

W H O | R U L E S

T H E | N E T ?

INTERNET GOVERNANCE AND JURISDICTION

Foreword by Vinton G. Cerf

edited by

Adam Thierer and Clyde Wayne Crews Jr.

CATO
INSTITUTE
Washington, D.C.

Copyright © 2003 by the Cato Institute.
All rights reserved.

Library of Congress Cataloging-in-Publication Data

Who rules the net? : Internet governance and jurisdiction / edited by Adam Thierer and
Clyde Wayne Crews, Jr.

p. cm.

Includes bibliographical references and index.

ISBN 1-930865-43-0 (cloth : alk. paper)

1. Internet—Law and legislation. 2. Computer networks—Law and legislation.
3. Freedom of speech. 4. Electronic commerce. 1. Thierer, Adam D. II.
Crews, Clyde Wayne.

K564.C6W48 2003

343.09'944—dc21

2003055299

Cover design by Amanda Elliott.

Cover Photo: © Bill Frymire/masterfile.

Printed in the United States of America.

CATO INSTITUTE
1000 Massachusetts Ave., N.W.
Washington, D.C. 20001

8. Caught in the Seamless Web: Does the Internet's Global Reach Justify Less Freedom of Speech?

Robert Corn-Revere

An instance of the inexplicable conservatism and arrogance of the Turkish customs authorities was recently evidenced by the prohibition of the importation of typewriters into the country. The reason advanced by the authorities for this step is that typewriting affords no clew to the author, and that therefore in the event of seditious or opprobrious pamphlets or writings executed by the typewriter being circulated it would be impossible to obtain any clew by which the operator of the machine could be traced. . . . The same decree also applies to the mimeograph and other similar duplicating machines and mediums.

Scientific American, July 6, 1901

Introduction: Technologies of Freedom

The history of censorship is inextricably intertwined with technological progress. From the printing press, through television, and on to the Internet, innovations in communication inevitably have prompted official efforts to limit or control new media. The United States was the first nation to provide formal protection for freedom of the press. Nevertheless, despite America's foundational commitment to liberty for the technology of print, policymakers and courts in the United States historically have been slow to extend the same freedom to newer innovations.

The Internet bucked that trend. In the brief time between 1996 and the present, U.S. courts were presented with a number of significant cases involving attempts to restrict information available on the Internet and the World Wide Web.¹ That growing body of law

required courts to devote significant attention to the nature of the Internet as a medium of communication and to assess its importance to the American system of free expression. As a result of this review, virtually every federal judge who was asked to rule on direct censorship of protected expression on the Internet held that such restrictions violate either the First Amendment to the U.S. Constitution or the Commerce Clause, or both. The U.S. Supreme Court struck down key portions of the Communications Decency Act, and federal courts have invalidated similar laws in New York, Michigan, Virginia, New Mexico, Arizona, and Vermont.² Most recently, the Supreme Court held that restrictions on Internet speech based on community standards did not necessarily invalidate a federal law targeting such speech, but the Court kept in place an injunction blocking the law's enforcement while lower courts grapple with other difficult issues, including whether the law bans too much speech, is unconstitutionally vague, or supplants less restrictive alternatives.³

The consensus thus far is that the Internet fulfills the ultimate promise of the First Amendment and should receive the highest level of constitutional protection. The Supreme Court found that the information available on the Internet is as "diverse as human thought" with the capability of providing instant access to information on topics ranging from "the music of Wagner to Balkan politics to AIDS prevention to the Chicago Bulls."⁴ Judge Stuart Dalzell of the U.S. District Court for the Eastern District of Pennsylvania characterized the Internet as "a never-ending worldwide conversation" and "the most participatory form of mass speech yet developed."⁵ Judge Lowell Reed wrote that in "the medium of cyberspace . . . anyone can build a soap box out of Web pages and speak her mind in the virtual village green to an audience larger and more diverse than any the Framers could have imagined."⁶ Another district court judge, noting that "it is probably safe to say that more ideas and information are shared on the Internet than in any other medium," suggested that it may be only a slight overstatement to conclude that "the Internet represents a brave new world of free speech."⁷

One key aspect of this "brave new world" that has played a central role in the decisions to fully protect Internet speech is the global nature of the medium. The Supreme Court described the Internet as a "unique and wholly new medium of worldwide human communication" that makes information available "not just in Philadelphia,

but also in Provo and Prague."⁸ As it more recently noted, "One can use the Web to read thousands of newspapers published around the globe" and "can access material about topics ranging from aardvarks to Zoroastrianism."⁹ Cyberspace has no particular geographical location, has no centralized control point, and is available to anyone, anywhere in the world, with access.¹⁰ It is "ambient—nowhere in particular and everywhere at once."¹¹ That quality makes geography "a virtually meaningless construct on the Internet."¹² Accordingly, U.S. courts have been strongly influenced by the "unique character of these new electronic media."¹³

Such a reaction is not unexpected where a free and open medium of communication is compatible with a political system predicated on the free exchange of ideas. But that also is the very reason the Internet is seen as a threat in societies that lack the same free speech traditions as the United States. Other nations have responded to the advent of the Internet in various ways, ranging from open hostility to attempts to regulate it in the same way as traditional electronic media. Such divergent national responses to technology and political freedom are nothing new and historically have had little impact on the United States. But when such differences are applied to a global medium of communication, the resulting legal conflict can have significant ramifications for freedom of speech in this country.

The Yahoo! Case

A decision by a county court in France has crystallized questions arising from the application of national standards to an international medium. The case began in April 2000, when La Ligue contre le Racisme et l'Antisemitisme (LICRA) and L'Union des Etudiants Juifs de France (UEJF), two organizations opposed to racism and anti-Semitism, sent a "cease and desist" letter to the California headquarters of the Internet service Yahoo! demanding that "unless you cease presenting Nazi objects [on the U.S. online auction site] within 8 days, we shall seize [sic] the competent jurisdiction to force your company to abide by [French] law." The law on which the demand was based, Article R645-1 of the French Criminal Code, prohibits the display of any symbol associated with an organization deemed criminal, such as the Nazis.¹⁴

Yahoo! is an Internet service provider that operates various Web sites and Internet-based services that are offered through its main

WHO RULES THE NET?

U.S. servers as well as through servers operated by foreign subsidiaries. Yahoo! subsidiary corporations operate regional services in 20 countries (for example, Yahoo! India and Yahoo! Korea) through Web sites that use the local region's primary language, direct their services to the local population, and abide by local laws. Yahoo!'s services include an automated auction site, online shopping, e-mail, a search engine, personal Web page hostings, Internet chat rooms, and club listings. The auction site allows users to post items for sale and to solicit bids from other users from around the world. In short, Yahoo! epitomizes the type of worldwide communication made possible on the Internet. Yahoo!'s home Web site (<http://www.yahoo.com>) is accessible globally, even though its services are in English, are oriented toward a U.S. audience, and are hosted entirely on servers located in the United States.

That the Yahoo! U.S. site can be reached by French citizens was the basis of the demand by LICRA and UEJF. They did not send a cease and desist letter to Yahoo! France, the regional subsidiary that serves the local population, because that service complies with French law, including Article 645-1. Instead, it was sent to Yahoo!'s U.S. service, which is, like all Internet-based services, available internationally for those who seek it. When Yahoo! declined to alter its U.S.-based service in response to the demand, the French groups filed suit in Paris.

In May 2000 the French court ordered Yahoo! to dissuade and render impossible any access through yahoo.com by Internet users in France to the Yahoo! Internet auction site displaying Nazi artifacts, including objects, relics, insignia, emblems, and flags. It also ordered Yahoo! to block access by French citizens to personal Web pages displaying text, extracts, or quotations from such works as Adolph Hitler's *Mein Kampf* and *The Protocol of the Elders of Zion*, the anti-Semitic report of the czarist secret police. After an interval during which the court heard evidence on the technical feasibility of its order, it reaffirmed its directive for Yahoo! in November 2000 and ordered it to "take all necessary measures to dissuade and make impossible any access via Yahoo.com to the auction service for Nazi merchandise as well as to any other site or service that may be construed as an apology for Nazism or contesting the reality of Nazi crimes."¹⁵ The French court held that "the simple act of displaying [Nazi artifacts] in France violates Article R645-1 of the Penal Code

and therefore [is] a threat to *internal* public order."¹⁶ It described the mere availability of such information as "a connecting link with France, which renders our jurisdiction perfectly competent to rule in this matter."¹⁷

In specific terms, the order of the Paris county court directed Yahoo! to (a) reengineer its content servers in the United States and elsewhere to enable them to recognize French Internet protocol (IP) addresses and block access to Nazi material by end-users assigned such IP addresses, (b) require end-users with "ambiguous" IP addresses to provide Yahoo! with a declaration of nationality when they arrive at Yahoo!'s home page or when they initiate any search using the word "Nazi," and (c) implement these changes within three months or face a penalty of 100,000 francs (approximately \$13,300) for each day of noncompliance. The French court order also provided that the penalties assessed against Yahoo! Inc. may not be collected from Yahoo! France. In other words, if the plaintiff groups want to enforce the judgment, they must persuade a U.S. court to recognize it and apply it against Yahoo!'s U.S. service.

The French Yahoo! decision cuts sharply against the grain of the emerging jurisprudence in the United States that strongly protects Internet speech because of its global reach. The French view is not that geography is "a virtually meaningless construct on the Internet" but that geography is all-important and should determine which information should be available online. It envisions a world in which Internet surfers must "show their papers" at the border, even when that border exists in a server located wholly outside the nation whose law would be applied. Accordingly, the French Yahoo! decision represents a direct attempt by a foreign nation to apply its law extraterritorially to restrict the freedom of expression of U.S.-based online speakers who are protected by the First Amendment.

You Say That Like It's a *Bad* Thing

The French Yahoo! decision has its defenders—not just among Europeans who sneer at America's "free speech fetish." Supporters include people who evidently would like to see the Internet get its comeuppance. Sebastian Mallaby of the *Washington Post's* editorial page staff cited the Yahoo! case to support his conclusion that "the real story on the Net these days is that the cyberanarchists are losing." He noted the existence of technology "that can pinpoint the

geographic whereabouts of cybernauts." "Once that is done," he concluded, "French surfers can be blocked from Nazi sites while leaving Americans to enjoy the full freedoms of the First Amendment." Such creative use of law and technology debunks "the old cyberanarchist nostrum that national governments can no longer expect to enforce national laws."¹⁸

Mallaby's repeated use of the word "cyberanarchist" as an epithet brings to mind the February 2002 Vatican position paper decrying the "radical libertarianism" of the Internet.¹⁹ The paper notes that a consequence of deregulation has been "a shift of power from national states to transnational corporations" and that the Internet has produced "a mindset opposed to anything smacking of legitimate regulation for public responsibility." That has led to an "exaggerated individualism" and a view of cyberspace as a "new realm" where "every sort of expression was allowed and the only law was total individual liberty to do as one pleased."

In the Vatican's view, "The only community whose rights and interests would be truly recognized" would be "the community of radical libertarians." Such thinking "remains influential in some circles," according to the Vatican paper, "supported by familiar libertarian arguments also used to defend pornography and violence in the media generally."²⁰ Describing the "ideology of radical libertarianism" as both mistaken and harmful to "legitimate free expression in the service of truth," the paper concludes that the Internet "is no more exempt than other media from reasonable laws against hate speech, libel, fraud, child pornography, and pornography in general." Accordingly, it calls for "international cooperation in setting standards and establishing mechanisms to promote and protect the common good."²¹

Coming, as it did, just as stories were breaking about the pedophilia scandals in the Catholic Church and decades of cover-ups, the Vatican paper's theme of "freedom" versus "truth" might seem a bit hypocritical.²² Nevertheless, the pontifical pronouncement dovetails with Mallaby's conclusions that "government must act as the ultimate enforcer" of norms in cyberspace²³ and that the "real debate will not be whether you can enforce rules on the Net but how the enforcers should adapt to the new medium."²⁴ In addition to discussing the French Yahoo! case, Mallaby pointed out that the Chinese dictatorship has found new ways to stifle dissent online:

"The regime blocks out much of the content it dislikes, official news agencies get a new way of disseminating the party line and dissidents become the victims of Web-enabled smear tactics."²⁵ As for regulating pornography, Mallaby notes, "Scary offshore porn sites won't seem so scary anymore. If a government wants to block them, it can tell credit card companies not to process payments to them."²⁶

Mallaby has recognized that applying myriad national laws to cyberspace could cause the Net to "lose some of its borderless appeal" and that we risk converting the World Wide Web to "Numerous National Nets."²⁷ He notes, for example, that an online magazine oriented toward teens could violate the law in countries with severe restrictions on advertising to children. But from the perspective of other countries, Mallaby concludes, there is no reason to abandon local regulation. "If a European country feels strongly about marketing to kids, why should it let American publishers subvert its policies? Countries have varying regulations for the good reason that cultures vary. The Internet won't change that."²⁸

Jack Goldsmith, formerly a professor at the University of Chicago School of Law, agreed with this assessment: "When French citizens are on the receiving end of an offshore communication that their government deems harmful," he wrote, "France has every right to take steps within its territory to check and redress the harm."²⁹ Although Goldsmith assumed incorrectly that "a country can enforce its regulations only against companies with assets in its territory," he described the French Yahoo! decision (which applies primarily to Yahoo! in the United States and not to Yahoo! France) as a "reasonable middle ground." He argued that it is legitimate to force offshore content providers to use filtering technology "to identify recipients of information by geography and screen out content to them."³⁰ Goldsmith acknowledged that such measures will "marginally raise the cost of doing e-business" but concluded that geographical filtering will "force Yahoo! to take account of the true social cost of its auction activities."³¹

A Little Bit Pregnant

Goldsmith's balancing approach assumes that cross-border regulation of the Internet can be carefully calibrated by using technology to keep information out of restrictive jurisdictions while allowing its free availability everywhere else. Unfortunately, the real world

WHO RULES THE NET?

is not so amenable to neat solutions that sound plausible only in academic journals (or in France). The sheer volume of information, much of it posted by third parties, and the fact that it is constantly changing distinguish the type of communication available on the Internet from most traditional communication. Attempting to restrict the availability of information in certain countries on Yahoo!'s auction Web site is not the same thing as declining to publish a book in England because of its plaintiff-friendly libel laws or refusing to mail an adult video to Tennessee for fear of its Bible Belt obscenity standards.

Under the logic of the French Yahoo! decision, an Internet publisher or Web host must create filters to block access to any content that is illegal in the jurisdictions in which its service is available—that is, everywhere. The publisher need not preclude access to all offending content in all jurisdictions but may use geographic filtering to coordinate its blocking decisions with local laws. Even assuming this is technically possible, it presents Web publishers with a daunting task. At least 59 different countries limit freedom of expression online.³² Theoretically, publishers would have to code each item of information they posted (or otherwise made available) to meet each of the national standards, and set their geographic filters to block access to the content in the relevant jurisdictions. A few examples illustrate the widely varying restrictions that would apply.

China

The People's Republic of China severely restricts communication by the Internet, including all forms of dissent and the free reporting of news. The so-called Measures for Managing Internet Information Services are regulations that prohibit private Web sites from publishing "news" without prior approval from Communist Party officials.³³ Another set of laws, known as the "Seven No's," bars the publication of materials that negate "the guiding role of Marxism, Leninism, Mao Zedong, and Deng Xiaoping's theories," go against "the guiding principles, official line or policies of the Communist Party," or violate "party propaganda discipline." Chinese law also bans "content that guides people in the wrong direction, is vulgar or low."³⁴ Armed with that authority, Chinese officials are trying to stop online protest messages available on overseas Web sites, particularly those located in the United States, from which so much pro-democracy speech

emanates.³⁵ Such restrictions pose a particular threat to groups like VIP Reference (also known as Dacankao), the leading Chinese pro-democracy electronic newsletter. Although it is based in Washington, D.C., VIP Reference is read by countless individuals in mainland China.³⁶ If U.S. courts begin enforcing foreign speech standards such as the French law that gave rise to the judgment against Yahoo!, Chinese authorities could pursue similar quasi-civil penalties in the hopes of silencing other pro-democracy speech.

Singapore

The Singapore Broadcasting Authority (SBA) maintains strict control over the free speech activities of that country's Internet users. A U.S. human rights audit explained that the SBA has regulated access to content on the Internet since 1996 by licensing both domestic Web sites and Internet service providers (ISPs). Service providers must install "proxy servers" that filter out content that the government considers objectionable. The SBA directs service providers to block access to Web pages that, in the government's view, undermine public security, national defense, racial and religious harmony, and public morals. In 1997 the SBA announced an Internet Code of Practice to block access to material that contains pornography or excessive violence or that incites racial or religious hatred.³⁷ In July 2001 the government of Singapore imposed new restrictions on political content, which led at least one organization, Sintercom, to shut down its online activities.³⁸

Saudi Arabia

Saudi Arabia bans publishing or even accessing various types of online expression, including "anything contrary to the state or its system," "news damaging to the Saudi Arabian armed forces," "anything damaging to the dignity of heads of states," "any false information ascribed to state officials," "subversive ideas," and "slandering or libellous [sic] material."³⁹ All 30 of the country's Internet service providers (ISPs) are linked to a ground-floor room at the Riyadh Internet entranceway, where all of the country's Web activity is stored in massive cache files and screened for offensive or sacrilegious material before it is released to individual users.⁴⁰ The central servers are configured to block access to "sensitive" sites that might violate "the social, cultural, political, media, economic, and religious values of the Kingdom."⁴¹ Several key overseas Web sites have

received special scrutiny and blocking, including the Movement for Islamic Reform in Arabia—a group based in England. Saudi Arabian authorities have also issued a fatwa against Pokémon, claiming that the popular children's games and cards possess the minds of children while promoting gambling and Zionism.⁴²

Syria

Syria bans many types of content on the Internet, such as statements that would endanger "national unity" or otherwise divulge "state secrets"—categories that include pro-Israeli speech.⁴³ Syrian citizens can be jailed for sending e-mail to people overseas without government authorization. Syrian authorities enforce the bans in several ways, including by intensive surveillance. Online access is severely restricted. There is only one Internet service provider in the country, which is government run and imposes heavy blocking and monitoring schemes.⁴⁴

Australia

The Australian government has issued regulations that bar many forms of expression on the Internet. Amendments to the Broadcasting Services Act require Australian-based content hosts to deny access to sites that lack content-based classifications or are X-rated. In addition, the scheme is designed to deny Australian minors access to any R-rated Web sites. Specifically, access to Internet content hosted outside Australia may be prohibited if the Internet content has been classified RC or X by the Classification Board.⁴⁵ The list of subjects that can be banned as unsuitable for minors includes suicide, crime, corruption, marital problems, emotional trauma, drug and alcohol dependency, death and serious illness, racism, and religious issues.⁴⁶ Violators may be subject to Web site shutdowns and other criminal penalties.⁴⁷

Italy

Italy restricts both online and offline speech in various ways. The Italian constitution contains broad language that forbids "printed publications, performances, and all other exhibits offensive to public morality."⁴⁸ Italy also allows law enforcement agents to seize questionable "periodical publications" under certain conditions.⁴⁹ The ability of the state to regulate speech gains added significance in light of a court decision declaring that those standards should be

applied globally—not just in Italy. A Roman tribunal held that it has the power to shut down foreign Web sites to the extent they can be viewed in Italy.⁵⁰ The court found that “if confronted with a [defamatory statement] initiated abroad and terminated . . . in our Country, the Italian State is entitled to jurisdiction and the meting [out] of punishment.”⁵¹ The court added that “the use of the Internet for defamatory statement embodies one of the cases of aggravation described in Article 595 of the penal code” and that in this case “the sender deserves to be meted a more severe form of punishment.”⁵² The court’s decision may well have been influenced by the fact that the speech at issue contained not only statements about a private party but also “extremely negative defamatory opinions” about “the work of the Italian judicial authorities.”⁵³

Sweden

Swedish laws ban several types of Internet speech, including “illegal description of violence” and “racial agitation.”⁵⁴ Those strictures require the proprietors of “electronic bulletin boards” to remove or make inaccessible such content.⁵⁵ In March 2002 a Swedish court applied those rules to the Web site of the country’s biggest newspaper, *Aftonbladet*, and fined the Web site’s editor for anonymous statements posted to the newspaper’s online comment forum.⁵⁶

France über Alles

Because the French Yahoo! decision applies to Yahoo! U.S., the plaintiffs in that case must seek enforcement of the order by an American court. Normally, courts will enforce such foreign judgments as a matter of international cooperation. But, the Yahoo! case presents special problems: enforcing the judgment here would have practical and legal ramifications that extend far beyond one nation’s law or a single court order. It would establish a legal framework wherein *all* Web sites on the global Internet potentially are subject to the laws of *all* other nations, regardless of the extent to which such a requirement conflicts with the law of the place where the speakers are located. Any finding that the French order may be enforced in the United States portends the development of an international law in which any nation would be able to enforce its legal and cultural “local community standards” on speakers in all other nations. In such a regime, Internet service providers and content providers would have no practical choice but to restrict their speech

to the lowest common denominator to avoid potentially crushing liability.

The impact of such a lowest common denominator approach is not measured by counting the number of nations that already have sought to apply their laws beyond their borders, although that number is growing. It is determined by assessing the effects on Web site operators, considering how the challenged rule "may interact with the legitimate regulatory regimes of other [nations] and what effect would arise if not one, but many or every, [nation] adopted similar legislation."⁵⁷ By that standard, Web publishers could be forced to block access to information that "sabotages national unity" in China; undermines "religious harmony and public morals" in Singapore; offends "the social, cultural, political, media, economic, and religious values" of Saudi Arabia; fosters "pro-Israeli speech" in Syria; facilitates viewing unrated or inappropriately rated Web sites in Australia; or makes available information "offensive to public morality" in Italy—to cite just a few examples.

Many Web publishers and service providers likely would cease offering content that could run afoul of such restrictions. But assuming it is even possible to monitor the various national requirements as they might apply to all of the information available by a particular site, and to calibrate filters accordingly, the effect on Internet communication would be significant. In the international arena, inconsistent regulation of Internet content acts like a "customs dut[y]."⁵⁸ A 1997 White House report on electronic commerce called for a minimum of international government regulation and warned that content regulation "could cripple the growth and diversity of the Internet." The report described content regulations as nontariff trade barriers.⁵⁹ Similarly, the U.S. Department of Commerce has said, "Full realization of the economic promise of information technology depends on the development of the same safeguards and predictable legal environment that individuals and businesses have come to expect in the offline world."⁶⁰

By contrast, refusing to enforce the French judgment would in no way undermine the rule of law in France. France has full authority to regulate the behavior of its citizenry and to require that citizens limit their Web browsing to conform to local norms, just as other nations do. Countries such as China, Singapore, and Saudi Arabia permit their citizens to see only officially approved Web sites and

