BRING IN THE NERDS: THE IMPORTANCE OF TECHNICAL EXPERTS IN DEFEATING SOPA AND PIPA

ANDREW MCDIARMID AND DAVID SOHN

Andrew McDiarmid and David Sohn both work for the Center for Democracy and Technology, where McDiarmid is a senior policy analyst and Sohn is general counsel. The Center for Democracy and Technology is a nonprofit public policy organization and the leading Internet freedom organization working at the critical edge of policy innovation. When the Internet was in its infancy, CDT helped shape the first legislative choices and court decisions that allowed this technology of freedom to flourish. Today, it is committed to finding innovative, practical and balanced solutions to the tough policy challenges facing this rapidly evolving medium.

The scene is familiar to many among the millions who mobilized to defeat SOPA: some Members of Congress proudly declaring technical ignorance and defiantly dismissing free speech and cybersecurity concerns over DNS-blocking, while a vocal few underscored these problems and insisted that Congress "bring in the nerds" to learn more.

This dynamic at SOPA's December 2011 markup meeting of the House Judiciary Committee became a rallying point for opponents of the legislation. We saw articles declaring it "no longer ok" for Congress not to know how the Internet works, and proponents' steadfast refusal to entertain the technical objections to the bill fueled the sentiment that experts, Internet communities, and the public at large had been shut out of the behind-the-scenes work that went into both SOPA and PIPA.

Now, it isn't exactly realistic to expect politicians to write code or understand all the technical workings of networks and the DNS. Nobody is seriously suggesting that they should. These intricacies are worlds away from the many pressing issues on policymakers' minds, and we hire them to be effective representatives of their constituents, not network engineers.

Nonetheless, when the issue on the table is undeniably technical—and fiddling with Internet addressing is nothing if not technical—it's not unreasonable to expect at least engagement with the details. Lucky for us, despite skewed hearings and the unwillingness of PIPA and SOPA's sponsors to budge on the technical concerns (at least until it was too late), a small group of opponents used the SOPA markup as a platform to ask the right questions and bring attention to issues too long ignored in the lead-up to what could have otherwise been easy passage out of committee.

But where did those arguments come from? The efforts of Reps. Lofgren, Issa, Polis, Chaffetz, and others were invaluable in stalling SOPA and fueling the fire over the next five weeks until the January 18th protests—but what fueled their fire? In this chapter we want to make a case for the important groundwork done before SOPA grabbed the Internet's attention, in particular

the contributions of impartial technical experts who weighed in not on the side of copyright or the "copyleft," but on behalf of the integrity and security of the world's most important communications network. It is not at all certain that things would have played out as they did without these experts' written contributions and on-the-ground efforts to educate Congress about the risks they identified.

When COICA (PIPA's predecessor, the "Combating Online Infringements and Counterfeits Act") was introduced in September 2010, a small handful of familiar voices in Internet-meets-copyright policy circles weighed in with a laundry list of arguments against the bill. Our organization, CDT, published one of the first analyses of the bill, focusing in large part on the overblocking and cybersecurity concerns that DNS-filtering presents. The same day, the Electronic Frontier Foundation organized a letter from over ninty prominent Internet engineers who decried the bill as censorship and expressed their fear that it would fragment and destabilize the Domain Name System (DNS).

We were joined over the next weeks and months by other D.C.-based advocates like Public Knowledge and the library associations, Internet trade associations, and the human rights community. But despite our growing coalition, we faced long odds to overcome the well-connected momentum behind the bill. The bill's supporters worked to brand us as apologists for infringers and insisted that the legislation was a simple matter of deciding to take a stand against rampant theft. Despite our community's expertise and deep understanding of both the policies and technologies that have made the Internet such a remarkable vehicle for innovation and free expression, our warnings about the folly of mandated interference with the DNS went largely unheeded.

As fall turned into winter, the 111th Congress into the 112th, and COICA eventually into PIPA, new voices began to weigh in. Dan Kaminsky, the DNS security folk hero who would go on to play a major part in educating Congress about the risks of mandated blocking, reiterated concerns about stability and governance and raised new issues in a short letter on COICA. He also participated in a panel debate on the subject at the January 2011 State of the Net conference in Washington. His fear was that mandating filtering in an attempt to block what is, for better or for worse, hugely popular content would drive users to use untrusted and risky DNS servers. He argued that such a migration would undermine the benefits of securing U.S. nameservers against malicious sites, exposing users and networks to botnets and phishing attacks. Kaminsky also worried that the migration would weaken ISPs' "eyes and ears" into their networks; DNS traffic can provide a rich dataset on network usage to help diagnose and mitigate attacks as they occur.

In March 2011, as his name was invoked by COICA's supporters and opponents alike, Paul Vixie entered the debate with a pair of blog posts describing the relationship between mandated blocking and DNSSEC (secure DNS) and the long-term risks of mandated blocking to the DNS's primary value, universal naming. For Vixie, founder of Internet Systems Consortium and one of

the world's leading experts on DNS, a key issue was "alignment of interests" and the fragility of Internet infrastructure. He feared that the interference envisioned by COICA would for the first time put nameservers in the role of frustrating rather than fulfilling user requests, create widespread motivation for users to circumvent current DNS arrangements, and ultimately fracture the Internet into a network without a single naming system for reaching everything.

Kaminsky and Vixie, respected in computer security circles but relative newcomers to Internet copyright debates, lent new credibility to the argument of CDT and others that the legislation carried serious risks for cybersecurity. They also started a serious conversation in engineering circles about the technical implications of the bills, including the extent to which the legislation would conflict with or undermine DNSSEC. The growing attention and involvement of the technical community would prove invaluable in PIPA and SOPA's demise.

During the spring of 2011, CDT worked to bring the analysis of the DNS experts into the legislative debate. In March, CDT's David Sohn flagged the technical and cybersecurity issues in hearing testimony to the key panel of House lawmakers, the House Judiciary Committee's subcommittee on intellectual property. Meanwhile, CDT helped organize an effort to have top DNS experts document the technical concerns in detailed yet accessible fashion. In the late 1990s, a technologists' report coordinated by CDT had helped swing the hard-fought debate over encryption policy; CDT urged that an authoritative explanation of the technical implications could be similarly pivotal now.

Kaminsky, Vixie, and three other heavyweights in DNS and Internet-security circles answered the call and co-authored a whitepaper, "Security and Other Technical Concerns Raised by the DNS Filtering Requirements in the PROTECT IP Bill". They released the paper in May 2011, shortly after PIPA was approved unanimously by the Senate Judiciary Committee, and it quickly had a powerful impact on the debate.

The whitepaper offered more detailed examinations of several key arguments against DNS filtering: the tension with DNSEEC deployment, the problems for security and network intelligence that flow from user-circumvention, and the potential for collateral damage due to interdependencies in the DNS. For those of us working against the bills in Washington, the paper was an invaluable asset. We joined Ernesto Falcon of Public Knowledge and other colleagues at many of his meetings on the bills, and once it was published this paper was the first thing we would hand to staff as we urged them to reject the bills' approach. Of course, the technical problems were far from our only concerns, but having experts with unassailable credentials—and without strong interests one way or the other on copyright enforcement questions—made the technical arguments harder to ignore.

On several occasions, some of the authors even joined us in meetings with congressional staff to explain their concerns.

The whitepaper garnered significant media attention as well. Beyond being picked up by the tech-press outlets already covering the issue, it was cited prominently in a *Los Angeles Times* editorial opposing PIPA and urging a "more measured approach". The *New York Times* also relied on the experts' analysis in declaring that the bill "shouldn't pass" as it then stood. The closing line of the *NYT* editorial nicely summed up opponents' reasonable position: "If protecting intellectual property is important, so is protecting the Internet from overzealous enforcement."

Pro-PIPA critics tried to dismiss the arguments made in the whitepaper, but more often than not their rebuttals took the form of "but something needs to be done" or "surely the technical standards community can come up with a way to fix these problems" instead of actually refuting the problems themselves. Within most of the technical community, the paper met with general consensus. In the fall, groups such as the Internet Society, the Anti-Phishing Working Group, and the Brookings Institute released papers or letters reiterating the technical concerns posed by the legislation. Most prominently, the director of computer sciences and information systems at Sandia National Labs, Dr. Leonard Napolitano, assessed the technical claims in November at the request of Rep. Zoe Lofgren. His office's response cited the whitepaper and was unequivocal: "we agree with the conclusions of that report." In addition, Stewart Baker, former NSA General Counsel and former Head of Cyber Policy for DHS, penned two widely read op-eds in which he focused on the harm mandated blocking would cause for DNSSEC deployment.

The whitepaper's authors remained active as well. On several occasions they joined CDT, PK, or other advocates to meet in person with congressional staff and explain the technical arguments. They sent letters to Congress in October and December rebutting efforts by the legislation's supporters to dismiss the whitepaper's conclusions. Importantly, they also spoke to Executive Branch officials. In particular, CDT arranged a high-level meeting in early December between the paper authors and key White House staff. That meeting included Howard Schmidt, the Cybersecurity Coordinator, and Victoria Espinel, the Intellectual Property Enforcement Coordinator—both of whom would go on in January to coauthor the critical blog post announcing the Obama Administration's opposition to DNS filtering.

SOPA and the Unraveling

Despite the growing opposition through the summer and early fall, there was little indication that Congress was listening. In the Senate, PIPA had been approved without objection by the Judiciary Committee, had numerous bipartisan cosponsors, and looked like it would have the votes to pass. Then, in late October, the leaders of the House Judiciary Committee introduced SOPA. Rather than addressing the problems with PIPA, SOPA was far worse. It expanded the field of sites that could be targeted and not only kept PIPA's problematic remedies, but added new ones that threatened a broad range of

legal sites. Even though it moved in the wrong direction, SOPA had similarly ominous bipartisan support.

In contrast to the earlier Senate committee process, however, the House Judiciary Committee included some lawmakers who opposed or were at least skeptical of the legislation. SOPA was too extreme, and the technical and other arguments against it too serious, for it to command unanimous support. The whitepaper and other warnings of cybersecurity and technical problems gave these opponents crucial ammunition for the fight.

At the November 16th committee hearing on SOPA, a number of Members raised questions about the cybersecurity impact of the legislation. This included not only Rep. Lofgren, a leading critic of PIPA even before SOPA's introduction, but also Members who said they were still undecided on SOPA. Rep. Lungren, the Chairman of the House subcommittee on cybersecurity, was particularly outspoken, asking panel members about DNSSEC and noting that serious concerns had been raised by expert engineers with no axe to grind in the fight over copyright policy. MPAA's witness expressed the view that the cybersecurity issues were greatly overstated, but Lungren and at least a few other Members were clearly troubled by the absence at the hearing of any engineers or cybersecurity experts who could speak to the issue on a technical level.

During the pivotal committee markup in mid-December, the analyses regarding cybersecurity—the whitepaper, the Sandia letter, the op-eds by Stewart Baker, a new EFF-organized letter signed by eighty-three Internet engineers—were cited repeatedly by Reps. Lofgren, Issa, Chaffetz, Polis, and the other SOPA skeptics as they criticized the bill. Rep. Chaffetz memorably chided his colleagues, "We're going to do surgery on the Internet … without bringing in the doctors. To my colleagues I would say, if you don't know what DNSSEC is, you don't know what you're doing" with this legislation.

One of critics' principal frustrations was the way the harms and risks of DNS-filtering were simply brushed aside by SOPA's proponents. Opponents asked, at the very least, that the committee slow down and fully consider the consequences. While they were not successful in getting the committee to do a careful assessment of the potential negative consequences, the skeptics' constant refrain of questions focused attention on what had been ignored—SOPA's myriad problems, technical and otherwise—and exposed the flawed process that gave rise to the bill in the first place. What had been intended as a smooth markup of a bipartisan bill turned into a two-day slog of debate and amendments that never made it to a final vote.

What followed the markup is the truly remarkable story of how various communities on the Internet woke up to the dangers on the path Congress was heading down. The markup was streamed online, and the spectacle of the debate—with SOPA's supporters at times acknowledging little understanding of the cybersecurity or technical questions but insisting that the bill be passed anyway—gave rise to rallying cries like "Bring in the nerds" and "It is no longer ok to not know how the Internet works." Bill supporters were mocked on social networks for their fumbling or dismissive reactions to the technical

side of the debate. Popular dissatisfaction mounted, both with the legislation and the process by which it was being considered, and it spread like wildfire in the online communities fostered by popular social networking platforms. As Congress headed home for the winter holidays, grassroots activists had powerful new fodder and a huge receptive audience for organizing petitions and call-in campaigns.

By early January, the criticism was hitting home in the Senate as well. PIPA's lead sponsors, probably sensing growing concern among other Senate offices about whether the technical questions had received fair consideration, organized a private briefing for Senate staff on the cybersecurity issue specifically, with opportunities for both the legislation's supporters and opponents to explain their side of the cybersecurity question.

Then, on January 14th, the Obama Administration finally weighed in. In a response to two petitions against the bills that had received more than fifty thousand signatures, three key White House officials—Intellectual Property Enforcement Coordinator Victoria Espinel, U.S. Chief Technology Officer Aneesh Chopra, and Cybersecurity Coordinator Howard Schmidt—stressed that antipiracy measures must not come at the expense of free expression, legitimate use of the Internet, and cybersecurity. The response specifically and unambiguously rejected DNS filtering and confirmed that SOPA and PIPA, as drafted, posed a threat to cybersecurity:

"Proposed laws must not tamper with the technical architecture of the Internet through manipulation of the Domain Name System (DNS), a foundation of Internet security. Our analysis of the DNS filtering provisions in some proposed legislation suggests that they pose a real risk to cybersecurity and yet leave contraband goods and services accessible online. We must avoid legislation that drives users to dangerous, unreliable DNS servers and puts next-generation security policies, such as the deployment of DNSSEC, at risk."

Around the same time, the bills' lead authors, Chairpersons Leahy and Smith, both issued statements acknowledging that the DNS portions of their respective bills would need to be removed. But it was too little, too late. The technical problems were not the bills' only problems, and the various communities of opponents were mobilized and well prepared to make that known. The debate over the technical arguments had also highlighted fundamental flaws in the process that produced PIPA and SOPA. The Internet-engaged public was not going to be satisfied by grudging and last-minute concessions; the bills were viewed as too flawed and too much the product of back-room deals and a process that had been rigged from the start.

Much has been and will continue to be written about the public SOPA/PIPA protests that followed, and deservedly so. The petitions, calls, and blackout that took place on January 18th in response to the bills were unprecedented in scale, and may indeed stand out as a watershed moment for Internet policymaking and the democratic process. But they were fueled by a growing body of powerful arguments regarding the nitty-gritty substance of the legislation, including impartial technical analysis that exposed glaring flaws. That analysis,

and the role it played in the ultimate withdrawal of the bills, should not be overlooked.

What we saw in SOPA and PIPA was an attempt to make Internet policy from a narrow perspective, with little if any input from the community of people who best understand and care about how the Internet actually works. One of the key reasons we were successful in defeating these bills was that the community spoke up anyway. Millions of Internet users all over the country—indeed, all over the world—demanded that their concerns be heard. Imagine how much better Internet policymaking could work in the future if the public—and the experts—are included in the discussion from the start.