Why Filtering Is Not the Solution

by David Sohn [1], Mark Stanley [2]
February 14, 2012

Updated Below

Bill Keller, former executive editor of *The New York Times*, recently responded [3] to detractors of a column [4] he penned on PIPA/SOPA.

In a blog post, Keller writes, "Much of the mail bristles with resentment of the corporate behemoths that have tried to protect music, film and books by building higher legal walls around their property."

CDT is among the immense and philosophically diverse crowd [5] that bristled during the PIPA/SOPA debate. By now it should be well understood that our objections weren't focused on rightsholders' desire to protect their work, but rather on the methods by which they wanted to protect it.

Keller continues, "[I]t should be well within the capability of the Internet giants to filter their traffic for the most egregious pirates, just as good citizenship (and in some cases the law) would oblige a bus company to notify police if the bus line was being used to facilitate a crime. At least it's worth exploring."

In fact, relying on "Internet giants" to filter user traffic is far more problematic than it first appears. This is precisely what was "explored" in the PIPA/SOPA debate – and precisely what made the bills so controversial.

(Incidentally, the analogy to a bus company is off base, in part because it assumes that it is obvious to the bus company when riders are engaged in criminal activity. A better analogy would be requiring the bus company to search riders for contraband or demand that riders disclose the purpose of each trip. In addition, Internet filtering carries technical and international consequences that have no parallel in local bus routes.)

Proponents of PIPA/SOPA rallied behind the proposal that Internet service providers (IPSs) be required by law to engage in domain name system (DNS) filtering; that is, ISPs would interfere with the Internet's addressing system to prevent domain names from connecting to their corresponding numerical IP addresses. As CDT has explained [6], including in testimony [7] and letters [8] to Congress, DNS filtering would threaten significant collateral damage without any serious prospect of achieving meaningful reduction in infringement.

DNS filtering is ineffective because there are a variety of easy techniques to circumvent it, including using a simple browser plug-in or bookmarking a site's IP address. Meanwhile, Sandia National Labs [9] and some of the Internet's most respected engineers [10] have warned that it would undermine cybersecurity. The White House, after lengthy analysis of the matter, concluded [11] that "[p]roposed laws must not tamper with the technical architecture of the Internet through manipulation of the . . . DNS" because such provisions "pose a real risk to cybersecurity and yet leave contraband goods and services accessible online."

Moreover, if the U.S. government were to embrace this technique to block websites that it deems—to use Keller's term—"egregious," it would be that much more difficult to advocate that oppressive regimes not block sites *they* find egregious. As Julian Sanchez of Cato has noted [12], if we were to embrace DNS filtering, the only thing separating oppressive regimes and the U.S. in this case would be what's on our respective blacklists. And if each country enforces its own blacklist, the end result would be a highly balkanized Internet. The U.S. State Department is the leading global advocate for a unified, global Internet; embracing a technique that fragments the Internet would seriously erode U.S. credibility in this cause.

Are there other, non-DNS techniques ISPs could use to filter user traffic? Well, they could engage in deep packet inspection to monitor user behavior and ferret out illegal activity. But this kind of pervasive surveillance comes at a high cost to privacy and, like DNS filtering, sets a dangerous international precedent.

Even for Internet entities other than ISPs, filtering carries significant policy implications. Companies required to monitor and filter illegal activity may well overblock in order to play it safe. To ensure they won't be accused of shirking their responsibilities, the tendency will be to block disputed material or anything that carries even a whiff of legal controversy. The risk of lawful speech getting caught up in the filters is especially high when, as with PIPA/SOPA, the filters aim to block entire domain names. Domain names are often shared among multiple users of separate subdomains, and also among multiple uses (such as a company's public-facing website and internal email server). Domain name filtering is a very blunt instrument that can sweep in lawful content inadvertently.

Finally, we should all be realistic about the long-term consequences at stake here. If we establish both the technical infrastructure and the legal and social norms to support pervasive Internet filtering, its use will be demanded for a wide range of causes. There is, after all, no shortage of undesirable content and behavior online. With "Internet giants" now tasked with online policing functions, the online environment would effectively become subject to a new set of centralized gatekeepers.

That may be an appealing vision to some, but it would jeopardize the many benefits of the Internet's open and decentralized nature. CDT would urge Keller, and other thought leaders delving into this area of policy as a result of the PIPA/SOPA uproar, not to cast aside the core principles that make the Internet such a powerful force for free expression and innovation. A good place to start in understanding those principles, we would humbly suggest, is the CDT document "What Every Policymaker Needs to Know About the Internet." [13]

None of this is to say that nothing can be done about combating offshore piracy. CDT has suggested [14] that a "follow the money" approach offers a higher likelihood of effectiveness with less collateral damage. But hopefully one of the biggest lessons that has emerged from the months-long national debate over PIPA/SOPA—which included a sea of articles, blog posts, and reports [15] about the risks the bills posed—is that filtering the Internet is not the answer.

Update

CDT Fellow David Post, who helped organize the law professors'