian leanings, it should not be surprising that my list of good Internet laws is both brief and skewed toward laws that minimize the scope of Internet regulation.

2: [Internet Tax Freedom Act](#)

Many people mistakenly think that this law eliminated sales tax for purchases over the Internet. It didn't (if you don't pay sales tax, you owe use taxes on those purchases). Instead, the law placed a temporary moratorium on states enacting Internet access taxes or e-commerce-specific taxes. By freezing new taxes, the law forestalled a tax frenzy during the dot-com boom. The current moratorium expires in November, but Congress is proposing to extend the law permanently (see the Permanent Internet Tax Freedom Act of 2007: [S. 156](#) & [H.R. 743](#)). To which I say amen!

1: [47 USC 230](#)

This law was enacted in 1996 (as part of the [Communications Decency Act](#), discussed below) during the heyday of the cyberspace exceptionalism movement—about the same time as [Barlow's Declaration of Independence](#) and Johnson/Post's [Internet self-governance article](#). Indeed, this law is one of the most conspicuous examples of how a legislative body has set different rules for physical space and cyberspace. In this case, the law provides websites and other intermediaries a near-absolute immunization from liability for their users' content—even if offline publishers would be liable for publishing the exact same user content in dead trees.

It's hard to overstate the importance of this law to the Internet's evolution. Without this law, all Internet content probably would be subject to a notice-and-takedown regime like we have for copyright law (see discussion about the DMCA Online Safe Harbors below). If websites had to remove user content upon notice to avoid liability, they would act conservatively, quickly pulling down complained-about content without much fuss. So, any company unhappy with negative consumer comments could simply contact the web host, claim that the comments were defamatory (making the web host potentially liable for the content), and expect the web host to scramble to take down the user's comment.

But in this takedown melee, only negative remarks would be targeted (there would be

no legal grounds—or reason—to target positive comments). Thus, notice-and-takedown rules would result in "lopsided" databases in which only positive opinions/commentary would remain, but many negative comments could be quickly excised. This would ruin the capability of the consumer opinion sites (for example, eBay's feedback forum and Amazon product reviews) to hold people and companies accountable for their choices. Indeed, by undermining the credibility of Internet content generally, a notice-and-takedown scheme could diminish the Internet's vitality as a mainstream information resource.

47 USC 230 eliminates the notice-and-takedown option for people and companies trying to escape accountability. As a result, 47 USC 230 is a big part of the reason why the Internet has been such a massive success.

Effective but Questionable Internet Laws

Two laws are noteworthy for substantially accomplishing their intended goals, even though I can't classify them as "good" because of their deficient policy rationales.

2: [No Electronic Theft Act](#) (NET Act)

In 1997, Congress changed the basic paradigm for criminal copyright infringement. Previously, the law required that defendants had to infringe for the money. The NET Act expanded the scope of criminal law to cover both commercial and non-commercial infringers.

Specifically, the NET Act targeted warez traders, a group of hobbyist infringers who aggregate and disseminate copyrighted works as trophies—by finding and publicly presenting a hard-to-get copyrighted work, the warez trader demonstrates his/her prowess as a trader and earns recognition from the community. Warez traders generally subscribe to the "information wants to be free" philosophy, so they never exchange copyrighted works for the money, but their trading can have adverse consequences for copyright owners.

There are many reasons why [the NET Act is lousy policy](#), most importantly because criminal sanctions [do not deter warez traders](#). Yet, it has given the Department of Justice (DOJ) an effective tool to nail warez traders, and [a couple of hundred warez traders have been busted using the law](#). Removing warez traders from the Net, one by one, is a crude but ultimately effective method for curtailing warez trading.

1: [Anti-Cybersquatting Consumer Protection Act](#) (ACPA)

The 1990s saw a frenzy of domain name registrations, often involving the registration of domain names containing well-known trademarks by someone other than the trademark owner (a process called *cybersquatting*). Courts struggled to apply trademark law to this behavior, so trademark owners appealed to Congress for help. Congress initially hoped that the Internet Corporation for Assigned Names and Numbers (ICANN) would promulgate its own anti-cybersquatting administrative regulations (which ultimately became the [Uniform Domain-Name Dispute-Resolution Policy \[UDRP\]](#)). But ICANN took too long, and an impatient Congress enacted the ACPA.

The ACPA targeted cybersquatting, and in that respect the law has worked well. The classic 1990s cybersquatting "land-grab" registrations of [trademarkowner].[tld] have effectively dried up, and the few cases in which a true cybersquatter has defended an ACPA claim in court generally have resulted in resounding victories for the trademark owner.

A silver lining of the ACPA: It contains an immunization of domain name registrars and registries that completely eliminated them as the targets of trademark owners. Prior to

ACPA, domain name registrars (especially Network Solutions, the monopoly .com registrar for most of that time) had been sued repeatedly. Now, plaintiffs don't even think about it.

However, the ACPA isn't all good news. From a defense perspective, the ACPA has emerged as a tool to [attack grippers and other critics](#). From a trademark owner's perspective, the ACPA hasn't curbed domain name parking, domain tasting and other AdSense-fueled sites using trademarks or typographical versions of them. So no one is really happy with the law. Nevertheless, as a point solution to the cybersquatting problem, I think ACPA is fairly characterized as a solid success.

Worst Internet Laws

I want a little credit for finding four laws that I could say something good about. It wasn't easy. In contrast, the list of bad laws is *much* longer, so I limited myself to 10.

What makes a law "bad?" Unfortunately, there are many routes to ignominy, and mere legislative cluelessness isn't sufficient. Some common themes: poor/ambiguous drafting, unintended consequences, justification bait-and-switch (publicly declaring that the law was intended to accomplish a goal it was never designed to do), and attempts to legislatively manufacture markets or change consumer behavior.

The dishonor roll:

#10: E-Sign

[E-Sign](#) generally says that online contracts are not denied enforcement simply because they are in electronic form rather than on paper. Superficially, this sounds positive because it stops courts from underenforcing electronic contracts or overreacting to new communication technologies. The problem? This law was unnecessary. Although there was a little concern that some states would enact a non-standard version of the law, by the time that Congress passed E-Sign, there was a lot of momentum toward adopting the [Uniform Electronic Transactions Act](#) (UETA), and [a lot of states](#) had already implemented UETA. Worse, E-Sign has a partial preemption clause that makes it difficult/impossible to figure out which state laws survived it. So E-Sign is a prime example of how Congress cannot resist the lure of Internet regulation—even if it adds no value (or even subtracts value) in the process.

#9: [DMCA Online Safe Harbors](#)

Another law that looks good on the surface, this law purports to provide safe harbors to protect online intermediaries from copyright infringement caused by other people. However, this law has at least two major flaws. First, it sets up a notice-and-takedown procedure that has led to [significant abuse](#), such as content owners effectively "spamming" online service providers with poorly researched junk notices that impose significant investigatory costs on the provider-recipients.

Second, and perhaps more importantly, the law governs only late 1990s technologies; it doesn't contemplate P2P file sharing and other decentralized forms of communications. This technological dependency makes the safe harbor increasingly irrelevant as technology evolves. As a stark example, consider that the online safe harbors didn't get mentioned—not once!—in the most important online secondary infringement case to date: the [Grokster Supreme Court opinion](#).

#8: Unlawful Internet Gambling Enforcement Act of 2006 (see the end of [this file](#))

As I have [said elsewhere](#), this law is "a flagship example of how special interest lobbying combined with legislative mumbling can produce an unreadable mess." First,

the law is written in unintelligible Congress-ese. Second, the law is pockmarked with special interest exceptions, clearly showing who has the best lobbyists. Third, and most importantly, Congress did not specify (in this law or elsewhere) what constitutes illegal Internet gambling, yet the law requires third-party money sources to block the flow of money to illegal gambling operations. Thus, just like Kafka might write it, Congress deputizes private actors to block illegal activity without deciding for itself what constitutes illegal activity. As a result, banks and other money sources probably will curtail lots of legitimate activity to be on the safe side.

#7: [Digital Millennium Copyright Act \(DMCA\) Anti-Circumvention](#)

There are lots of reasons not to like the DMCA anti-circumvention law. Most obviously, the law targets "bad" technology rather than bad behavior—a regulatory model that usually fails when technological innovation bypasses such restrictions; or worse, the restrictions inhibit the development of socially beneficial technology.

However, the anti-circumvention laws make this list principally because of their unintended consequences. The law was designed to bolster content protection technology: the purported justification was that content owners wouldn't feel comfortable putting content online without content protection measures, and this law restricts the capability to bypass those measures.

As it turns out, the hottest area of anti-circumvention litigation has nothing to do with such content protection schemes, but instead involves companies using the DMCA as an anti-competition law. Two flagship examples—[Chamberlain](#), involving the sale of compatible after-market universal garage door openers (a case the EFF calls "mind-bogglingly absurd") and [Lexmark](#), involving refilled printer cartridges—ultimately reached pro-competitive outcomes, but only after significant litigation and some disconcerting early rulings. Even with these rulings, companies now routinely consider anti-circumvention claims as part of a general anti-competitor campaign (for a very recent example, see [here](#)). As a result, the law has increased the cost of doing business and given plaintiffs another tool to try to restrict legitimate competition, while doing almost nothing to advance its principal goal of increasing protection for content owners.

#6: [Electronic Communications Privacy Act](#)

This law was written in 1986 (amending earlier versions), back when the Internet was an obscure academic network. Although the law wasn't written with the Internet in mind, it has the heroic responsibility of governing a huge swath of private Internet communications, including email, private chat, VOIP, and others. Even if the law were well-drafted, applying a pre-Internet law to these communications would create plenty of ambiguity and friction. Unfortunately, this is not a well-drafted law; in my opinion, this law is one of the most poorly drafted statutes ever. The result is a tangled convoluted hairball that no one (even privacy experts) can understand or apply.

#5: [Utah Digital Signatures Act](#)

In 1995, there was some concern that the lack of Internet authentication would inhibit the development of e-commerce. As a result, VeriSign (and others) advocated that everyone on the Internet—both users and websites—should have digital certificates to validate their identity (the equivalent of an Internet driver's license) so that websites and users each could figure out who they were dealing with. However, VeriSign and others expressed concern that a digital certificate issuer would face significant liability if the authenticated information was wrong. Thus, the argument went, if only digital certificate vendors could get some liability protection, digital certificate vendors would provide the necessary authentication that would allow e-commerce to explode.

In response to these concerns, Utah enacted the Digital Signatures Act to regulate the process of granting accurate certificates and limit the liability of digital certificate

vendors. Utah hoped the law would encourage digital certificate vendors to relocate to Utah to take advantage of its friendly legal climate, making Utah a leader in e-commerce.

As it turns out, digital certificates weren't needed to catalyze e-commerce, nor did the market materialize for digital certificates in the form contemplated by the statute (as a PKI-based system). As a result, this law was a complete failure, and [no companies ever complied with the statute's formalities](#). Indeed, the law proved to be so irrelevant that Utah has taken the highly unusual step of [repealing the law](#). At least it owned up to its mistake (this time).

4: Anti-Kid Spam Laws in Utah and Michigan

Nothing fires up the legislative machine like trying to protect kids from Internet dangers. In this case, [Utah](#) and [Michigan](#) created "do-not-email" registries, similar to the national Do-Not-Call registries, for the registration of kids' email addresses. Porn spammers are supposed to check these databases and eliminate any registered kids' addresses from their porn spam distributions.

While do-not-contact registries are generally popular, I'm in the minority of people of who think they are suboptimal policy (I explain my thinking, by deconstructing the federal Do-Not-Call registry [here](#)). In these cases, the do-not-email registries claim to be protecting kids, but they actually don't try to authenticate registrants' ages—making them a generic do-not-email registry, something even the [FTC doesn't favor](#). Most importantly, assuming that the database actually contains kids' email addresses, it becomes a juicy target for criminal hackers, pedophiles, and other bad actors. Based on this concern, many privacy advocates, including the [FTC](#), have advocated against kid-specific do-not-email registries.

3: [Dot Kids Implementation and Efficiency Act of 2002](#)

As we saw with the Utah Digital Signatures Act, legislators can't stimulate market demand simply by legislating the market into existence. In my opinion, no legislative act better illustrates this principle than the Dot Kids Implementation and Efficiency Act of 2002. In the name of providing a safe online haven for kids, Congress co-opted the .kids.us domain and decreed that only kid-safe content could reside there. In theory, parents would feel safe letting their kids loose there, and content publishers would have a good place to reach kids. Ultimately, Internet filters could simply enable .kids.us websites and shut off the rest of the Internet to kids.

The problem? Not many content publishers saw the value of creating kid-safe websites and housing them under the restrictive rules of the law. As a result, [.kids.us is a virtual wasteland](#), housing fewer than 20 websites—almost all of which have less-than-compelling content. (You mean to tell me you've never been there? [Check it out](#) yourself.) Not exactly the most enticing destination for Junior. So .kids.us is a ghost-town-like reminder that legislators should stay out of the business of trying to manufacture markets.

2: Utah/Alaska Anti-Adware Laws

Have you noticed a trend here? Utah makes my dud-law list *three* times—a hat trick of legislative incompetence. This is such a remarkable feat that we might consider banning Utah from enacting further Internet regulations until Utah can show that it will use its powers wisely.

This law makes my list because of the deceptive rationales used to justify it. Touted as an "anti-spyware," "consumer-protection" law, it was neither. The [law](#) targeted only adware, not spyware, and it gave enforcement rights to trademark owners, not consumers. As a result, the law gave trademark owners the power to take software out

of consumers' hands—even if the consumers actually *wanted* the technology. Further, by allowing trademark owners to attack competitors for engaging in comparative advertising, the law tried to inhibit beneficial competition rather than promoting it. Thus, despite its billing, this law was a profoundly regressive anti-consumer law.

Given its deceptive nature and adverse policy effects (which I explain in lengthy detail [here](#)), it should not be surprising that the law was quickly [enjoined](#). (Disclosure note: I worked on an [amicus brief](#) challenging the law.) Chastened, the act's sponsor subsequently amended the law to make it [effectively irrelevant](#).

However, before Utah amended its law, Alaska implemented its own [bastardization of Utah's initial law](#). Among the Alaska law's defects, it expects adware vendors to pop up a notice to potential downloaders, asking them for their geography. With this information, in theory, the vendor can avoid downloading the regulated software to Alaska residents. In other words, in an effort to fight unwanted pop-ups, the Alaska law mandates that software vendors deliver lots of unwanted pop-ups to consumers—even when both the vendors and consumers are located outside of Alaska. Classic legislator logic!

NOTE

While this article was in press, Utah revisited this area yet again. This time, Utah enacted a law that controls *all* keyword-triggered advertising, raising serious questions about its effect on Google and other search engines. As I explain [here](#), regulating the use of keywords to trigger advertising is profoundly anti-consumer and is very bad policy.]

1: [Communications Decency Act](#) (CDA)

Based on the discussion above, clearly there was plenty of competition for the worst Internet law of all time. However, I found picking a "winner" surprisingly easy. In fact, in my book, it isn't particularly close.

The Communications Decency Act, passed in 1996, was Congress' first comprehensive attempt to regulate Internet content. Not surprisingly, Congress made a lot of rookie mistakes. The CDA tried to keep kids away from Internet porn, a reaction to a sensational 1995 article (the "[Rimm Report](#)") published in the *Georgetown Law Journal* that proclaimed that the Internet was awash in porn. But later examinations [thoroughly discredited the Rimm Report](#)—meaning that Congress' efforts/overreactions were based on bad social science.

Worse, Congress mistakenly assumed that non-porn content could be easily segregated from porn. In defense of this assumption, the government's expert witness proposed a content-tagging system that would enable browsers to wall off porn. But this exposed a deep flaw in the law: the tagging system didn't exist, browsers weren't written to honor the tag, and it turns out that requiring publisher self-tagging for all Internet content is burdensome and cost-prohibitive.

Because web and email content publishers had no easy way to comply with the law, the law threatened to restrict virtually every Internet speaker. Further, Congress imposed punitive and draconian sanctions (including stiff jail time) for breaking the law. Congress really, really wanted to wipe porn off the Internet, but it chose a particularly mean-spirited way of doing so.

Not surprisingly, the law fared poorly in the courts. Within a week, it was [enjoined](#). The next year, the U.S. Supreme Court [unanimously struck down the law](#) (although two judges would have found a way to preserve some of the law). For its lack of policy support, its sloppy blunderbuss approach to regulating speech, and its flat-out meanness, I hereby crown the CDA the worst Internet law (to date...).

800 East 96th Street Indianapolis, Indiana 46240