# **Technology and Society**



# Free Speech and Child Protection on the Web

Daniel J. Weitzner • MIT Computer Science and Artificial Intelligence Laboratory

arch 2007 was a big month for the ongoing question of how to protect children from controversial and potentially harmful Web content. On 22 March, a US court rejected, for the fifth time, a proposal from the US Congress to criminalize the online publication of so-called harmful-to-minors material. (The term "harmful to minors" is generally understood to stand for what lay people would identify as pornography. It isn't precisely defined, however, and does leave some question about what information is included.) Just a week later, ICANN rejected, for the second time, a proposal to create a new top-level domain (TLD) that would host "responsible adult entertainment." Do these developments mean that children in the US and around the world are less safe when they surf the Web? Will the incidence of children accidentally or intentionally accessing pornographic material increase? Have we missed an opportunity to make the Web safer? The answer to all of these questions is "no." Rather, we should take the opportunity to relearn a lesson about how to approach content regulation on the global, decentralized system that is the Web.

Since the Web first became widely used in the mid 1990s, it's been impossible to regulate all, or even most, of its content according to a single substantive standard. Instead, diversity and decentralization rule. To protect children or anyone else from content regarded as inappropriate or harmful, we must find user-centered alternatives that leverage the Web's decentralized social organization, rather than trying to fight it.<sup>1</sup> Around the world, while regulators have struggled with laws that seek to restrict children's access to material that is otherwise legal for adults, Web technology developers have been building increasingly accurate and powerful content filters. These filtering approaches can be either the basis of parental empowerment technologies (see http://getnetwise.org or www.sip-bench.eu/sip bench.php) or tools for repression and censorship by authoritarian regimes. What should be clear by now, though, is that attempts at national or culturally narrow content regulation simply won't work in democratic societies.

#### Filters vs. Government Censorship

The Web's ability to provide homes and schools worldwide instant access to global information brought much excitement but no small measure of concern to policy makers in governments used to regulating mass media to keep certain content away from children. On TV, for instance, adultthemed material is broadcast only in the late evening hours, put on pay-per-view channels, or sometimes simply banned by national regulatory authorities. Following that tradition, then, many governments' first impulse was to try to censor Internet content in the same way.

The US, the first major democracy to attempt to censor Web content, made the first and most visible set of mistakes. In 1996, Congress passed a law known as the Communications Decency Act (CDA) as part of an overall deregulation of the telecommunications marketplace. The CDA made it a crime to make "indecent or patently offensive" material available on the Internet to anyone under 17 years old. As a practical matter, because Web publishers can't effectively block access to their Web sites based on age, this law amounted to a total ban on this type of content. While US legislators were debating the law, advocates from the freedom of expression community and the nascent Internet technology industry pointed out that attempting to censor the Internet at the publisher end is both impractical and ineffective given the medium's global nature. I, along with others, argued that the only way to protect children from material that either society at large or their parents, in particular, consider "harmful" is with content-filtering technology at the user end.

In the meantime, the European Commission took a more deliberative view and moved toward a policy encouraging the development of various filtering technologies, mirroring the great diversity of content standards among EU members.

The US Congress, moved somewhat more by a rush to act against pornography, passed the CDA. In 1997, however, the US Supreme Court struck it down as a violation of basic free speech rights. The Court noted that filtering technologies were likely to be far more effective in a global medium than national laws could ever be.

## Failing to Learn from the CDA

The lessons about effective versus ineffective content regulation on the Web haven't been easy to learn. Legislators, some members of the Internet technical community, and even sage legal cyberspace scholars have fallen into the trap of believing that centralized regulation is still possible. Examining these mistakes reveals that decentralization and user control are even more relevant today as the Web grows to include more users, more diverse cultures, and more of the world's information.

#### Child Online Protection Act (COPA)

Not willing to leave well enough alone, the US Congress responded to the Supreme Court's 1997 CDA rejection by passing another law in very much the same vein. Drafters tried to offer a somewhat narrower law that would meet the Court's constitutional requirements. However, as we will see, the law is similar to CDA in important ways and doesn't reflect any lessons learned from that act's failure. This new law, the Child Online Protection Act (COPA), makes it a crime to make harmful-to-minors material available to children on the Web for commercial purposes. Congressional attempts at narrowing include criminalizing only "harmful to minors" speech, as opposed to all "indecency." The limitation to "commercial use" is also narrower than the CDA, but might include any Web site that has advertising on it, even if the site doesn't charge for access.

Since the US adopted COPA in 1999, several courts, including the Supreme Court, have found that it violates constitutional rights in the same way as the CDA. According to the Federal District Court in Philadelphia, COPA can be acceptable under the Constitution only if it meets what's known as the "least restrictive means" test. That is, a law restricting speech is allowed under the First Amendment only if it's the least restrictive approach to achieving an important government interest. In this case, the Court agreed that protecting children from pornographic material online is important but found that there are more effective and less restrictive means to do so. Specifically, just as with the CDA case, a federal judge found that relying on filters is both more effective and less restrictive than government censorship.

Filters don't censor content at the point of creation or publication rather, they rely on individual users to make filtering decisions on their end. The content itself is available to those who want it, but anyone who is responsible for protecting kids (parents, teachers, and so on) can block it. This approach is inherently less restrictive because it doesn't interfere, on a wholesale basis, with the free flow of information on the Web. It's also a more effective approach, for two reasons. First, filters work better in a global environment in which no national law can possibly control the behavior of all Web publishers worldwide. In some cases, governments do succeed in coordinating law in a globally consistent

manner. The universal revulsion against child pornography has resulted in coordinated enforcement efforts – the EU, for example, has led the way in encouraging cooperation among ISPs and law enforcement authorities to remove child pornography from the Web. However, this is the exception when it comes to controversial practices. Second, requiring that Web sites verify their visitors' ages is both unduly burdensome on site operators and also inherently unreliable, given how easy it is to spoof credentials.

Ultimately, this new law fails to account for the Internet's global nature, and, more important, doesn't recognize that user- and parentally controlled filters allow each family to control the Web content that comes into their homes according to their own values, and on a global scale.

#### The .xxx Saga at ICANN

COPA isn't the only example of people failing to recognize the Internet's global and diverse nature. Over the past few years, a group of Canadian entrepreneurs has been lobbying ICANN to create and operate a new TLD called .xxx. Proponents argue that with this new domain in place, "responsible" adult content of the sort that COPA seeks to ban would be contained within this "part" of the Internet and thus be easier to filter for those who want to avoid it. Some suggest, with some reason, that ICANN should allow any group of people to operate any TLD at all, provided it's not actively harmful. The .xxx proposers, however, suggest that they should be allowed to operate and profit from this new TLD because it would make the Internet a safer place for children. Commenting on the recent court ruling striking down COPA, the leader of the .xxx effort, Stuart Lawley, attempted to associate his cause with the free speech rights upheld in that decision (see www. circleid.com/posts/copa\_ruling\_on\_ xxx\_self\_regulatory):

'Now, more than ever, it underscores the need for ICANN to approve the proposal for a voluntary .xxx domain as another alternative to government regulation ... These findings fully support the approval by ICANN of the .xxx domain,' Lawley said, 'because doing so would improve the accuracy of voluntary filters and would put in place best practices by adult websites.'

In his zeal to win support for his proposal, Lawley missed the point of the COPA decision entirely, failing to see that trying to group all "adult" content under a single designation falls into the same trap of ignoring the Web's diverse, global nature.

The .xxx proposal stands for the extraordinary and implausible proposition that the world can agree on what sort of content should be filtered in the name of child protection and good values. It requires that people from Northern Europe, Australia, the US, Saudi Arabia, China, and more than a hundred other countries agree on a category of content that, if filtered out, would make the Internet "safe" for children. In the US, it's not even possible to come to such an agreement between one state and another, or between more liberal major cities and conservative rural areas. Anyone who believes that it's possible to come to a global consensus on such matters must be either naïve, blinded by profit motive, or willing to accept a leastcommon-denominator definition of content that would reduce the world's greatest medium of expression to a kindergarten.

After a contentious debate, ICANN decided for a second time that it would not create .xxx. Some lament this decision as bowing to pressure from some governments and antipornography advocates who felt that ICANN's actions would give legitimacy and comfort to what they regarded as immoral content. ICANN made its decision despite intensive, bareknuckled lobbying from ICM, the company that hoped to collect registration fees from porn sites under the .xxx domain. In the end, ICANN's board rejected the application because it wasn't sure that the domain added value and worried that it would draw ICANN into disputes regarding Internet content regulation, an area the board rightly considers outside its jurisdiction and competence.

Not all agreed with the decision, however. For example, ICANN board member Susan Crawford (www.icann. org/meetings/lisbon/transcript-board -30mar07.htm), a long-time supporter of Internet self-governance, stated that

It is very clear that we do not have a global shared set of values about content online, save for the global norm against child pornography. But the global Internet community clearly does share the core value that no centralized authority should set itself up as the arbiter of what people may do together online, absent a demonstration that most of those affected by the proposed activity agree that it should be banned.

Crawford is concerned that ICANN's decision marks a blow to the Internet's independence and global diversity, but I think the opposite will be the case. Rejecting .xxx rejects the notion that there is such a thing as a centralized authority for meaning and values on the Internet. To be commercially successful, .xxx would have to gather a large proportion of the Web's controversial content into a single, catch-all category. This collection would either be limited to a very narrow notion of what some community considers harmful to minors and thus useless to most of the world, or would become the place into which governments force all content any community considers objectionable. The former option is unworthy of ICANN's role as a trustee of a global resource. The latter would do considerable damage to the global free flow of information and ideas online. Most importantly, nothing that ICANN has done in any way

restricts the manner in which any or all members of the "adult entertainment" community can organize themselves online, as Crawford worries. They remain free to take various steps to enhance users' ability to avoid (or discover) adult content. What's more, by avoiding the very centralizing step of anointing a single approved TLD for this purpose, ICANN's rejection of .xxx will allow coexistence and competition among various filtering and labeling approaches, thus increasing the chances that user-control mechanisms can meet a diversity of needs around the globe.

## Is Filtering a Threat?

One surprising reaction to COPA's recent rejection comes from Internet legal scholar Larry Lessig. Lessig, known for his insights into the role that both code and law play in regulating the Internet, and for his pioneering work in developing the Creative Commons copyright metadata scheme, worries that privately developed filtering could end up being worse that is, from a free speech perspective, private filters could end up suppressing more speech than an updated, narrow censorship law.<sup>2</sup> Indeed, some in the field are concerned that some filters "overblock" information. Firstgeneration filtering technology was based on simplistic keyword matching; some filters blocked Web pages about breast cancer, for example, along with pages with sexually explicit images of breasts. Today, however, evidence shows that overblocking rates are low – in the range of 5 to 11 percent of the overall content - and there's some evidence that a portion of this overblocking reflects some parents' desire to offer only a very restricted view of the Web to their children.<sup>3</sup>

As an alternative to privately developed filters, Lessig suggests instead that there be a legal requirement that all harmful-to-minors material be labeled by its publisher with an  $\langle h2m \rangle$  tag in the page mark-

# Free Speech and Child Protection

up. With this tag in place, software could more accurately filter pages by searching for that metadata and blocking it.

From a technical perspective, the labeling approach is much more coherent than attempting to use the DNS to sort and filter content. Although the .xxx proposal would require authors to move the sexually explicit content into another domain, thereby creating the unwieldy situation that some pages on a site would be served from an entirely different TLD, using metadata as Lessig proposes could make it easy for page authors to label their pages appropriately and just as easy for search engines or filtering software to block those pages. The H2M proposal appears to draw its inspiration from other policy-aware designs for the Web that address privacy (P3P) and copyright (Lessig's Creative Commons system). I've been a big fan and supporter of these approaches - Creative Commons, for example, has had groundbreaking impact on the way that Web authors approach copyright questions.

But do these successes mean that H2M will work? Sadly, I doubt it. First, the legal requirement to use the  $\langle h_{2m} \rangle$ label would have force only against US-based Web sites. So, the filtering this approach enables would be limited to a small fraction of Web content. US courts have rejected US-centric approaches as ineffective in the past, and this new version does no better. Second, self-labeling, whether it's with an  $\langle h_{2m} \rangle$  tag, or any other scheme that attempts to describe content with a single vocabulary for the entire world seems bound to fail.

In the end, Lessig's worry about bad filters is a bit like worrying about bad newspapers. Indeed, there's lots of irresponsible news reporting and editing both in print and on the Web. However, we rely on the international decentralized marketplace of ideas to encourage the development of editing styles, including filtering approaches, which represent a wide variety of values. There's clearly room for improvement and innovation in filtering approaches, but relying on government censorship to achieve this purpose is shortsighted.

round the world, most ISPs and A search engines already provide content-filtering and labeling tools for free or at very low cost. They aren't perfect, currently reflecting more North American bias about what's appropriate for kids, and, as mentioned, problems continue with blocking sites that shouldn't be blocked. Once and for all, let's learn the lesson of the globalized, decentralized Web and put our energies into improving already proven approaches. Users and individuals at the edges of the Internet can exercise control over what they see; centralizing institutions should concentrate on maximizing this control for each individual, rather than trying to exercise centralized control, which is neither effective nor consistent with the best of our democratic values. 1

#### References

- D. Weitzner and J. Berman, "Abundance and Control: Renewing the Democratic Heart of the First Amendment in the Age of Interactive Media," *Yale Law J.*, vol. 104, no. 7, 1995, pp. 1619–1624.
- L. Lessig, "COPA Is Struck Down," Lessig Blog, 22 Mar. 2007; www.lessig.org/blog/ archives/003738.shtml.
- ACLU v. Gonzales, Civ. no. 98-5591, Mar. 2007, paragraphs 110-113; www.paed.us courts.gov/documents/opinions/07d0346 p.pdf.
- Daniel J. Weitzner is principal research scientist at the MIT Computer Science and Artificial Intelligence Lab, codirector of the MIT Decentralized Information Group, and the Technology & Society Domain Lead of the W3C. You can find his blog at http://people. w3.org/~djweitzner/blog/. Contact him via www.w3.org/People/Weitzner.html.

# The magazine that helps scientists to apply high-end software in their research!



### Peer-Reviewed Theme & Feature Articles

2007	
Jan/Feb	Anatomic Rendering & Visualization
Mar/Apr	Stochastic Modeling of Complex Systems
May/Jun	Python: Batteries Included
Jul/Aug	New Directions
Sep/Oct	Computing in Combinatorics
Nov/Dec	High-Performance Computing Defense Applications

#### Top-Flight Departments in Each Issue!

- Book Reviews
- Computer Simulations
- Education
- Scientific Programming
- Technology
- Visualization Corner
- Your Homework Assignment

@computer
society



Subscribe to CiSE online at http://cise.aip.org/cise or www.computer.org/cise