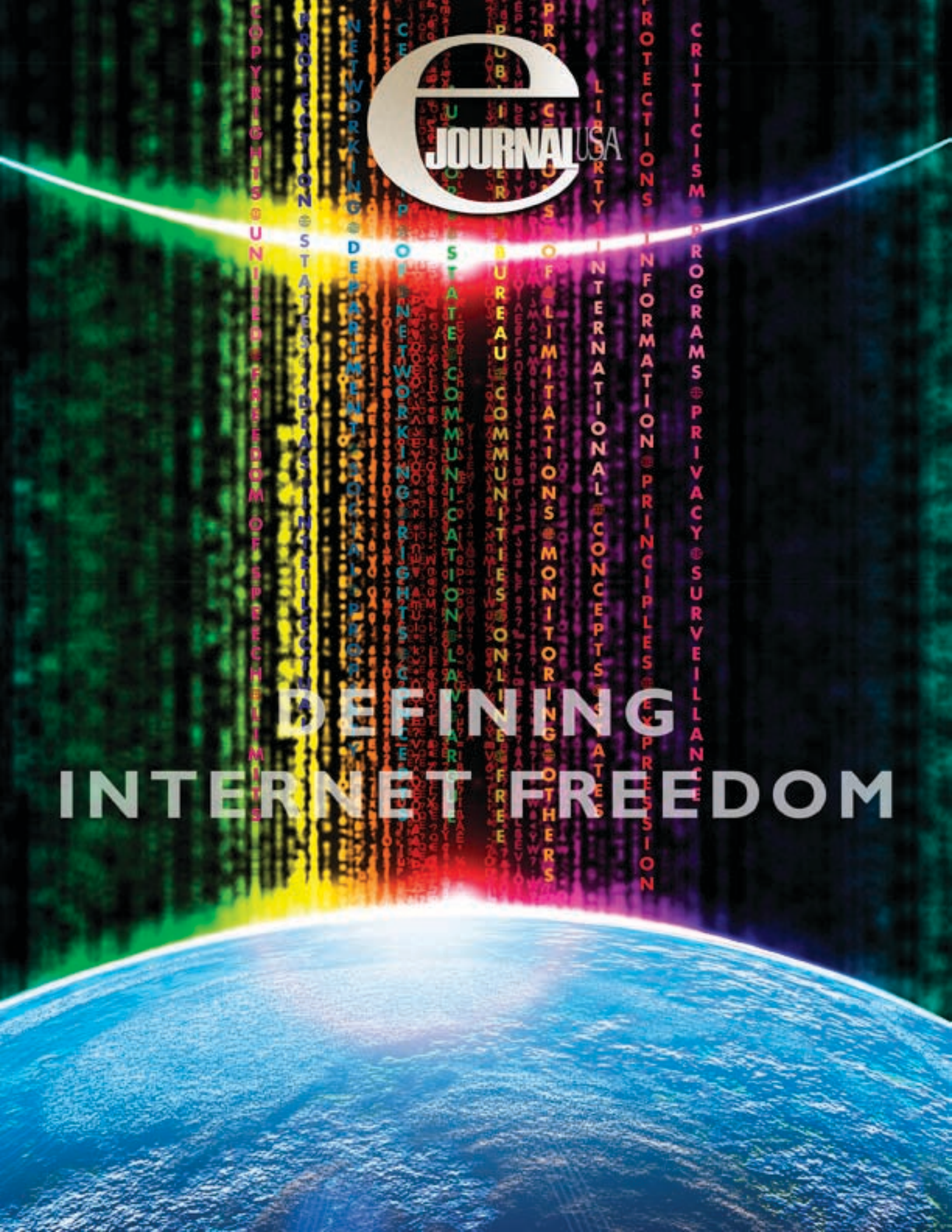

eJOURNAL USA
DEFINING
INTERNET FREEDOM

U.S. DEPARTMENT OF STATE / JUNE 2010
VOLUME 15 / NUMBER 6
http://www.america.gov/publications/ejournalusa.html

International Information Programs:

Acting Coordinator	Duncan H. MacInnes
Executive Editor	Jonathan Margolis
Director of Publications	Michael Jay Friedman
Editor-in-Chief	Richard W. Huckaby
Managing Editor	Charlene Porter
Production Manager/Web Producer	Janine Perry
Designer	Sylvia Scott
Photo Editor	Ann Monroe Jacobs
Cover Designer	David Hamill
Reference Specialist	Martin Manning

The Bureau of International Information Programs of the U.S. Department of State publishes a monthly electronic journal under the *eJournal USA* logo. These journals examine major issues facing the United States and the international community, as well as U.S. society, values, thought, and institutions.

Twelve journals are published annually in English. Each is followed by versions in French, Portuguese, Russian, and Spanish. Selected editions also appear in Arabic, Chinese, and Persian. Each journal is catalogued by volume and number.

The opinions expressed in the journals do not necessarily reflect the views or policies of the U.S. government. The U.S. Department of State assumes no responsibility for the content and continued accessibility of Internet sites to which the journals link; such responsibility resides solely with the publishers of those sites. Journal articles, photographs, and illustrations may be reproduced and translated outside the United States unless they carry explicit copyright restrictions, in which case permission must be sought from the copyright holders noted in the journal.

The Bureau of International Information Programs maintains current and back issues in several electronic formats, as well as a list of upcoming journals, at *http://www.america.gov/publications/ejournalusa.html*. Comments are welcome at your local U.S. Embassy or at the editorial offices:

Editor, *eJournal USA*
IIP/PUBJ
U.S. Department of State
2200 C Street, NW
Washington, DC 20522-0501
USA
E-mail: eJournalUSA@state.gov

About This Issue

© AP Images/Ng Han Guan

© AP Images/Gautam Singh

Governments adopt diverse legal and policy positions in response to increased availability of Internet-based communication technologies. Their motives are similarly diverse, and include cultural norms and political objectives. Internet cafes are part of the street scene in many cities, including (clockwise from top) Beijing, Cairo, and Bangalore.

Speaking in January 2010, Secretary of State Hillary Clinton likened the spread of Internet-driven information networks to "a new nervous system for our planet." "In many respects," she continued, "information has never been so free." But also "we've seen a spike in threats to the free flow of information." How different governments and societies confront these new and transformative technologies is the subject of this journal.

The first part of this *eJournal USA* addresses the difficulty agreeing on a universally applicable definition of Internet freedom. Nations impose many different kinds of restrictions. Some represent the efforts of authoritarian regimes to repress their opponents, but others instead reflect diverse political traditions and cultural norms.

Other materials survey the current state of 'net freedom in different parts of the world. Freedom House, a leading non-governmental organization, has studied government efforts to control, regulate, and censor different forms of electronic social communication. Its findings are explained here.

© Corbis/Mike Nelson

We also explore a number of issues that help define the contours of Internet freedom. The term "intermediary liability" may not pique one's interest, but it assumes new relevance when phrased as whether YouTube is liable for an offensive video posted by a third party. From dancing babies to public libraries, the issues that will delimit global citizens' access to information are being contested every day.

— *The Editors*

U.S. DEPARTMENT OF STATE / JUNE 2010 / VOLUME 15 / NUMBER 6
http://www.america.gov/publications/ejournalusa.html

Defining Internet Freedom

DIFFERENT NATIONS, DIFFERENT FREEDOMS?

4 The Enigma of Internet Freedom
DEREK BAMBAUER, ASSISTANT PROFESSOR OF INTERNET LAW AND INTELLECTUAL PROPERTY, BROOKLYN LAW SCHOOL
Countries and societies define "Internet freedom" differently. While some repressive governments shape the term to suit their own purposes, many other differences are legitimate and value-driven. We should respect the underlying values that drive those decisions.

7 Promoting Internet Freedom Through the Copyright System
PETER K. YU, DIRECTOR, INTELLECTUAL PROPERTY LAW CENTER, DRAKE UNIVERSITY
Internet freedom and intellectual property rights can represent mutually reinforcing or partially conflicting values. Their relationship, and the proper balance between them, depends upon historical, political, social, cultural, and religious contexts.

10 *WHO'S RIGHT?* DEBATING INTERNET CENSORSHIP
DEREK BAMBAUER, ASSISTANT PROFESSOR, BROOKLYN LAW SCHOOL, AND RICHARD A. EPSTEIN, PROFESSOR OF LAW, UNIVERSITY OF CHICAGO
An excerpt from the America.gov *Who's Right?* debate series. Here, two legal scholars address how governments restrict Internet freedom.

ESTABLISHING THE BOUNDARIES

12 Freedom on the 'Net: A Global Assessment
DANIEL CALINGAERT, DEPUTY DIRECTOR OF PROGRAMS, FREEDOM HOUSE
SARAH COOK, RESEARCH ANALYST, FREEDOM HOUSE
A leading nonprofit research organization studied Internet policies in 15 nations and found threats to Internet freedom growing and diversifying.

17 Phones Boost 'Net Access for South Africans
The Freedom House survey examines the rapid increase in mobile phone use in South Africa.

18 Estonia Becomes E-stonia
Estonia became an "e-country" in the years since it regained its independence, according to Freedom House.

INTERNET FREEDOM ISSUES

19 Don't Blame the Messenger: Intermediary Liability and Protecting Internet Platforms
CYNTHIA WONG, ATTORNEY, CENTER FOR DEMOCRACY AND TECHNOLOGY
Holding Internet service providers responsible for offensive materials posted by their customers can slow innovation and expansion of communications technologies.

21 The Global Broadband Divide
A world map illustrates the differences in Internet accessibility in various regions of the world.

22 Dancing Baby Tests Internet Law
KAREN A. FRANKEL, SCIENCE AND TECHNOLOGY WRITER
A young mother posts her baby's antics online and runs afoul of an international pop star.

23 Google Video Slapped with Privacy Violation in Italy
An Italian judge finds Google officials responsible for an offensive online video they did not produce.

24 Public Librarians Help Define Internet Freedom
BARBARA JONES, DIRECTOR, OFFICE FOR INTELLECTUAL FREEDOM, AMERICAN LIBRARY ASSOCIATION
Librarians help defend intellectual freedom and work to balance intellectual property rights with public access to Internet content.

27 Industry Players Take a Stand for Online Freedom
Corporations and nonprofit groups join forces to counter encroachment upon Internet freedom.

28 Breaking Online Barriers
Organizations provide tools for hundreds of millions of Internet users worldwide to find a way around government-imposed censorship.

29 Additional Resources
A selection of books, articles, and Web sites.

The Enigma of Internet Freedom

Derek Bambauer

Countries and societies define "Internet freedom" differently. While some repressive governments shape the term to suit their own purposes, many other differences reflect diverse political and cultural traditions. We should respect the underlying values that drive those decisions.

Derek Bambauer teaches Internet law and intellectual property at the Brooklyn Law School in New York. He also writes Info/Law, a blog that addresses online legal issues.

Rhetorically, everyone supports Internet freedom. "Freedom" though, means quite different things, and carries diverse weights when measured against other interests in various countries and cultures. This normative divergence plays out in debates over access, threats to freedom, online content controls, and governance. In short, the concept of "Internet freedom" holds within it a set of conflicts about how the 'net should function. Acknowledging openly these tensions is better than clinging to wording that masks inevitable, hard choices.

First, access to the network is a prerequisite for enjoying Internet freedom, however defined. [See "Estonia Becomes E-stonia" and "'Net Access Via Phone Serves South Africa," this issue.] States differ, though, on whether individuals are entitled to that access. Some see Internet access — particularly high-speed broadband access — as a right, while others conceive it as a privilege. Finland, for example, has stated that having a 1MB connection is a basic human right of Finnish citizens. Similarly, France's Constitutional Council declared that Internet access is a legal right. The United States, by contrast, views the ability to go on-line as a market good like any other, rather than seeing it as an entitlement. If you can't afford to connect to the 'net, you remain offline, or dependent on publicly available access sites at libraries and schools.

Whether Internet access is treated as a right or a privilege also holds implications for loss of that access. The United Kingdom's new Digital Economy Act sets up a "graduated response" system that would suspend users' accounts if they are repeatedly accused of online copyright infringement. France's HADOPI (French acronym for the nation's law promoting the distribution and protection of creative works on the Internet) regime similarly disconnects users after three allegations of infringement. Thus, even states that establish access as a right balance it against other considerations, such as protecting intellectual property owners. [See "Promoting Internet Freedom Through the Copyright System," this issue.] That balancing act is the key to differing conceptions of Internet freedom.

© AP Images/Richard Vogel

An Internet café in Hanoi. The Vietnamese government blocks access to pornographic and other "unhealthy" material. The author suggests that its real objective is to block human rights and political dissent content.

Second, societies vary on the orientation of Internet

freedom — in short, free from whom, or from what? One key threat is government. States can impinge online liberties in numerous ways, such as by criminalizing speech or conduct, by monitoring communications, or by blocking material. American views on freedom are typically concerned foremost with preventing unchecked government power. But there are other threats as well. For example, European countries are often wary of the power of corporations to gather private, personally-identifiable information about users. Recent controversies over Facebook's privacy settings, Google's video service in Italy, and Google's Street View geo-mapping project demonstrate the worry over remaining free from private sector data gathering as well as governmental surveillance.

In addition, countries may seek to prevent impingements on one's freedom generated by other users — for example, the harm to one's reputation that occurs from false and defamatory content. Some states press intermediaries such as Internet service providers and social networking sites to police this kind of material via the threat of liability, while others provide immunity for anyone but the author. Countries thus demonstrate a range of concerns about threats to freedom.

Third, nations balance differently freedom of expression, and access to information, against concerns about the harms that online material can cause. Those harms can be to individuals (as with defamation), to identifiable groups such as religious or ethnic minorities, or even to shared societal values. The United States views the free exchange of information as sufficiently weighty to displace many competing concerns, which is why material such as hate speech and pornography is protected by its constitution. However, U.S. law does prohibit certain types of information, such as true threats, obscene materials, and child pornography. France and Germany also strongly protect open expression, but ban hate speech online. For example, the countries require Google to filter hate speech sites from its search results on its local language sites. Singapore formally bans pornographic content online, and blocks users from a small set of such sites as a symbolic measure. Saudi Arabia, a country where the majority of citizens are followers of the Sunni branch of Islam, prevents access to certain religious content contrary to Sunni beliefs, such as sites on the Baha'i faith or on the Shia branch of Islam. In short, if we view Internet freedom as protecting unfettered expression, this liberty is counterbalanced to varying degrees by competing concerns, even in countries with strong traditions for protecting speech.

Lastly, countries differ on who should govern

© AP Images/Rob Griffith

Sydney, Australia. The Australian government has proposed a mandatory Internet filtering regime. Opponents charge it is too broad.

Internet freedom, and how it should be implemented. Debates over Internet governance are nearly as old as the commercial 'Net itself. The United States created the Internet's initial architecture, and retains a baseline level of control over its workings through the relationship between the Department of Commerce and ICANN (the Internet Corporation for Assigned Names and Numbers), which runs the Domain Name System among other tasks. The United States has resisted transfer of ICANN's functions to other entities based, in part, on a concern that placing the Internet under international control would weaken freedom — in particular, freedom of expression. Other states, though, seek a greater voice in decision-making about the 'net's underlying protocols and standards, and do not want the network to be locked into American conceptions of the proper balance among demands such as security, privacy, and open expression. This has led to heated debate in fora such as the World Summit on the Information Society (WSIS) and to the creation of consultative bodies such as the Internet

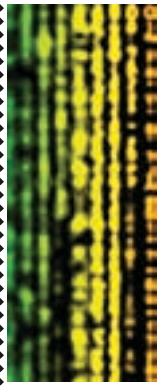
Governance Forum (IGF). Thus, countries not only differ on what constitutes Internet freedom, they also diverge on how it should be achieved in practice.

Freedom is a loaded term. It holds rhetorical power; portraying one's opponents as averse to Internet freedom is a potent tactic. What makes Internet freedom a difficult goal to achieve is that adherents employ the same term for a range of meanings. Freedom can be conceived of as strongly individualistic, where users are free to act as they please so long as they do not directly harm others. Or, it can be viewed as community-based, where privileges depend upon compliance with a societal framework of rules and norms. Freedom can shield us from interference by states, by companies, and by each other. It can dictate that we have a right to go online, or that we have the opportunity to do so. Internet freedom is thus a dependent term: Its meaning varies with context.

This mutability carries risk, though. Governments may argue that their societies have an understanding of Internet freedom that justifies certain actions while, in fact, those steps are for the benefit of the governing, not the governed. Vietnam, for example, blocks access to certain online material based putatively on concerns about exposure of minors to unhealthy material such as pornography. Yet, the state's system prevents users from reaching sites on human rights and political dissent, while failing to block even a single pornographic page. Plainly, Vietnam's government is engaged in pretextual behavior. We should be alert to the risk that states will employ legitimate differences about the normative content of "freedom" online as a cover for activities that undermine that liberty.

Perhaps, in the end, Internet freedom is a term that should be abandoned as too general to be useful. Instead, countries, cultures, and users should grapple with the difficult tradeoffs that Internet communication presents. The 'net empowers pamphleteering as well as pornography. Anonymous communication can be used to inform about political corruption and to infringe intellectual property untraceably. Data aggregation can personalize one's online experience, or profile one's communication and activities. Being explicit about the compromises we make, and being respectful of the underlying values that drive those decisions, will serve us better than using "Internet freedom" to build a false sense of consensus. ■

The opinions expressed in this article do not necessarily reflect the views or policies of the U.S. government.



INFO BYTES

1.9 billion people worldwide had access to a computer at the end of 2009.

Promoting Internet Freedom Through the Copyright System

Peter K. Yu

Policy makers interested in promoting freedom and creativity in their nations need to design a copyright system that mutually promotes and protects intellectual property rights and Internet freedom.

Peter K. Yu holds the Kern Family Chair in Intellectual Property Law and is the founding director of the Intellectual Property Law Center at Drake University Law School in Des Moines, Iowa.

© AP Images/Eric Risberg

The tension between creative freedoms and intellectual property protections has been tested on the online video site YouTube, founded by Chad Hurley, left, and Steve Chen, right.

Internet freedom and intellectual property rights are complementary protections, but they sometimes imply competing values, resulting in conflicts. Because these conflicts vary according to historical, political, social, cultural, and religious contexts, the intellectual property standards each country has fashioned have different ramifications for the protection of Internet freedom.

The Benefits of Copyright Protection

In many countries, including the United States, copyright protection helps sustain an independent creative sector. Before the emergence of copyright, writers, musicians, playwrights, and other creative artists relied upon state sponsorship and elite patronage. With this support came constraints on artistic freedom. Brave were those artists who dared to offend their supporting patrons or, worse, risked their lives for the sake of art.

Copyright protection solves this dilemma. By granting exclusive rights to profit, copyright enables artists to recoup their investment in time, effort, and resources. It allows them to create and disseminate works according to their interests, tastes, and talents. It also protects them against pressure from government or wealthy patrons.

Copyright serves the same function on the Internet. Although many netizens have created and disseminated content online without any commercial motivation, copyright enables online artists to reap rewards when and where they choose. Just as in print or on a canvas, copyright allows artists to create without constraints imposed by others. It gives them an important form of Internet freedom.

Balancing Between Competing Freedoms

Unfortunately, the freedom of Internet creators sometimes conflicts with that of Internet users. Because

copyright law restricts the users' ability to reuse stories, artwork, photos, music, and videos they find on the Internet, users complain about their lack of freedom online.

To strike a balance between these competing freedoms, copyright law includes an array of limitations, exceptions, and defenses. For example, the law distinguishes between unprotectable ideas (all humans are equal) and protectable expressions (an essay arguing for human equality). It also allows for fair use of copyrighted content, such as quoting a passage, writing a book review, or making a parody. Although copyright law does not afford Internet users unlimited freedom, it actively balances this freedom against the freedom of Internet creators.

A Different Balance for Repressive Countries

In countries that heavily restrict information flows or substantially control local cultural industries, greater conflict between Internet freedom and intellectual property rights may arise. While support of an independent creative sector is important, enabling the public to express itself online is equally important. Under certain circumstances, the need for the latter outweighs that of the former.

In those situations, Internet users have a strong need to reuse without permission materials previously approved by censors or that are only available abroad. For example, to provide an alternative source of information, users may need to repost copyrighted stories, videos, or photos that otherwise would not have been available. They may also need to repurpose preexisting materials to address issues that they otherwise cannot discuss because of government censorship.

In repressive societies, parodies, satires, coded words, euphemisms, and allusions to popular culture have become dominant vehicles of communication. Materials seemingly unrelated to the original intended message are often used to create associations, build in tacit meanings, provide emotional effects, and ultimately avoid censorship. Whether it is a remix of video clips from Western movies or the synchronization of content to rock 'n roll songs, repurposed contents carry within them rich hidden meanings that provide important social commentary.

Although we sometimes distinguish works that are of public interest — such as news stories — from those that are created for commercial or entertainment purposes, this type of distinction is usually unhelpful in countries where circulation of information is limited. Although many entertainment products are uncontroversial, highly commercial, and seemingly frivolous, they nonetheless may contain useful political information.

It is, indeed, not uncommon to find movies or television programs portraying different forms of government, the need for checks and balances or separation of powers, and the protection of constitutional rights and civil liberties. While these commercial products may have been created to provide entertainment, in some countries they also supply an important window to the outside world.

Moreover, not everybody can be an original artist. Nor is it ideal for everybody to do so, given how some governments have mistreated artists and original thinkers. In some countries, reusing, sampling, or repurposing materials drawn from popular culture can be an effective means of capturing public attention and imagination. Because these materials are created and copyrighted by others, conflict can arise between Internet freedom and intellectual property rights.

If the copyright system strikes an inappropriate balance between these two forms of protections, citizens in a repressive country will have fewer opportunities to creatively reuse existing materials. With fewer politically secure ways to express themselves, they will also be less empowered to speak. In the end, they will have fewer

© AP Images/Pablo Martinez Monsivais

Actor and recording artist Todd Smith — stage name LL Cool J — testifies at a U.S. Senate hearing on illegal sharing of online music files.

opportunities to engage in civic debate, foster democratic self-governance, promote ideological and expressive diversity, and ultimately provide political, social, and cultural change. The development of civil society will be stifled.

Potential Abuse of Copyright Protection

Intellectual property protection has sometimes been used as a pretext to silence dissent. Where reused materials are copyrighted, political authorities can easily claim copyright infringement without admitting censorship. Copyright protection, while fully legitimate in other contexts, has unfortunately been used in this context to provide legitimization for actions that may violate human rights.

Required monitoring of Internet users is another growing and disturbing trend. Here, governments require Internet service providers to facilitate copyright protection by monitoring users, filtering web content and retaining data about subscriber activities. The similarities between these requirements and those of censors are obvious. After all, copyright started in England as a political tool to suppress heresy and dissent.

Internet surveillance for copyright purposes can be as dangerous as Internet surveillance for censorship purposes. Political authorities, for example, can easily ask Internet service providers to turn over information about their subscribers' potentially illegal online activities, such as copyright infringement. This information could lead to arrest, harassment, intimidation, or detention of Internet dissidents. It could also be used as evidence to substantiate prison sentences.

Even worse, the collection of subscriber information can lead to self-censorship. If Internet users fear that officials would use the collected information to reconstruct past Internet activities, they might become more reluctant to discuss sensitive matters online. A vicious cycle would emerge. Not only would Internet users enjoy less freedom, they also would have fewer incentives to create — precisely the opposite result copyright intends to achieve.

The Need for a Proper Balance

The protection of intellectual property rights can be a boon for Internet freedom, but it can also be a bane. For each to beneficially reinforce the other, the intellectual property system must be harnessed to promote Internet freedom. In countries where information flows are heavily restricted, the balance in copyright law may need further adjustment to reflect the drastically different local circumstances.

To promote greater Internet freedom, policymakers need to pay special attention to the limitations and exceptions to copyright. For example, they can introduce the fair use doctrine, the parody defense, an exception for educational use, or limitations on adaptation rights. They can also confine criminal penalties to commercial-scale piracy, as opposed to ordinary infringement by Internet users.

By introducing these balancing measures, policymakers will be able to turn the conflict between Internet freedom and intellectual property rights into an opportunity for creating useful and synergistic complements. Combined together in a constructive way, Internet freedom and intellectual property rights will help citizens realize the full potential of the Internet. They will also provide freedom for both Internet creators and Internet users. ■

The opinions expressed in this article do not necessarily reflect the views or policies of the U.S. government.

Who's Right?
Debating Internet Censorship

The Who's Right *debate series, found at* http://www.america.gov/whos_right_archives.html*, engages experts to explore controversial issues in a debate format. Recently, Professors Derek Bambauer (Brooklyn Law School) and Richard A. Epstein (University of Chicago Law School) addressed the subject of Internet censorship. Excerpts from their encounter appear below.*

Derek Bambauer: We live in a world of ubiquitous Internet censorship and surveillance. Tech companies confront these questions not just when doing business in China or Egypt or Pakistan, but in Australia and India. America requires telecommunications companies to build wiretapping capabilities into their products and services; once spying is part of the core functionality of, say, Internet telephony, it's available to countries whose snoops are far less restrained than the FBI.

We should acknowledge that China, Australia and Ethiopia do the same thing: They restrict access to content online through both technology and law, and they spy on Internet communications. Thus, we need a new way to guide business decisions about when to participate in filtering and surveillance, because the binary world — censorship or freedom — no longer exists.

My response to this is a bit radical: I think there are circumstances under which countries can legitimately censor the Internet. (It's less controversial to concede that states can spy on their own citizens at times — every country has a long history of doing so.) I argue that the key factors determining legitimacy are found in the process by which a country arrives at the decision to filter the Net, and how precisely it blocks content in practice.

Richard Epstein: You suggest that it is hard to tell which reasons are valid because nations filter different kinds of Internet content. I am not so sure this is correct. Do we have one attitude toward the Chinese who restrict political speech? Another to the folks in Mumbai who block the speech only of extremist Hindu groups? A third to the French who ban images of white supremacist groups? What about New Zealand's decision to block child pornography? And yes, the United States' decision to block the unauthorized use of copyrighted material? Five countries with five different agendas….

you suggest that we turn instead to procedures — how the governments made these decisions…. I disagree. My entire constitutional career as a classical liberal scholar has persuaded me that we should judge legislation and other government action by what it does. I am more confident that we can find the right principles to look

at the output of the process than by guessing about the many ways that different nations make their laws. I see no reason why a bad law that comes out of good processes should be tolerated. At the same time I see no reason why good laws that emerge, as if by chance, from less democratic political processes should be condemned.

Derek Bambauer: Your methodology is appealing because it looks at ends and not means. I would be interested to hear more — what values should we prioritize in assessing censorship? Do they derive from American thinking, or are they more universal? I worry that an approach grounded explicitly in U.S. values is likely to draw resistance from outside actors whose help we need. Other countries are often reluctant to appear to yield to overtly American standards, whether due to conflicts with their own values or because their governments fear being painted as lackeys. Yet, a universal approach risks weakening core commitments as the price of achieving consensus. An approach driven by one country's ideas about information seems impractical.

Substance-based decisions call upon tech firms to make very fine-grained decisions about what is inflammatory and what is simply critical. Should YouTube, for instance, accede to demands from Iran's government to take down video of Neda Salehi Agha Soltan's shooting on grounds it could inflame protests in that country? The line between inflammatory material and content that critiques a government is hard to draw.

The British and the American colonists certainly disagreed about Thomas Paine's writings, for the same reasons that Burma restricts information from Aung San Suu Kyi and the National League for Democracy. Here, the process-based analysis may provide clearer rules for firms, letting them make faster and cheaper decisions (as well as, we hope, better ones). Iran's decision-making methods for filtering are arbitrary, lack opportunities for participation, and lack transparency; YouTube should reject any request to take down the video of Neda's shooting out of hand.

Richard Epstein: I remain a universalist on matters of morals and ethics. My training in Roman law has convinced me that just social relations do not differ in fundamental ways across societies. What do differ are the formalities and institutions used to enforce these bedrock principles. The U.S. Constitution is relatively successful because it accepts the universal standards of sanctity of property and contract that require government control of aggression and fraud. These values are not distinctively American but are found in both Roman and English systems across the globe. Nor did the American founders regard these principles as distinctively American. They were happy to learn and borrow from others. ■

The opinions expressed in this article do not necessarily reflect the views or policies of the U.S. government.

Freedom on the 'Net A Global Assessment

Daniel Calingaert and Sarah Cook

© AP Images/Javier Galeano

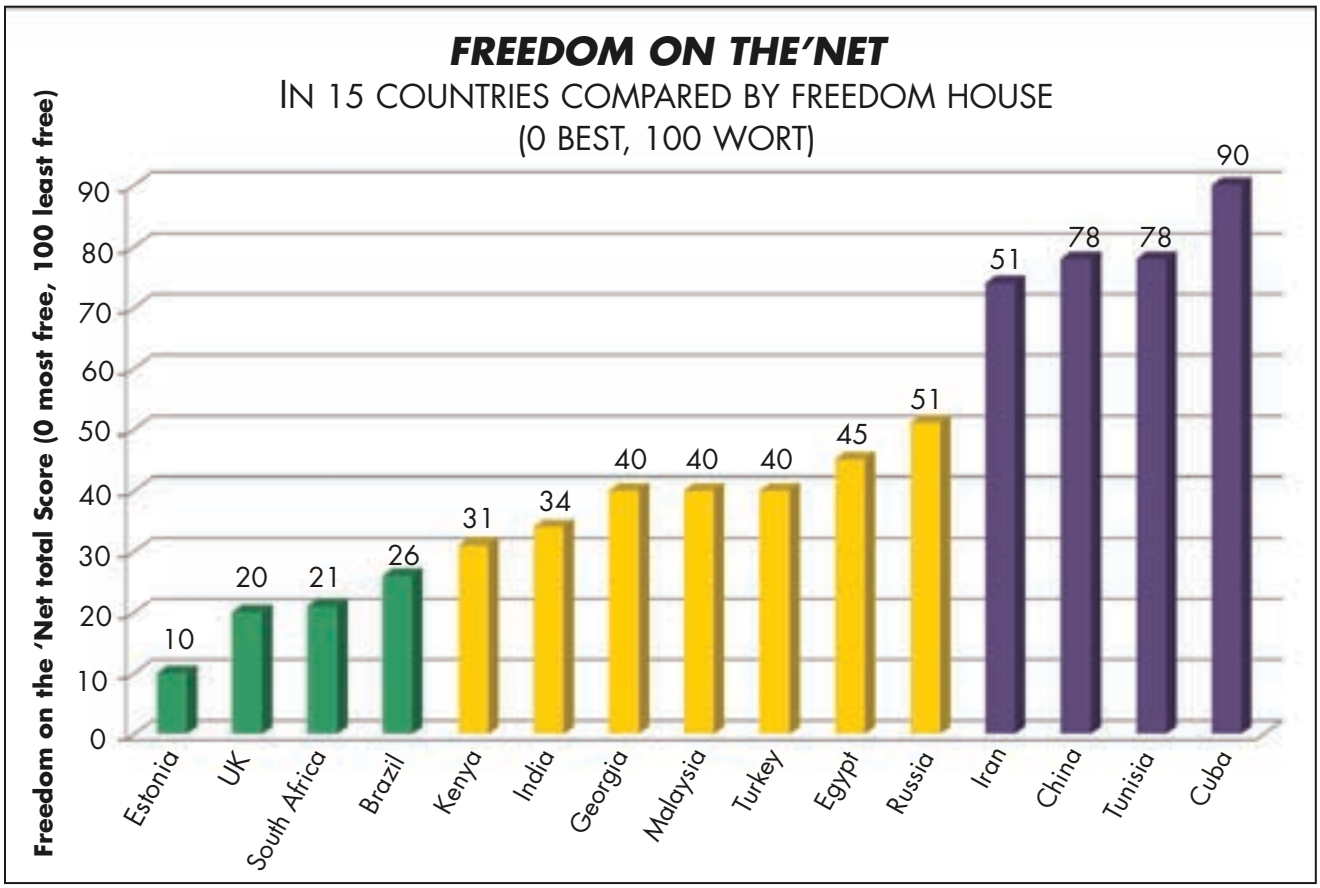
Yoani Maria Sánchez Cordero has become internationally known for her blog. Generation Y, despite the Internet restrictions imposed by the Cuban government. The Freedom House survey ranks Cuba as the least free of the 15 nations studied.

Even as the Internet offers citizens greater means of expression, a leading nongovernmental organization reports that many governments seek to restrict Internet access and content.

Danliel Calingaert is deputy director of programs at Freedom House, a nonprofit organization receiving funding from the U.S. State Department, Google, and other sources to promote Internet freedom. Sarah Cook is a research analyst specializing in Asia. She served as assistant editor for the 2009 publication Freedom on the Net.

As access to online technologies has grown exponentially in recent years, the Internet has increased opportunities to enrich public discourse, expose abuses of power, and facilitate citizen activism. It has provided greater space for free expression in both democratic settings and countries where traditional broadcast and print media are restricted. Many governments have responded with measures to control, regulate, and censor the content of blogs, Web sites, and text messages.

These developments raise several fundamental questions: What are the primary threats to Internet freedom? Will the Internet bring freedom to oppressed people or will it strengthen the power of repressive regimes which control it? Are democratic societies immune from Internet repression or are threats to digital media freedom emerging there as well?



The international NGO Freedom House examined the state of Internet freedom in 15 selected nations. A green-colored bar (far left) represents a status of "Free," a yellow-colored one, the status of "Partly Free," and a purple-colored one, (far right) the status of "Not Free" on the *Freedom on theNet index.*

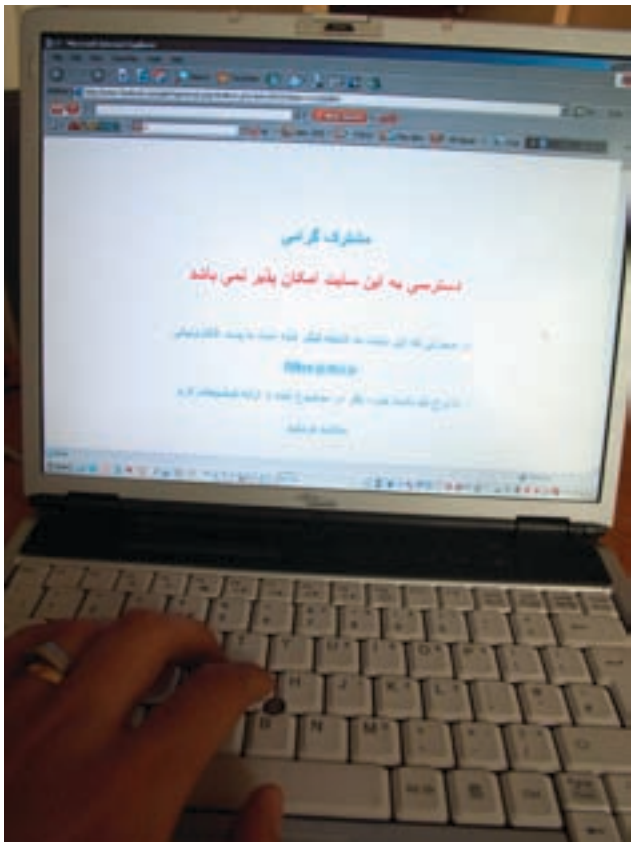
Freedom House explored these questions in Freedom on the Net, a 2009 survey that rated Internet freedom in 15 countries, spanning four continents and covering a range of national regulatory environments from free to highly repressive. According to the findings, threats to Internet freedom are growing and diversifying both in the array of countries that impose restrictions and in the range of methods employed.

Authoritarian rulers understand the power of the Internet and are actively curtailing its impact. A few highly repressive governments — such as that of Cuba — restrict access to a very small segment of the population. There are few public Internet access points, and the cost of service is prohibitive for the vast majority of citizens.

Other authoritarian governments, such as those in China, Iran, and Tunisia, actively promote Internet use to stimulate innovation and economic growth, but place wide-ranging controls over digital media to prevent their use by government critics. These regimes maintain extensive, multilayered systems of censorship and surveillance to stifle online dissent or exposure of official corruption. They place severe limits on the content that citizens can access, post on the Internet, or transmit via cell phones. Surveillance of Internet and mobile phone communications is pervasive, and citizens who criticize the government online are subject to harassment, imprisonment, and torture.

In less restrictive settings, for instance in Egypt, Malaysia, and Russia, the Internet has emerged as a haven of relatively free speech in otherwise restrictive media environments. The space for free speech, however, is slowly closing, as governments devise subtle methods to manipulate online discussion and apply deliberately vague security laws to intimidate and arrest their critics. This intimidation leads to self-censorship among online journalists and commentators.

Even in more democratic countries — such as the United Kingdom, Brazil, and Turkey — Internet freedom is increasingly undermined by legal harassment, opaque filtering procedures, and expanding surveillance.



ATTA KENARE/AFP/Getty Images

Iran ranked among the least free nations in Internet policy. Signing on to Facebook led to this Farsi message, "Access to the site is not possible" during one government crack down in May 2009.

Web 2.0

Just as the number of Internet users has grown exponentially since 2000, the second generation of Web design and the emergence of online social networks has empowered average users to produce and disseminate information. Where traditional media transmit information vertically to audiences, Web 2.0 applications spread information horizontally, and have thus profoundly affected how we communicate.

Tens of millions of ordinary citizens around the world have become content publishers and distributors. They write online journals; produce videos; investigate sensitive issues; and comment on political, social, and other topics. In restricted media environments, bloggers often stand at the forefront of efforts to push the bounds of free expression. Web 2.0 applications promote not only independent expression but also freedom of association. They facilitate discussions and interactions among individuals, regardless of physical location. They build online communities of citizens with shared interests and make possible the rapid spread of information, such as news updates or calls to action. Digital media are thus used extensively for civic activism. In Kenya, activists launched an initiative called Ushahidi during a burst of postelection ethnic violence in 2007. It catalogued incidents using messages sent by ordinary citizens with their mobile phones and posted them onto a map to track the unfolding events. The program has since been deployed again in the context of other tumultuous events: elections in India, fighting in Gaza, and earthquake relief in Haiti.

As a result of its horizontal configuration, the Internet usually provides greater space for free expression than traditional media. All of the countries surveyed in Freedom on the Net, with a single exception, received a higher rating for Internet freedom than for overall media freedom, as measured on the same scale by Freedom House's Freedom of the Press survey. The difference in ratings for Internet freedom and traditional media freedom was most pronounced among countries ranked "partly free."

Repression 2.0

The horizontal nature of the Internet both empowers citizens in ways that traditional media cannot, and makes the flow of information far more difficult to control. Regardless, authoritarian governments try to restrict horizontal communication and impede the spread of domestically generated content they find objectionable. Although the primary aim is to silence domestic critics and prevent the emergence of political alternatives, the controls imposed to accomplish this necessarily are more intrusive and directly affect larger numbers of people than restrictions on traditional media.

Several countries have developed an array of censorship and surveillance methods to curtail Internet freedom:

- Access to Web 2.0 applications such as Facebook and YouTube is blocked permanently or temporarily. These blocks are often imposed around particular events, as the Chinese government did during the 2009 unrest in Xinjiang. Burma cut off all access to the global Internet for several days in 2007 after the violent crackdown on peaceful protests in the "Saffron Revolution." Iran denies home and Internet café users access to broadband.

- Technical filtering at the level of Internet service

providers (ISP) prevents access to specific online articles or Websites. Where employed more extensively, the filters effectively "black out" broad swaths of information. Filters can target keywords, particular Web addresses, or entire domain names. At least 25 countries, according to the Open Net Initiative, conduct technical filtering of the Internet in some capacity.

- Human censors monitor and manually remove blog posts. They shut down online discussion forums that address forbidden subjects, such as human rights violations, criticism of political figures, or official corruption. Authorities in Russia and elsewhere resort to behind-the-scenes phone calls to pressure bloggers or Web site hosts to remove certain content.

- Rather than rely entirely on direct intervention by government agencies, some regimes increasingly "outsource" censorship and surveillance to private companies — to Internet service providers, blog-hosting companies, cybercafés, and mobile phone operators. Companies risk fines or loss of business licenses if they fail to filter political content, monitor Internet activity, or collect data on Internet users. Users are required to register with an ISP when they purchase Internet access at home or at work, so they cannot operate online anonymously.

- A number of governments use clandestine, paid pro-government commentators or state-funded Web sites to influence online discussions. The Chinese government employs an estimated 250,000 or more "50 Cent Party" commentators, who reportedly receive 50 Chinese cents for each pro-government post.

- Authoritarian governments use general press laws against insult, blasphemy, leaking state secrets, etc. to punish online dissidents. Cuba prosecutes online journalists under generic charges such as presenting a "pre-criminal social danger." China has issued more than 80 decrees that specifically address Internet-related issues and imposes among the harshest prison sentences in the world for online violations, typically between three and ten years. Numerous prosecutions have also occurred in Tunisia, Iran, Syria, Egypt, and Malaysia, where laws against insulting the head of state or Islam are most frequently invoked. According to the Committee to Protect Journalists, for the first time in 2008, more online journalists were behind bars than traditional journalists, due to either legal prosecution or extralegal detention.

- When not imprisoned, bloggers and online journalists face intimidation, including 24-hour surveillance, harassment, arbitrary arrest, and even torture. Egypt permits a relatively open Internet environment but targets a few prominent individuals to make an example of them and create a chilling effect on their peers.

- Blogs and Web sites are hacked or subjected to denial-of-service attacks, which disrupt or shut down the sites. On the first anniversary of Burma's Saffron Revolution, for example, independent news Web sites hosted in Thailand, such as the Irrawaddy and the New Era, became targets of cyber attacks.

> In 2008, more online journalists were behind bars than traditional journalists, due either to legal prosecution or extralegal detention.

The full panoply of repressive methods is used to control the Internet in the most restricted environments, for instance in China, Iran, and Tunisia, ranked "not free" in Freedom House's study. They have developed sophisticated, multilayered systems to control the free flow of online information.

Other countries, such as Egypt, Malaysia, and Russia, allow substantial freedom online but seem headed toward greater controls. They encourage expanded access to the Internet and rarely directly block online expression, despite their heavy restrictions on traditional media. However, they exert more subtle state influence on content via proactive manipulation or behind-the-scenes pressure, repress citizen attempts to mobilize online, and impose harsh penalties on their online critics. Freedom House ranks these countries "partly free."

Internet Freedom and Restrictions in Democratic Settings

Countries that scored in the "free" range in the Freedom on the Net study included Estonia (the best performer in the pilot sample), the United Kingdom, South Africa, and Brazil. These countries all have a generally open environment for new media, with few or no government obstacles to access, a low level of content control, and few violations of users' rights. Democratic settings have also shown the capacity for "self-correction" following public exposures of restrictions on Internet freedom. In Turkey, a parliamentary inquiry was launched into surveillance practices by law enforcement agencies following a series of scandals.

Even within these relatively free environments, however, areas of concern have emerged.

In Brazil, judicial decisions that lead to content censorship are a growing threat, while YouTube has been blocked repeatedly both there and in Turkey. Meanwhile, in countries such as the United Kingdom or Turkey, censorship decisions are made with a serious lack of transparency, even if the information targeted is primarily small amounts of well-defined content, such as child pornography. The lack of public lists of blocked Web sites or opportunity to appeal censorship decisions creates the risk of restrictions spreading to politically and socially important information.

Citizens Fight Back

Despite the growing range of threats and controls, citizens operating even in highly Internet-restricted environments are findings creative ways to produce and spread information. In Cuba, with its tight controls on access, citizens share downloaded Internet content offline, often through USB devices, a phenomenon termed "sneakernets." In China, persecuted Tibetans, Uighur Muslims and Falun Gong practitioners have used digital media to send abroad documentation of torture, while domestically challenging Communist Party propaganda via blogs and underground DVDs. In Tunisia, the blog NormalLand discusses Tunisian politics by using a virtual country with a virtual leader, and with various government positions being assigned to other local bloggers.

Citizens have also been able to use the Internet and mobile phones for activism against censorship itself. In 2009, Chinese netizens organized online resistance to the planned introduction of Green Dam Youth Escort censorship software. Domestic criticism — expressed via social networking tools and online petitions — along with foreign pressure persuaded the Chinese government to delay the large-scale introduction of Green Dam.

The broader political implications of online activism are especially striking in "partly free" internet environments. In Egypt, the Facebook group Elbaradei for Presidency has attracted more than 235,000 members in approximately five months. Malaysia's opposition political parties conducted a large part of their March 2008 general election campaigns through digital media — including blogs, YouTube and SMS (short message services on mobile phones), which contributed to unprecedented ballot-box gains.

Conclusion

Digital media technologies promise improved flow of information, enhanced civic participation and activism, and ultimately, greater freedom and quality of life. Nonetheless, the "Freedom on the Net" pilot study amply documents that this potential cannot be taken for granted. As Freedom House prepares a second, 37-country edition of the study for release in 2011, this has become more evident. From Kazakhstan and Belarus to Australia, restrictive new laws have been approved or are being considered.

Vigorous efforts by netizens and their advocates in democratic countries are a necessary response to these and other restrictions on online freedom. In a fast-changing digital world, the proponents of free expression must take the initiative to defend and advance freedom on the Internet. ■

The opinions expressed in this article do not necessarily reflect the views or policies of the U.S. government.

Phones Boost 'Net Access for South Africans

South Africans enjoy a high degree of digital media freedom, according to the *Freedom on the Net* survey. As of 2008, 9.5 million South Africans accessed the Internet via mobile phones, slightly more than double the number of those who connected via computers.

Price is the chief reason South Africans use their phones to reach the Internet. Mobile phone subscriptions offer online access with some of the world's lowest fees for the service. Several companies in South Africa provide mobile phone Internet service, while only one company provides fixed line Internet service. With the total number of mobile-phone subscribers estimated to be 45 million, Internet connections via mobile phone likely will continue to outpace those on broadband. Various factors are working to increase competition in broadband access in the near future, the Freedom House study says, which may lower the costs of a fixed line.

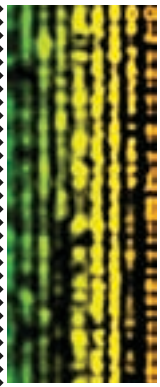
The government has not imposed restrictions on Internet access, and no reports indicate that the authorities use control over Internet infrastructure to limit connectivity. The South African panel regulating the industry acts with autonomy, according to Freedom House research. Access providers and other Internet-related groups are self-organized and quite active in lobbying the government for better regulations. Individuals and groups can engage in peaceful expression of views using e-mail, instant messaging, chat rooms, and blogs. The video-sharing site YouTube, Facebook, and international blog-hosting services are freely available.

© AP Images/Denis Farrell

Cell phone users worldwide are able to send a birthday greeting to Nelson Mandela in a campaign launched by his charitable foundation.

The predominance of English on the Internet does act as a persistent obstacle to potential South African users who speak only local dialect, concludes the Freedom House report.

This summary is based on original findings from Freedom on the Net: A Global Assessment of Internet and Digital Media*, a 2009 report from Freedom House.*



INFO BYTES

64 percent of the residents of developed world nations and **18** percent of people in developing world countries use the Internet.

Estonia Becomes E-stonia

Estonia ranks among the most wired and technologically advanced countries in the world with high levels of computer literacy and connectivity, according to the Freedom House survey of Internet freedom. The Baltic nation's status as an advanced "e-country" stems from a government initiative to vault Estonia into the global economy after it regained independence in the early 1990s.

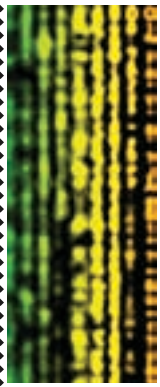
The number of Estonian Internet and mobile phone users has grown rapidly in the past 15 years. Two-thirds of the population, approximately 852,000 people, regularly access the Internet. Fifty-eight percent of households have Internet access, and 90 percent of those have a broadband connection. The country supports more mobile phone accounts — almost 2 million — than there are people. The government has also worked aggressively to broaden the availability of wireless broadband access for general public use in cafés, hotels, motels, and even gas stations.

Estonians use the Internet for many activities, including search engines, e-mail, local online media, news portals, social networking sites, instant messaging, and Internet voice communication solutions. Additionally, 83 percent of the population uses the Internet for online banking — the second highest percentage in the European Union.

Limits on Internet content and communication in Estonia are among the lowest in the world. Estonia has thorough privacy laws, and Estonian courts have ordered deletion of inappropriate comments posted to online articles. Generally, users are informed as to the media portals' privacy policy for commenting and are expected to follow the instructions.

The most serious threat to Internet freedom in the country in recent years was a spate of cyber attacks against Estonia's communication infrastructure in the spring of 2007. At that time, a series of "dedicated denial of service" (DDoS) attacks affected all of the government's Web sites, Estonia's largest bank, and the sites of several daily newspapers. In the aftermath of the attacks, however, Estonia has emerged as a world leader in cyber security, establishing the NATO Cooperative Cyber Defence Centre to provide cyber defense support for all the alliance's members.

This summary is based on original findings from Freedom on the Net: A Global Assessment of Internet and Digital Media*, a 2009 report from Freedom House.* ■



INFO BYTES

The cost of information and communications technologies services dropped an average of **15** percent between 2008 and 2009 in **161** nations surveyed by the International Telecommunications Union.

Don't Blame the Messenger: Intermediary Liability and Protecting Internet Platforms

Cynthia Wong

© AP Images/Richard Vogel

YouTube is an "intermediary provider." Protecting it from liability for content posted by users allows greater freedom and creativity on the Internet, the author says.

Holding Internet service providers responsible for offensive materials posted by their customers can slow innovation and expansion of communications technologies.

Cynthia Wong is the Ron Plesser Fellow and an attorney with the Center for Democracy & Technology. CDT is a public interest advocacy organization dedicated to keeping the Internet open, innovative, and free. Ms. Wong helps lead CDT's work on global Internet freedom.

When an Italian court held Google liable for a video uploaded by a third party to one of the Internet giant's Web sites, [see sidebar] it offered a stunning example of intermediary liability. Google, the platform host, was the *intermediary* between the content creator who made the video clip and the content consumers who viewed it. Other intermediaries include Internet service providers (ISPs), e-commerce platforms, and social media platforms like Orkut, Facebook, and YouTube. These services provide valuable open forums for user-generated content that are often free of charge and require minimal technical knowledge to use.

The open nature of these services also means that they can be used for ill as well as good. Governments wishing to censor free expression or address harmful behavior on the World Wide Web often seek to pressure, intimidate, or, more subtly, expose Internet intermediaries to legal liability for third party content. One way to prevent a citizen from posting videos of political dissent is to hold YouTube liable for material that users post.

The equities of intermediary liability often are not this simple. Sometimes even well-meaning governments are trying to circumscribe behavior that a deep social consensus in a given nation believes wrong: obscenity, defamation, hate speech, privacy violations (as in the Google Italy case) or criminal activity. [See "The Enigma of Internet Freedom," this issue.] One readily sees why the technique offers an attractive alternative: the intermediary often is large and easy to identify, while individual Internet users can be hard to find and at times are outside a particular government's jurisdiction (although this was not the case in Italy).

Whatever the reason a government allows intermediary liability, the substantial harm to information flows and Internet growth that follows outweighs the perceived benefits. First, freedom of expression inevitably is limited. A social networking platform, for instance, that can be held liable for money damages when a third party posts objectionable content, will wish to screen content before posting. Intermediaries will err on the side of caution in deciding what users may post, especially when the laws defining "illegal content" are vague and overbroad or where the speech is unpopular. Far safer simply to remove disputed content than to challenge a removal demand in court. In many cases, the sheer volume and associated cost of this task will be too much for many platforms to bear and they could not offer their services at all.

Second, intermediary liability disrupts the free flow of information and services on the Internet and thus stifles creative innovation and economic development. Companies are less likely to invest in technologies that may expose them to liability. The world may never see tomorrow's Twitters, eBays, or other startups holding the promise of lowering prices and better connecting global markets; or of new initiatives that might increase access to educational resources or in other ways spark broader, deeper, and more equitable economic development.

Approaches to Intermediary Liability

An early policy consensus emerged on the question of intermediary liability equities in the United States and the European Union. In the United States, two statutes address these concerns. Section 230 of the Communications Act generally immunizes intermediaries from a variety of claims arising from third-party content, among them negligence, defamation, and violations of civil rights laws and state criminal laws. Section 512 of the Digital Millennium Copyright Act affords online service providers a "safe harbor" from liability if they meet certain criteria, including removal of infringing material when notified by the copyright owner of its presence, known as a "notice-and-takedown" system.

The European Union similarly shields several kinds of intermediaries from a range of claims: "mere conduits" of information, "caching" services offering temporary data storage to facilitate onward transmission, and "hosting" services that quickly remove unlawful content upon becoming aware of it. Because the U.S. and E.U. policies do not generally oblige intermediaries either to monitor content on their services nor to investigate possible unlawful user activity, the policies help safeguard user privacy. If service providers faced liability, they might feel compelled to collect more information about users and keep that information longer.

The Chinese government is among those taking a very different approach. Beijing imposes responsibility for unlawful content on entities at every access point — from user to ISP, to social networking platform and Internet hosting company. If any intermediary allows users to distribute "harmful" content, or fails sufficiently to monitor or police the use of its services, it could face criminal liability, or revocation of its operating license. Further the government defines unlawful content in overbroad and vague terms. A blogging platform service like Blogger.com, for instance, may find it difficult to decide which postings are "harmful" or damaging to "the interests of the nation." China's approach to intermediary liability is a key component of its larger system of online information control.

Addressing Potential Concerns

One objection to protecting intermediaries is the fear that genuinely harmful and offensive expression will grow online. But governments already possess many tools to address this concern while minimizing the impact on lawful expression and innovation. They might, for instance, promote and subsidize voluntary consumer use of filtering software that blocks pornography and other objectionable material. Some countries also require notice-and-takedown systems like the approach in U.S. copyright law and E.U. law to address this concern. However, notice-and-takedown systems are often easily misused to silence critics, especially where it is difficult to assess whether the challenged content is actually unlawful (as in the case of defamation). Finally, intermediaries can and do take voluntary steps to define and remove harmful material from their services (like spam or sexually explicit

material) without government mandate, demonstrating that intermediary protections are compatible with advancing other important social goals.

Another key concern is that law enforcement officials must be able to legitimately pursue criminal wrongdoers, and victims must be able to pursue legitimate claims against those who have done them harm. An important aspect to the U.S. and E.U. approaches is that protection is afforded *only* to the intermediary, not to the parties that originally created or disseminated content deemed objectionable. Nothing under the U.S. or E.U. law prevents prosecution or claims against the original wrongdoer. One proper role for intermediaries might be to facilitate action against users (even anonymous users) in response to legitimate court orders, with procedures in place to safeguard privacy and some degree of anonymity.

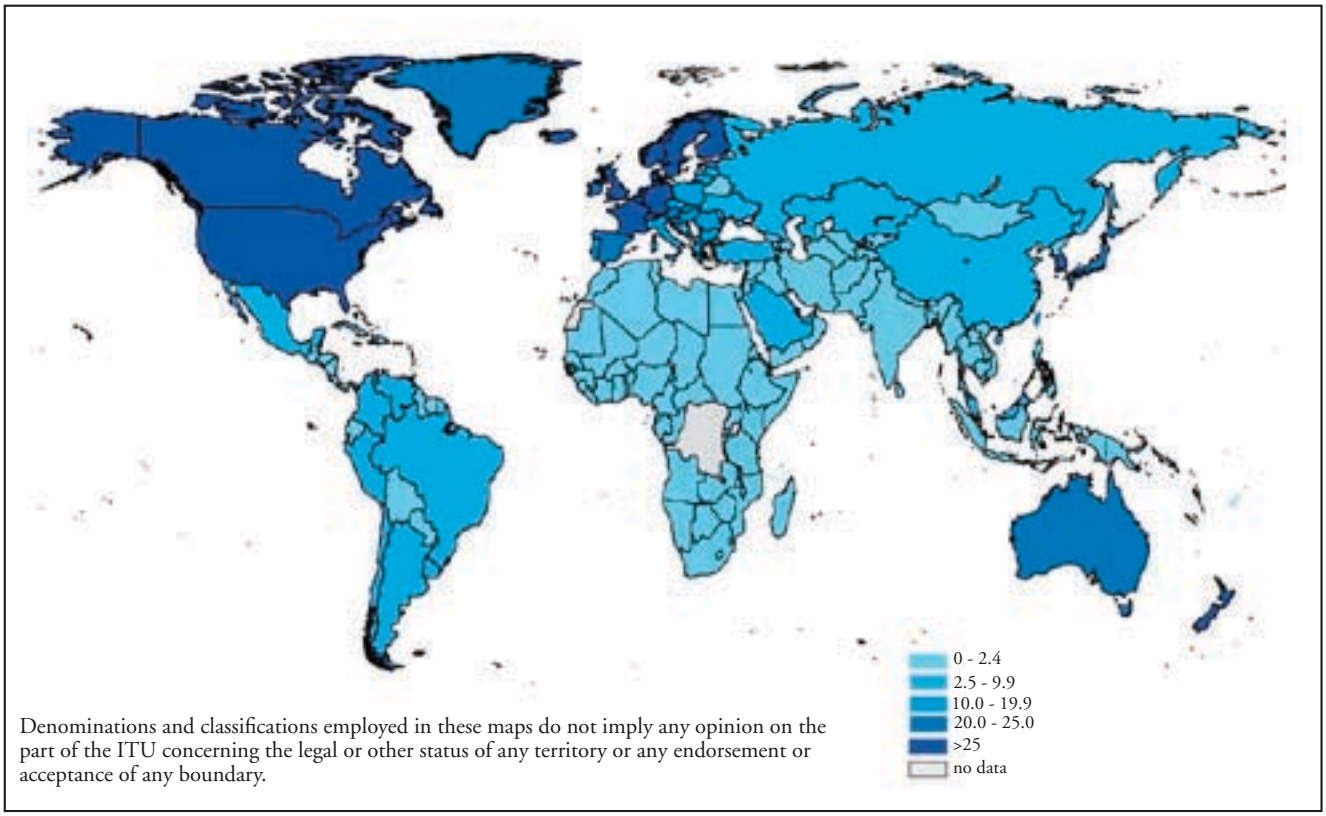
Conclusion

Protecting intermediaries from liability is critical to preserving the Internet as an instrument for free expression and access to information, and thus as an engine of innovation and economic development. If liability concerns force the closure of user-generated content sites and other vital forums for social, economic, and political expression, we all will be the poorer. Governments should instead strengthen and adopt policies that protect intermediaries as key enablers of innovation, human rights, and economic development. ■

The opinions expressed in this article do not necessarily reflect the views or policies of the U.S. government.

The Global Broadband Divide

Fixed Broadand Subscribers Per 100 Inhabitants, 2008



From "The World in 2009: ICT Facts & Figures," International Telecommunications Union

Dancing Baby Tests Internet Law

Karen A. Frenkel

A mother's act of whimsy leads to a legal showdown.

Karen A. Frenkel is a New York-based technology and science writer. Her articles appear on ScientificAmerican.com *and in* Communications of the ACM *(Association for Computing Machinery).*

When Pennsylvania mom Stephanie Lenz posted a video of her children dancing to Prince's song, "Let's Go Crazy." on YouTube in February 2007, she did not expect to tangle with a pop music superstar and a corporate giant. Universal Music Corporation, which owns the rights to Prince's song, halted her attempt to share her children's antics. The world's biggest record company requested that YouTube remove the video, which it did. The record label claimed Lenz had violated its copyright as protected by the Digital Millennium Copyright Act (DMCA), and asked YouTube to remove the video. Mrs. Lenz's dancing children lost their place on the Internet.

Courtesy of YouTube

Stephanie Lentz's video shows her laughing baby racing around the kitchen. The Prince song "Let's Go Crazy" is barely audible in the background.

"I was really surprised and angry when I learned my video was removed," Lenz told online free-speech advocates at the Electronic Frontier Foundation (EFF). "Universal should not be using legal threats to try to prevent people from sharing home videos."

The DMCA was enacted in 1998 as the United States' implementation of an international copyright treaty. It gives Internet hosting companies and interactive services like social networking sites near immunity from their users who violate intellectual property. These companies must remove material if a copyright holder sends a takedown notice, but they can restore that content if the copyright claimant does not sue and if the user who posted the material certifies that it is non-infringing.

As a result of DMCA, today's Internet breaks the barriers between content providers and content consumers, allowing a vast audience to create and distribute content without fear that hosts could be sued out of business. But there's ample evidence that amateur producers don't understand fully the intellectual property laws or their legal responsibilities.

The EFF sued Universal on Lenz's behalf. EFF argued that her 29-second video, featuring the barely audible song, did not infringe the label's copyright, that the record giant had failed to consider Lenz's "fair-use" right to post the clip, and had chilled her free speech.

Fair use is a grey area in U.S. copyright law because it allows limited quotations from an author's work without permission. But the law lacks specifics about the length and nature of allowable quotes, and how they might be used.

Meanwhile, Prince told Reuters he intended to "reclaim his art on the Internet," and Universal announced plans to remove all user-generated content involving the artist from the Internet as a matter of principle.

The court sided with EFF and Lenz, ruling in August 2008 that Universal had not considered fair use for each work before issuing indiscriminate takedown notices. It had therefore abused the DMCA, the court concluded. YouTube reinstated Lenz's dancing babies, and the parties are struggling over who should pay legal fees and damages. ■

The opinions expressed in this article do not necessarily reflect the views or policies of the U.S. government.

Google Video Slapped with Privacy Violation in Italy

Search engine company fights legal battle in the name of Internet freedom.

© AP Images/APTN

Italian Judge Oscar Magi (left) reads his verdict against Google executives in February 2010.

In late 2006, students at a school in Turin, Italy, recorded a video showing them illegally bullying an autistic schoolmate. They uploaded it to Google's video-sharing site, and Google took it down within hours of being notified by the Italian local police. But the video had been online for nearly two months by that time, and it caused national outrage, according to TheNextWeb.com. The video received 5,500 views, 80 comments, and made Google Italy's "most entertaining" list, according to an Associated Press report.

Google helped the police identify the individual responsible for uploading the offending video. A court sentenced her and her accomplices to 10 months of community service. That's where Google expected its involvement to end, according to a corporate blog posting on the case. However, a public prosecutor in Turin indicted four Google executives — chief legal officer David Drummond, global privacy counsel Peter Fleischer, former Google Video European Director Arvind Desikan, and former Chief Financial Officer George Reyes (who left the company in 2008) — charging them with criminal defamation and failure to comply with Italian privacy law. In February 2010, a judge convicted the first three defendants on the privacy charge. All four were found not guilty of criminal defamation.

Matt Sucherman, a Google vice president and attorney, called the ruling "astonishing," and the prosecutor's action to try the executives "outrageous." The company plans to appeal the conviction.

European Union law affords Internet hosting providers safe harbor from liability, wrote Sucherman in an official Google blog, "so long as they remove illegal content once they are notified of its existence." But the Italian decision means employees of hosting platforms like Google are criminally responsible for content that users upload, according to Sucherman. If sites such as YouTube, social networks, and community bulletin boards are held responsible for vetting every single piece of uploaded content, the Web as we know it will cease to exist, Sucherman wrote.

In April 2010, the judge explained the reasoning underlying his verdict. In an 111-page opinion, Judge Oscar Magi said the executives were guilty of violating the privacy of the victimized youth and acted with malice because they had sought to make a profit with advertising income while hosting the video. Judge Magi said his decision should be interpreted as a requirement that Internet service providers screen video posted on their sites. Press accounts further quoted the opinion: "There is no such thing as the endless prairie of the Internet where everything is allowed and nothing can be prohibited."

Google reiterated its initial reaction — that the verdict attacks the very principles of freedom on which the Internet is built.

Free expression and privacy advocates are still evaluating the potential impact of the opinion, including questions it raises for participatory media and user-generated content platforms. ■

— Karen A. Frenkel

The opinions expressed in this article do not necessarily reflect the views or policies of the U.S. government.

Public Librarians Help Define Internet Freedom

Barbara M. Jones

© AP Images/Dan Loh

Patrons access the Internet at a public library in Philadelphia. Books, traditional reference materials, and online resources all are provided there.

In the United States, public libraries are an important source of Internet access. Librarians help defend intellectual freedom and work to balance intellectual property rights with public access to Internet content.Barbara M. Jones is the director of the Office for Intellectual Freedom for the American Library Association based in Chicago, Illinois.

"The best reading, for the largest number, at the least cost."

The American Library Association (ALA) adopted that motto when it was founded more than 100 years ago, and those words still ring true for us today. Sometimes we wonder whether our colleagues of an earlier age even dreamt of the tools and resources used in our profession now — the invention of digitized information, potentially limitless reproduction of information, and dissemination of this material on a global basis.

Public Internet access is among the most popular and frequently used services in U.S. libraries today. Readily available printers and photocopy machines make it easy for our users to duplicate content to carry home or share.

Librarians want patrons to have access to content, but also assume responsibility for preventing dissemination in ways that violate the author's copyright. Thus we arrive at our current dilemma, pitting intellectual freedom against intellectual property. Web content can be disseminated to many people very quickly. Some content is created by the general public and available at no cost — witness the growth of "born digital" content such as blogs and Wikipedia. Music, videos, and other media can be shared easily via digital reproduction technologies, in ways unheard of when music was distributed on vinyl records or cassette tapes.

This ease of access to content is a real boon to libraries and their users. But it is a nightmare for publishers who are trying to stay in business under a traditional economic model. Ease of copying and the

speed of dissemination threaten to put them out of business. Publishers have responded with measures to protect their interests: dramatic increases in the prices of academic journals, for instance, and restricting online content through licenses. The recording industry has sued a number of individuals for downloading music illegally.

We in the library community are torn between the desire to support industries that provide rich, uncensored content and the library users who face frequently blocked access and rising content costs.

Librarians' Principles

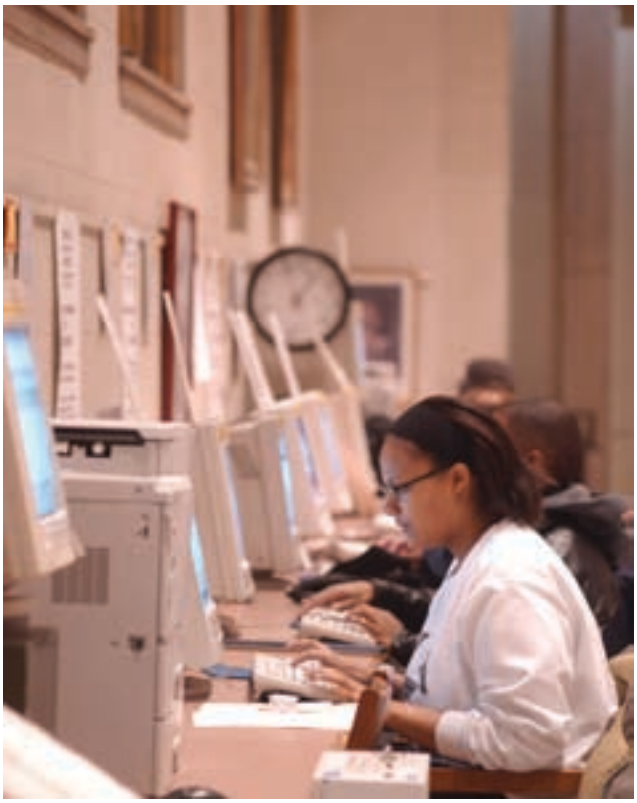
American public librarians are legally and ethically bound by the First Amendment to the U.S. Constitution: "Congress shall make no law… abridging the freedom of speech, or of the press… ." This principle is also enshrined in our professional codes: the *Library Bill of Rights and Its Interpretations*, and the *Code of Ethics of the American Library Association*. The Internet community slogan, "Information wants to be free" also captures this principle.

At the same time, librarians are bound by another section of the U.S. Constitution, which gives "authors and inventors the exclusive Right to their respective Writings and Discoveries." Copyrights and other intellectual property law is grounded in this principle. Librarians struggle to balance "freedom to read" values with the competing requirements of copyright laws and regulations. Meanwhile, some disciples of the information revolution argue that information published on the Internet belongs to everyone, ignoring the rights of the originator to be compensated. Library users demand more and more content, as publishers push back by licensing content and by other means to maintain their economic stability.

How can librarians collaborate with publishers to create an economic model that allows access to information for readers, while affording a livelihood for authors and publishers?

Protecting Intellectual Property

Fair Use: The Fair Use Doctrine of U.S. Copyright law permits limited use of a copyrighted work for criticism, teaching, or news reporting. A book reviewer may, for instance, quote passages from a new book, or news media may report a song lyric that sparks a controversy. Developed in a number of judicial decisions, the fair use exception remains ambiguous, and often relies



© AP Images/Sabina Louise Pierce

Internet access is the service in highest demand at many U.S. public libraries.

on the professional judgment of the librarian or user. The reviewer may not, however, reproduce entire chapters of a novel, nor may the news reporter play an entire album track. If an academic library wants to make 10 copies of a journal article for use of the students in a particular course, the librarian may well decide that two copies is a more "reasonable" limit, given the class demand and size. Fair use gets considerably more complicated with electronic reserves and the classroom use of films, recordings, and other digital media.

What if someone makes 100 copies of an article for a course, or places an article on a Web site without first getting the publisher's permission for that use? Library "best practices" mandate that public photocopiers prominently display a warning, citing U.S. copyright law and that libraries educate their users about the law with notices, brochures, or public information sessions. But library patrons are legally responsible for their own actions, and in recent years library users have, indeed, been sued for illegal downloading of music and other content.

Creative Commons Licenses: Librarians who are helping patrons find information can direct their search to materials licensed under one of the simple

licensing agreements drafted by the Creative Commons organization. These allow authors, artists, and other creators to make their work available to others while reserving certain rights, all in an easily understandable document. The Wikipedia online encyclopedia is one publication covered by a Creative Commons license. The Creative Commons license is an especially important option for researchers and academics who wish to see their work incorporated into the larger body of professional knowledge without relinquishing all their rights..

Protecting Intellectual Freedom

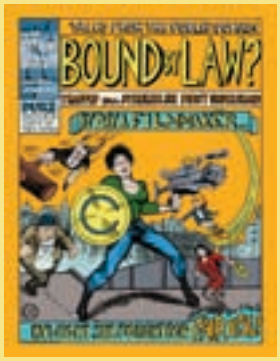
The ALA provides guidelines and ethical principles for librarians to protect intellectual property (IP), but also considers protection of intellectual freedom (IF) a core value. ALA's Office for Intellectual Freedom (OIF) plays a key role in education, advocacy, and policy creation in the freedom of expression arena. *The Intellectual Freedom Manual, Eighth Edition* (ALA Editions, 2010) contains current and historical documents tracing the evolution of the ALA Library Bill of Rights, a statement expressing library users' right to intellectual freedom and the steps libraries should take to support those rights. For example, when the original Library Bill of Rights was adopted in 1948, issues about library user privacy were not a prominent concern. Responding to today's worries about data privacy on library online catalogs and social networks, ALA adopted "Privacy: An Interpretation of the Library Bill of Rights" in 2002.

The September 11, 2001 terrorist attacks and the USA Patriot Act that followed sharpened the tension between national security and user privacy. Occasionally investigators track their suspects to libraries and seek records of materials patrons have used. The practice has caused an enormous controversy in our profession because it conflicts with existing library confidentiality statutes protecting library user privacy.

And so 21st-century librarians continue to supply the public access to ever-greater amounts of content, while simultaneously honoring an equally important legal and ethical mandate — observing the copyright law that protects the creators of that content. Librarians work actively with legal, publishing, and user communities to find solutions. ■

The opinions expressed in this article do not necessarily reflect the views or policies of the U.S. government.

Intellectual Property Guidelines



© 2006 Keith Aoki, James Boyle, Jennifer Jenkins; available under a Creative Commons license.

Duke University makes copyright cool, explaining intellectual property law in a comic book format. The book is freely available at *http://www.law.duke.edu/cspd/comics/*

The ALA provides guidance for professionals struggling with the issues of this new age in the document "Guidelines and Considerations for Adopting a Public Library Internet Use Policy."

Educating library users is a critical piece of copyright enforcement. One of the best practical sources for librarians is *Complete Copyright: An Everyday Guide for Librarians* by Carrie Russell (American Library Association: Office for Information Technology Policy, 2004). Updated information is provided by the University of Maryland Center for Intellectual Property*: [http://www.umuc.edu/distance/odell/cip/cip.shtml]*. They provide distance learning certificate programs for librarians to learn the very latest intellectual property issues from visiting scholars and attorneys in the field. Most universities have developed comprehensive intellectual property policies such as the one at Indiana University: [*http://www.iub.edu/~vpfaa/download/IPPolicy_Adopted_050208.pdf]*.

Duke University Law School's Center for the Study of the Public Domain has produced a comic book, "Bound by Law," that can be downloaded free and is a good way to engage young adults in the issues: [*www.law.duke.edu/cspd/artsproject/index]*.

Industry Players Take a Stand for Online Freedom

In response to government crackdowns on citizens' Internet freedom, a diverse group of institutions including human rights NGOs, investors, journalism schools, and a handful of major technology corporations in 2008 founded the Global Network Initiative (GNI).Drawing upon internationally recognized human rights laws and standards, GNI provides guidance on how companies can respond when faced with government pressure to infringe upon Internet freedom. The Electronic Frontier Foundation, Human Rights Watch, Google, Microsoft, and Yahoo, are among the participants.

© AP Images/Susan Walsh

Representatives from (left to right) Google, Inc.; Yahoo! Inc.; Human Rights Watch; Cisco Systems, Inc.; and the Global Internet Freedom Consortium are sworn in before a Senate Judiciary Committee hearing on global Internet freedom in Washington, May 2008.

While many industry leaders have not joined GNI, the group's influence continues to grow, according to some observers. "While only three companies have joined, GNI has laid out set of standards for privacy in industry that lots of companies are referring to so they're becoming the *de facto* standard," says Rebecca MacKinnon, GNI Board Member and Visiting Fellow at Princeton's Center for Information Technology Policy. Those companies do human rights assessments before entering markets and establish procedures to assure their practices adhere to the GNI principles. Yahoo, for example, elected to operate its Vietnamese service out of Singapore, to prevent Vietnamese police access to account holder information, MacKinnon said.

A test case for the GNI principles came with Google's 2010 decision to cease complying with Chinese censorship standards, and its threat to withdraw from the Chinese market after "a highly sophisticated and targeted attack" from within China. The company's investigation of the attacks found that they targeted accounts held by human rights activists. Human Rights Watch (HRW), another GNI partner, saluted Google's response, and urged others to follow. "We are pressing more companies to adopt GNI standards, while also calling for federal laws to make it illegal for [U.S.-based] Internet companies to take part in censorship or to share private user information," HRW said in an online article.

© AP Images/Kin Cheung

Supporters of Google's decision to cease cooperating with Chinese censorship policies leave flowers at the company's Hong Kong office. The move came after the company detected attacks on Google accounts held by human rights activists.

"With these steps, we will create a stronger foundation for Internet freedom around the world." ■

Karen A. Frenkel

The opinions expressed in this article do not necessarily reflect the views or policies of the U.S. government.

Breaking Online Barriers

Technology may provide the tools to overcome Internet censorship.

Millions of Internet surfers living in closed societies use free anti-censorship technology to break through online barriers imposed by their authoritarian governments. Several organizations produce that software, including the Censorship Research Center (CRC), the Global Internet Freedom Consortium (GIF), Torproject.org, and the University of Toronto's Citizen Labs (UTCL), which is affiliated with the OpenNet Initiative.

Governments that censor the Internet employ three technical methods. The first blocks visits to specified Internet Protocol addresses. The second filters content, cutting off access to any site with keywords prohibited by the censoring government. The third technique, called Domain Name Redirect, is similar to changing a person's phone number. It makes sites impossible to find.

Software designed to dodge the censor can also work in several different ways. GIF's software tools defeat the blocks, monitors, and traces authorities use to surveil individually owned computers. For example, censor-busting software might scramble the bits and bytes flowing in and out of a Chinese user's computer, so the "Great Firewall of China," as it's known, cannot see patterns in the traffic.

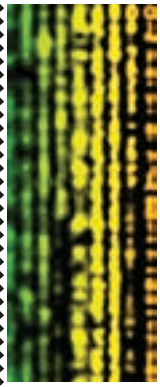
UTCL's software, called Psiphon, is a browser proxy. It enables users behind firewalls to see otherwise-blocked content by delivering Web pages through an intermediate server in an uncensored country. The system works based on trust; someone already with a Psiphon account must invite first-time users. The invitation is an Internet address combined with a code. These enable the newcomer to log in to get credentials and visit an address without anyone knowing they're using Psiphon to get there. The user enters that address into an address bar on any browser and can surf freely from then on.

Torproject.org's Tor software protects users' anonymity by preventing those watching from conducting traffic analysis. It distributes transactions along a random Internet pathway so no single point links a user to his or her destination.

The Censorship Research Center offers the newest addition to the anti-censorship toolkit. It developed "Haystack" software after an Iranian government crackdown on Internet use after 2009's disputed presidential election. Haystack uses a mathematical formula to hide users' real Internet identity when they visit Web sites. The program lets people in Iran use the Internet "as if there were no Iranian government filters," CRC Executive Director Austin Heap told *Business Week.* ■

Karen A. Frenkel

The opinions expressed in this article do not necessarily reflect the views or policies of the U.S. government.



INFO BYTES

The cost of information and communications technologies services dropped an average of **15** percent between 2008 and 2009 in **161** nations surveyed by the International Telecommunications Union.

Additional Resources

A selection of books, articles, and Web sites

GENERAL

Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace; edited by Ronald Deibert ... [et al.]. Cambridge, Mass. MIT Press, 2010.

Access Denied: The Practice and Policy of Global Internet Filtering; edited by Ronald Deibert ... [et al.]. Cambridge, MA: MIT Press, 2008.

Congressional-Executive Commission on China. "Google and Internet Control in China: A Nexus Between Human Rights and Trade?" March 2010 *http://www.cecc.gov/pages/hearings/2010/20100324/index.php*

Finkelstein, David M., Maryanne Kivlehan-Wise, and Kristen Gunness, eds. *The Chinese Media System: Continuity, Chaos, and Change*. Armonk, NY: M.E. Sharpe Publishers, 2007.

Freedom House. *Freedom on the Net: A Global Assessment of Internet and Digital Media*. Washington, DC: Freedom House 2009.

Jacobson, George V. [and Patricia M. Figliola]. *Cybersecurity, Botnets, and Cyberterrorism*. New York: Nova Science Publishers, 2009.

Lessig, Lawrence. *Code 2.0.* 2d ed. [New York]: SoHo Books; distributed under the terms of the Creative Commons Attribution ShareAlike 2.5 License, 2006.

Lessig, Lawrence. *Free Culture: How Big Media Uses Technology and the Law to Lock Down Culture and Control Creativity*. New York: Penguin, 2004.

McCaffrey, Paul, ed. *The News and Its Future*. New York: The H.W. Wilson Company, 2010.

Perelman, Michael. *Steal This Idea: Intellectual Property Rights and the Corporate Confiscation of Creativity*. New York: Palgrave, 2002.

Portela, Irene Maria and Maria Manuela Cruz-Cunha, eds. *Information Communication Technology Law, Protection, and Access Rights: Global Approaches and Issues*. Hershey PA: Information Science Reference, 2010.

Reporters Without Borders, *Handbook for Bloggers and Cyber-Dissidents*. Reporters without Borders: Paris, 2008. *http://www.rsf.org/IMG/pdf/guide_gb_md-2.pdf*

Sell, Susan K. *Private Power, Public Law: The Globalization of Intellectual Property Rights*. Cambridge, UK; New York: Cambridge University, 2003.

Stein, Richard J., ed. *Internet Safety, Vol. 81*. New York: H.W. Wilson, 2009.

United States. Congress. House. Committee on International Relations. Subcommittee on Africa, Global Human Rights, and International Operations. *The Internet in China: A Tool for Freedom or Suppression?*; (Joint Hearing, 109th Congress, 2nd session, February 15, 2006.) *http://www.internationalrelations.house.gov/archives/109/26075.pdf*

United States. Congress. Senate. Committee on the Judiciary. Subcommittee on Human Rights and the Law. *Global Internet Freedom: Corporate Responsibility and the Rule of Law*; 110th Congress, 2d session, May 20, 2008. Washington.

Vaidhyanathan, Siva. *Copyrights and Copywrongs*: *The Rise of Intellectual Property and How It Threatens Creativity*. New York: New York University, 2003.

Zittrain, Jonathan L. *The Future of the Internet and How to Stop It*. New Haven, CT: Yale University Press, 2008.

REPORTS AND ARTICLES

Anderson, Janna and Lee Rainie. *Future of the Internet IV*, Pew Center for Internet and American Life, February 19, 2010.
http://pewinternet.org/Reports/2010/Future-of-the-Internet-IV.aspx

Bandurski, David. "China's Guerrilla War for the Web," *Far Eastern Economic Review*, vol. 171, no. 6 (July/August 2008): pp. 41-44.

Calingaert, Daniel. "Authoritarianism vs. the Internet," *Policy Review*, (no. 160 April and May 2010)
http://www.hoover.org/publications/policyreview/89175117.html

Carlson, Matt. "Order Versus Access: News Search Engines and the Challenge to Traditional Journalistic Roles," *Media, Culture and Society,* (v. 29, November 2007): pp. 1014-1030.

Clinton, Hillary Rodham, Secretary of State, Remarks on Internet Freedom, Washington, DC,
January 21, 2010.
http://www.state.gov/secretary/rm/2010/01/135519.htm

Frenkel, Karen A. "The Wisdom of the Hive: Is the Web a Threat to Creativity and Cultural Values? One Cyber Pioneer Thinks So," *Scientific American*, (February 16, 2010).
http://www.scientificamerican.com/article.cfm?id=jaron-lanier-gadget

International Telecommunications Union."The World in 2009: ICT Facts and Figures,"
http://www.itu.int/ITU-D/ict/material/Telecom09_flyer.pdf
"Measuring the Information Society 2010"
http://www.itu.int/ITU-D/ict/publications/idi/2010/index.html

Karlekar, Karin Deutsch and Sarah G. Cook. "Access and Control: A Growing Diversity of Threats to Internet Freedom," Special Reports Section, Freedom House.
http://freedomhouse.org/template.cfm?page=384&key=194&parent=19&report=79

Posner, Michael H., Assistant Secretary of State for Democracy, Human Rights, and Labor,
"Briefing on Internet Freedom and 21st Century Statecraft," Washington, D.C., January 22, 2010.
http://www.state.gov/g/drl/rls/rm/2010/134306.htm

Reporters Without Borders
"Predators of the Press", March 5, 2010.
http://en.rsf.org/www-rsf-org-predators2010-03-05-2010,37235.html

U.S. Department of State. "2009 Country Reports on Human Rights Practices," Washington, D.C. March 11, 2010.
http://www.state.gov/g/drl/rls/hrrpt/2009/index.htm

Figliola Patricia M., Kennon H. Nakamura, Casey L. Addis [and] Thomas Lum. *U.S. Initiatives to Promote Global Internet Freedom: Issues, Policy, and Technology*, Washington, DC: Congressional Research Service, 2010.
http://www.fas.org/sgp/crs/misc/R41120.pdf

World Summit on the Information Society, "Tunis Commitment," Tunis, Tunisia, November 18, 2005.
http://www.itu.int/wsis/docs2/tunis/off/7.html

Wu, Tim. "The World Trade Law of Censorship and Internet Filtering," *Chicago Journal of International Law*, (vol. 7, no. 1, Summer 2006): pp. 263-287.

WEB SITES

U.S. Government

Internet Freedom: Free Expression in the Digital Age
http://www.america.gov/internet-freedom.html

National Telecommunications and Information Administration
Internet Policy Task Force
http://www.ntia.doc.gov/internetpolicytaskforce/

U.S. Department of Commerce
International Trade Administration
Strategy Targeting Organized Piracy (STOP)
http://www.export.gov/tradeproblems/eg_main_018580.asp

U.S. Department of Justice
Computer Crime and Intellectual Property Section (CCIPS)
http://www.cybercrime.gov/ip.html

U.S. Office of the United States Trade Representative
Office of Intellectual Property and Innovation (IPN)
http://www.ustr.gov/trade-topics/intellectual-property

INTERNATIONAL ORGANIZATIONS

Global Network Initiative (GNI)
http://www.globalnetworkinitiative.org

Internet World Stats
http://www.internetworldstats.com/stats.htm

World Intellectual Property Organization
http://www.wipo.int

World Trade Organization
Trade-Related Aspects of Intellectual Property Rights (TRIPS)
http://www.wto.org/english/tratop_e/trips_e/trips_e.htm

ASSOCIATIONS AND TRADE ORGANIZATIONS

American Intellectual Property Law Association
http://www.aipla.org

American Library Association (ALA)
Office of Intellectual Freedom
http://www.ala.org/ala/mgrps/committees/ala/ala-if.cfm

Business Software Alliance
http://www.bsa.org

International Intellectual Property Alliance
http://www.iipa.com

EDUCATIONAL INSTITUTIONS

Duke University Law School
Center for the Study of the Public Domain
comic book "Bound by Law"
http://www.law.duke.edu/cspd/artsproject/index

Electronic Frontier Foundation (EFF)
http://www.eff.org

Harvard University Law School
Berkman Center for Internet and Society
http://cyber.law.harvard.edu

Stanford University
Copyright and Fair Use
http://fairuse.stanford.edu

University of Maryland
Center for Intellectual Property
http://www.umuc.edu/distance/odell/cip/cip.shtml

University of Washington School of Law
Center for Advanced Study and Research on Intellectual Property (CASRIP)
http://www.law.washington.edu/Casrip

FILMOGRAPHY

Freedom of Expression: Resistance and Repression in the Age of Intellectual Property (2007)
Running time: 60 minutes
Director: Jeremy Smith
Summary: Documentary explores the battles being waged in courts, classrooms, museums, film studios, and the Internet over control of cultural commons.

I Am the Media (2010)
Running time: 56 minutes
Director: Benjamin Rassat
Summary: French film about bloggers and avid Internet users.

Unconstitutional: The War on Our Civil Liberties (2004)
Running time: 68 minutes
Director: Nonny de la Pena
Summary: This documentary investigates the encroachment on civil liberties enacted in the United States since the 2001 terrorist attacks and the passage of subsequent anti-terrorism laws.

now on facebook

ENGAGING THE WORLD

A MONTHLY JOURNAL
IN MULTIPLE LANGUAGES

http://america.gov/publications/ejournalusa.html

U.S. Department of State, Bureau of International Information Programs