GeoJournal
DOI 10.1007/s10708-010-9393-3

Geographies of global Internet censorship

Barney Warf

Abstract More than one-quarter of the planet's population uses the Internet today, although access to it is highly uneven throughout the world. While it is widely celebrated for its emancipatory potential, many governments view the Internet with alarm and have attempted to limit access or to control its contents. This project seeks to provide a comprehensive, theoretically informed analysis of the geographies of Internet censorship. It begins by clarifying the reasons, types, extent of, and opposition to, government limitations of Internet access and contents. Invoking an index of censorship by Reporters Without Borders, it maps the severity of censorship worldwide and assesses the numbers of people affected, and using the Freedom House index, it correlates political liberty with penetration rates. Second, it explores Internet censorship at several levels of severity to explicate the multiple means through which censorship is implemented and resisted. The third part offers a moral critique of Internet censorship via a Habermasian interpretation of cyberspace as the closest real-world approximation of an ideal speech situation. The summary notes the paradox of growing e-government and continued fears of an expanded domain of public discourse.

B. Warf (✉)
Department of Geography, University of Kansas,
219C Lindley Hall, Lawrence, KS 66045-7613, USA
e-mail: bwarf@ku.edu

Published online: 23 November 2010

Keywords Internet · Cyberspace · Censorship · Habermas

> The Internet interprets censorship as damage, and routes around it
> (John Gilmore, in Elmer-Dewitt et al. 1993, p. 62).

In mid-2010, more than 1.9 billion people used the Internet, making it a tool of communications, entertainment, and other applications accessed by roughly 28% of the world's population (www.Internetworldstats.com/stats.htm). The distribution of these netizens was highly uneven (Fig. 1). For many users these uses extend well beyond email to include bill payments, stock trading, "e-tail" shopping, digital gambling, videogames, telephony (e.g., Voice Over Internet Protocol), hotel and airlines reservations, chat rooms, downloading television programs, digital music, and pornography, as well as popular sites and services such as YouTube, Facebook, and Google. In all these ways, and more, cyberspace offers profound real and potential effects on social relations, everyday life, culture, politics, and other social activities. Indeed, for rapidly rising numbers of people around the world, the "real" and the virtual have become thoroughly interpenetrated. In this light, access to cyberspace is no longer a luxury, but a necessity. As its applications have multiplied, the Internet is having enormous impacts across the globe, including interpersonal interactions and everyday life,

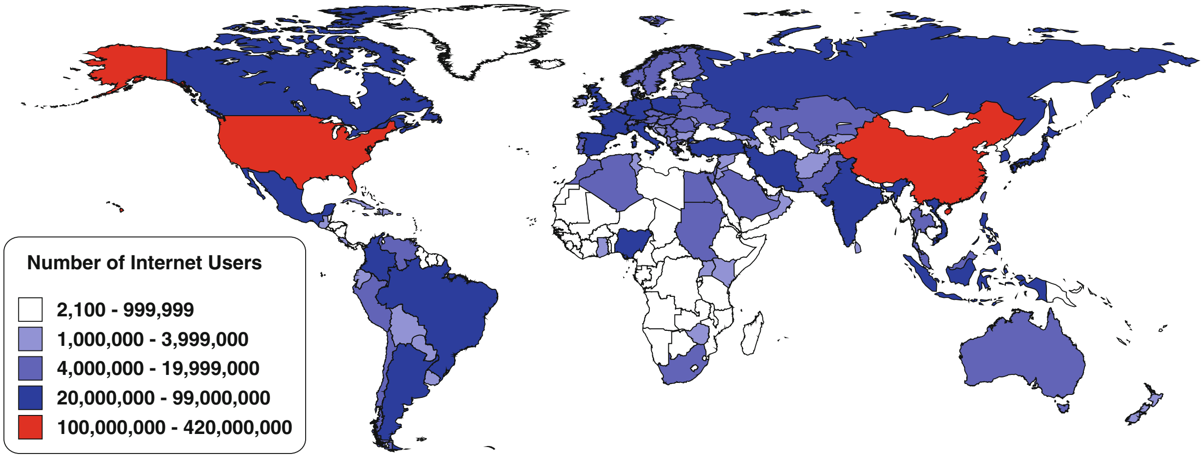

Fig. 1 Distribution of world's Internet users, June, 2010. *Source*: author, using data from www.internetworldstats.com

identity formation, retail trade and commerce, governance, and is affecting the structure and form of cities, in the process generating round upon round of non-Euclidean geometries in the context of a massive global wave of time–space compression.

A cottage industry of geographers has artfully charted the origins and growth of cyberspace, its uneven social and spatial diffusion, and its multiple impacts, ranging from cybercommunities to digital divides to electronic commerce (Dodge and Kitchin 2000; Castells 2001; Kellerman 2002; Crampton 2003; Zook 2005a, b; Malecki and Moriset 2008). Such authors typically embed the Internet within post-Fordist capitalism, and, drawing on the literature in critical cartography, view it as a power/knowledge constellation with decisive social roots and consequences. Zook and Graham (2007) note the Internet's "core and periphery" structure, as exemplified by the dominant role played by search engines such as Google, and voice concerns over the privatization of the digital commons. Similarly, Zook (2003) called attention to the Internet's role in the "online adult industry." This literature offers a valuable means for spatializing the Internet, demonstrating its rootedness in social relations and changing geographic relations of proximity, and serves as a necessary antidote to many prevailing utopian and technocratic interpretations such as those that proclaim the ostensible "death of distance" (Cairncross 1997) or the "end of geography" (O'Brien 1992).

One dimension, however, has received woefully little attention from geographers, concerns the strategies and tactics deployed by states the world over to limit access and shape the contents of what their denizens may view on-line. Brunn (2000), for example, explicates how cyberspace is closely intertwined with various geographies of regionalism, networks, non-state actors, and various transnational processes. Steinberg and McDowell (2003) delved into the mechanics of domain name policing, but not censorship per se. While the geographic literature has delved into issues of geosurveillance and governmentality, virtually nothing has been said about how governments erect obstacles to Internet access or massage its contents to their liking. Warf (2009a, b) touched upon Internet censorship in Latin America and the states that comprised the former Soviet Union, and Warf and Vincent (2007) addressed the marked government restrictions found in the Arab world. Nonetheless, no comparative geographic analysis of Internet censorship worldwide yet exists, and regional approaches are limited in scope and ability to detect differences in Internet censorship practices and outcomes among the world's states. Confronting this issue directly is essential if we are to achieve a robust understanding of the nuanced political implications of the digital domain.

Of all of the innumerable myths that swarm around cyberspace, one of the most insidious is that the Internet is an inherently emancipatory tool, a device that necessarily and inevitably promotes democracy by giving voice to those who lack political power, and in so doing undermines authoritarian and repressive governments. President Ronald Reagan, for example, asserted that “The Goliath of totalitarianism will be brought down by the David of the microchip” (quoted in Kalathil and Boas 2003, p. 1), while the chair of Citicorp, Wriston (1997, p. 174) argued that “the virus of freedom … is spread by electronic networks to the four corners of the earth.” Oh that such optimistic proclamations were true. Drawing on modernizationist theories of development, in which rising education levels and information access led inexorably to a liberalization of the public sphere via a well informed, rationale public that asserts itself politically, prevailing discourses about the politics of the Internet tend to be couched in an unrealistic utopianism rooted in technological determinism and a silence regarding the perpetuation of inequality. Such visions appeal widely to Western policy makers, who may exaggerate the extent and power of ostensibly freedom-loving cyberdissidents. Closely associated with this idea is that the global community of netizens is a self-governing one in which the state has become largely irrelevant (Goldsmith and Wu 2006).

The reality, unfortunately, is more complex and depressing, and the necessary corrective calls for a state-centered approach. As Lake (2009) notes, “the Web is not nearly the implacable force for freedom that some of its champions have portrayed. The world’s authoritarians have shown just as much aptitude for technology as their discontented citizens.” Many governments across the planet aggressively limit access to the Internet, and as Kalathil and Boas (2003) demonstrate, Internet opposition to censorship and political activism is typically confined to small groups of educated individuals, often diasporas, and has relatively little impact among the masses of their respective states.

The goal of this paper is to explicate the geographical nature of Internet censorship worldwide, to demonstrate that its uneven topography reflects spatially specific constellations of state power relations that intersect in diverse ways with the geography of cyberspace. The topic has largely been overlooked by geographers; despite its numerous renditions in academic texts in terms of its origins, technology, and applications, the Internet has been largely portrayed in insufficiently political terms. A focus on censorship assists in addressing this void. “Censorship,” of course, means many things and takes many different forms: parents who restrict their children’s access to pornography or corporations that monitor their employees at work are examples. The focus here, however, is on government restrictions on Internet access. The paper begins with a discussion of the dimensions of state restrictions on cyberspace, including the variety of forms involved, a rough conceptual model of the temporal sequence of different types of intervention, and a brief statistical confirmation that political liberty is indeed correlated with Internet penetration rates. Second, it turns to the specifics of Internet censorship as it is practiced, and resisted, within a variety of levels of severity. Third, by way of moral critique, it discusses these issues in light of a Habermasian conception of the ideal speech situation and the implications of Internet censorship for the broader process of truth construction. Finally, the conclusion notes how many governments are caught between the rock of promoting information technology and a hard place of fearing a widening of the domain of public discourse, a conundrum bound to rise in intensity as many states initiate electronic government (e-government) measures.

Dimensions of Internet censorship

Internet accessibility reflects, inter alia, the willingness of governments to allow or encourage their populations to log into cyberspace. Repressive governments often fear the emancipatory potential of the Internet, which allows individuals to circumvent tightly controlled media. Theorizations of Internet censorship can draw fruitfully on contemporary geographic discussions of the state, power, and discourse. Foucauldian perspectives loom large in this regard. Critical analyses of cyberspace, for example, point to geosurveillance, invasions of privacy, and the formation of digital panopticons (Crampton 2007; Dobson and Fisher 2007). Such work has demonstrated that clearly the Internet can be made to work against people as well as for them. Far from being innately emancipatory in nature, cyberspace can be used to reinforce hegemonic powers, cultivate a climate of fear, and prevent or minimize dissent.

There are multiple motivations for Internet censorship, and thus several forms and types, including political repression of dissidents, human rights activists, or comments insulting to the state (e.g., in China, Iran, Burma/Myanmar); religious controls to inhibit the dissemination of ideas deemed heretical or sacrilegious (as found in many Arab states); protections of intellectual property, including restrictions on illegally downloaded movies and music; or cultural restrictions that exist as part of the oppression of ethnic minorities (e.g., refusal to allow government websites in certain languages) or sexual minorities (i.e., gays and lesbians). Typically, governments that seek to impose censorship do so using the excuse of protecting public morality from ostensible sins such as pornography or gambling, although more recently combating terrorism has emerged as a favorite rationale. Deliberately vague notions of national security and social stability are typically invoked as well. Other proponents hold that some degree of censorship is needed to combat "cyberanarchy" (Goldsmith 1998) or to prevent crime (Katyal 2001).

Governments face a choice in the degree of censorship, including its *scope* (or range of topics) and *depth* (or degree of intervention), which ranges from allowing completely unfettered flows of information (e.g., Denmark) to prohibiting access to the Internet altogether (e.g., North Korea); most opt for a position between these two poles. Thus, the conflict between Internet free speech and national territorial laws speaks to Taylor's (1994) well received notion that the "power container" of the nation-state has sustained mounting "leakages" to and from the world-system. Most frequently, interventions to limit access or shape the contents of cyberspace reflect highly centralized power structures, notably authoritarian one-party states concerned with an erosion of legitimacy. As Villeneuve (2006) points out, states seeking sovereignty over their cyberterritories often generate unintended consequences to censorship (e.g., diminished innovation, negative publicity that may lead to pariah status, reduced tourism, or offended corporations), results that policy makers rarely anticipate or acknowledge when putting such systems into place.

Essentially, censorship involves control over Internet access, functionality, and contents (Eriksson and Giacomello 2009). Precise filtering is almost impossible, but there is a wide variety of methods are used to control the flow of digital information, including requiring discriminatory ISP licenses, content filtering based on keywords, redirection of users to proxy servers, rerouting packets destined for a specific IP address to a blacklist, website blocking of a list of IP addresses, tapping and surveillance, chat room monitoring, discriminatory or prohibitive pricing policies, hardware and software manipulation, hacking into opposition websites and spreading viruses, denial-of-service (DOS) attacks that overload servers or network connections using "bot herders," temporary just-in-time blocking at moments when political information is critical, such as elections, and harassment of bloggers (e.g., via libel laws or invoking national security). Content filtering often relies on keyword matching algorithms that evolve as the Internet's lingo changes, and filtering may occur at the levels of the ISP, the domain name, a particular IP address, or a specific URL. Most forms of filtering are difficult to detect technically: the user may not even know that censorship is at work. Most ISPs lack the ability to block transmission to an individual IP address or URL, so governments undertaking this task in volume frequently purchase foreign (usually American) software for this purpose. Filtering mechanisms suffer the risk of overblocking, or "false positives," i.e., blocking access to sites that were not intended to be censored, and underblocking, or "false negatives," i.e., allowing access to sites that were intended to be prohibited (Murdoch and Anderson 2008). Most common and particularly important is self censorship, as the bulk of casual Internet users well understand the boundaries of politically acceptable use within their respective states. Often cultivating a persuasive, hegemonic view of dominant powers is more efficient than outright force. Typically both persuasion and coercion are combined as local contexts demand. Once formal censorship is initiated, no matter how benign or transparent, the temptation to enlarge its scope, or what Villeneuve (2006) calls "mission creep," is always there.

The institutions used to enforce such policies, which are typically outgrowths of older media regulatory regimes concerned with newspapers, radio, and television, are usually government ministries of information and communication. The degree of centrality in the management of Internet censorship varies considerably. Because the state is not a monolithic entity but composed of diverse agencies, sometimes working at cross-purposes, rather than view censorship as the simple repression of oppositional discourses it is more instructive to think of it in terms of multiple, sometimes contradictory authorities that invoke diverse strategies of suppression of various groups and individuals for a broad array of reasons and motivations. Adding to this complexity is the rapidity with which the Internet has grown and changed technologically; often government censors have difficulty keeping up-to-date with changing technologies (e.g., text messaging) or slang terms used to communicate hidden meanings.

The degree and type of Internet censorship obviously varies widely and reflects how democratic and open to criticism different political systems are. Reporters Without Borders, an NGO headquartered in Paris and one of the world's preeminent judges of censorship, ranks governments across the planet in terms of the severity of their Internet censorship (Fig. 2; see also Quirk 2006). Their index of Internet censorship is generated from surveys of 50 questions sent to legal experts, reporters, and scholars in each country. Thus, countries in northern Europe, the US and Canada, Australia and New Zealand, and Japan exhibit minimal or no censorship (scores less than 10). Conversely, a rogue's list of the world's worst offenders, including China, Vietnam, Burma/Myanmar, Iran, and Turkmenistan, exhibit the planet's most severe and extensive restrictions (scores greater than 80). In North Korea, Internet access is illegal, although the government uses it to send messages to the outside world (Hachigian 2002). In between these extremes lies a vast array of states with modest to moderate forms of Internet censorship that reflect their diverse systems of governance, the presence or absence of civil liberties, and the ability of various groups to resist limitations on their ability or right to use the Internet in whatever manner they so prefer. Using the categories of Fig. 2, Table 1 summarizes the distribution of the world's population and Internet users according to the level of severity of censorship. Thus, only 13% of the world's people, but a third of Internet users, live in countries with minimal censorship; conversely, roughly one-quarter of the world's people and Internet users live under governments that engage in very heavy censorship (the vast bulk of whom are located in China).

Internet penetration rates—the proportion of the population with regular access to cyberspace at home, school, or work—also shape the contours of censorship geography (Fig. 3). Rates vary from as low as 0.2% (Myanmar) to 100% (Falkland Islands).

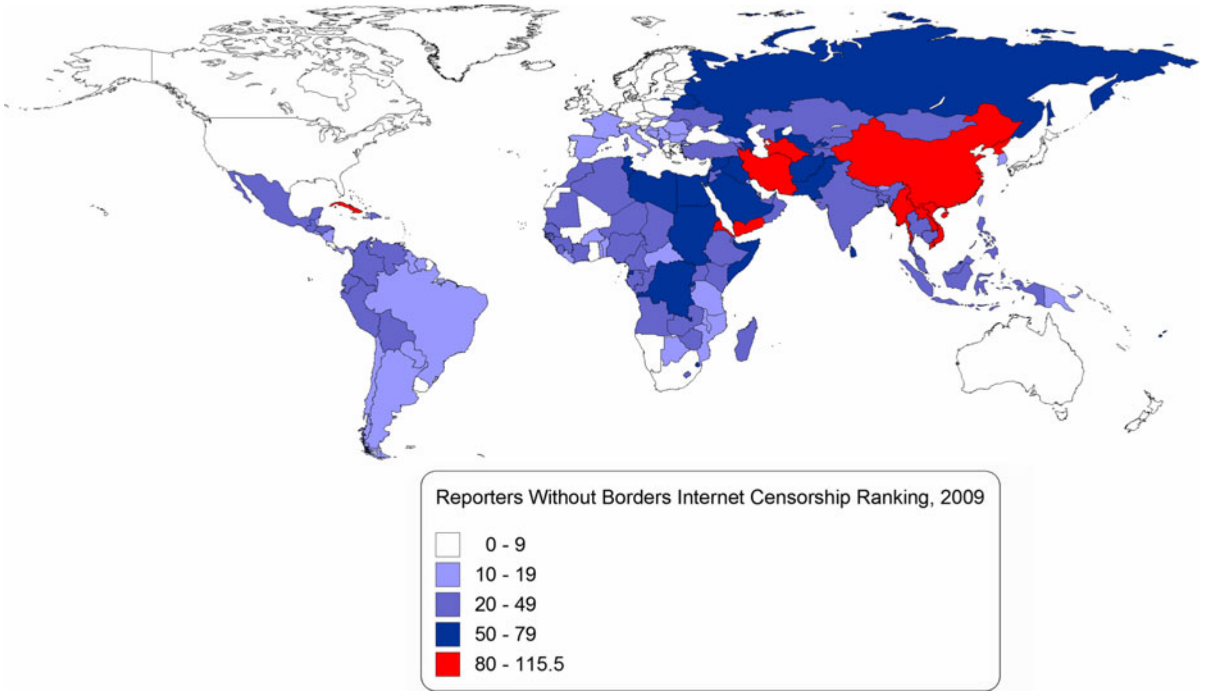

Fig. 2 Reporters Without Borders Internet Censorship Ranking 2009. *Source*: data drawn from http://www.rsf.org/en-classement1003-2009.html

Table 1 Global population and Internet users by severity of Internet censorship

RWB[a] score	Population (000s)	%	Internet users (000s)	%
0–9	912,137	13.4	629,208	31.9
10–19	743,610	10.9	320,059	16.2
20–49	2,826,536	41.5	400,853	20.3
50–79	732,971	10.8	139,775	7.1
80–115	1,602,751	23.5	480,462	24.4
Total	6,818,006	100.0	1,970,357	100.0

[a] Reporters Without Borders

Source: calculated by author

Penetration rates have important implications for state attempts at control. In impoverished states, in which penetration rates are low and users rely heavily on cybercafes, censorship is relatively easy and resistance is futile. However, falling prices for personal computers, expansion of home ownership, and rising technological prowess of users generate a population that is more difficult to monitor and discipline. Moreover, rising incomes, literacy rates, and technical skills often lead to modernizing elites that actively resist censorship through organized means. Indeed, unlike traditional media such as newspapers and television, whose centralized structures make them amenable to state control, the decentralized, rhizomic, interactive structure of the Internet makes it much more difficult for state authorities to manipulate. Nonetheless, it should be remembered that "it is actually easier for a government to computer search vast quantities of e-mail than to open regular mail or monitor tapped telephones" (Dunn 2000, p. 467). There is no guarantee, however, that censorship measures succeed. As Hachigian (2002, p. 41) points out, "The subtle choices regimes make about how to treat the Internet are designed to reinforce their broader strategies for retaining power, and those choices do not predict regime viability in a clear way."

However, Internet censorship should be seen as part of a more complex array of contested relations in cyberspace: the Web is not simply a tool a tool of government control, but an arena of conflict. Thus, the Internet also serves a variety of counter-hegemonic purposes, including human rights groups and ethnic or political movements in opposition to governments (Warf and Grimes 1997; Kreimer 2001; Crampton 2003). Attempts at censorship are often resisted, sometimes successfully, by local cyberactivists, such as through the use of anonymizing proxy servers in other countries that encrypt users' data and cloak their identities. Today, numerous groups in civil society use the medium to connect isolated once-invisible populations (e.g., gays and lesbians), unite and empower women's movements, give voice to human rights activists, and allow political minorities to promote their own agendas. Thus, Internet usage both reflects and in turn shapes prevailing political orders. In authoritarian regimes with relatively weak civil societies, opposition to

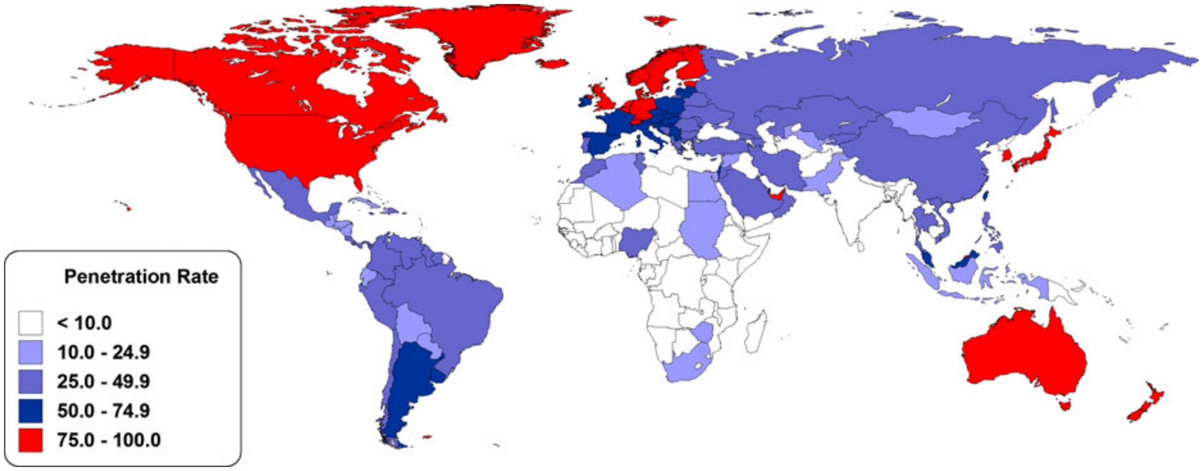

Fig. 3 Internet penetration rates, December, 2009. *Source*: calculated by author using data from www.internetworldstats.com/stats.htm

state-control is often weak and ineffectual; in more democratic states, opposition can be organized, vociferous, and effectual. When seen as a contested terrain of political struggle, the interactions between government Internet censors and the various groups that resist such impositions resembles a cat-and-mouse game that continually evolves over time. As the context of Internet censorship changes, including rising penetration rates, deregulation of telecommunications providers, and new geopolitical circumstances (e.g., openness to foreign investment), both government authorities and their opponents resort to changing tactics. Overt control over cybercafés, for example, may give way to government blockages of dissident websites, while opposition groups may utilize foreign proxy servers, anonymizing software, or texting by cell phones to circumvent such obstacles. The outcome of such contestations is inevitably path dependent, contingent, and unpredictable.

In this light, a rough sequence of stages of Internet censorship summarizes the major forms of state political intervention as they vary over time. Generally, authoritarian governments in countries with low Internet penetration rates resort to relatively crude measures, such as restricting public access through licenses and monitoring of cybercafes. A national, sanitized intranet may be offered as a substitute for the global Internet. Cuba, Vietnam, and Burma/Myanmar exemplify this approach. As more people move on-line, including rising home personal computer ownership rates, a more complex, expensive, and cumbersome set of censorship mechanisms is called for, including firewalls and blocking or filtering web-site access. Arrests and imprisonment of cyberdissidents may be common. China, Kazakhstan, and Saudi Arabia are prime exemplars of these tactics. A third stage involves widespread Internet access, in which "soft" censorship tactics are the norm, particularly self-censorship and encouraging ISPs to police their users. Singapore and Russia illustrate this type and degree of government intervention. Finally, at least in the hopes of many optimistic observers, widespread Internet usage can overwhelm the state's capacity to control dissent, as in northern Europe and the US and Canada.

To assess the effects of authoritarianism empirically, the analysis includes a brief statistical analysis of the relations between national Internet usage rates and political openness, or lack thereof, via the widely used Freedom House index of political freedom (www.freedomhouse.org). A non-governmental organization founded by Eleanor Roosevelt, Freedom House assesses countries on the basis of electoral freedoms, political pluralism, and civil liberties, including the number of political parties, degree of corruption, human rights abuses, autonomy of minorities, media censorship, and tolerance of political discussion. This measure ranges between 1 and 7 score (1 = most open). Of course, the Freedom House measure is not without its critics, who claim the group masks a conservative political agenda behind a façade of neutrality, demonizing governments at odds with the United States and overlooking faults of US allies. Despite these objections, its measure of political openness remains highly popular among social scientists in many different disciplines.

When compared with Internet penetration rates, a scattergram indicates that political freedom is an important driver of Internet usage (Fig. 4). A correlation of −.62 was statistically significant at the 95% confidence level ($N = 180$). Thus, the least democratic countries have among the lowest penetration rates, while the comparatively wealthy and democratic republics have by far the highest rates. Of course, the standard objection to such an approach is that both political freedom and Internet access are functions of national wealth. As several political observers maintain (Tilly 2007; Inglehart and Welzel 2005), wealthier countries are far more likely to be democratic ones. Controlling for wealth (as measured by GDP per capita in 2009), political freedom still exerts a powerful influence over penetration rates,[1] testifying to the autonomy of the political. In short, statistically at least, there are grounds for supposing that censorship does affect Internet penetration rates, although this analysis is admittedly preliminary, descriptive, and not predictive. Moreover, because censorship also occurs in countries with significant penetration rates, a more nuanced analysis is called for.

[1] The regression equation is $P = .18 - \underset{(3.9)}{6.8F} + \underset{(4.1)}{1.1\mathrm{GDP}}$, where P = internet penetration rate in 2009, F = Freedom House index in 2009, and GDP = GDP per capita in 2009. Numbers in parentheses below the equation are t-values of coefficients. $R^2 = .79$ ($N = 180$), significant at .95 confidence level.

Levels of severity of Internet censorship across the globe

There is a highly uneven topography of Internet censorship around the globe, one that reflects the geographies of the world's diverse political systems, the extent of Internet penetration rates, the social, cultural, and economic constitutions of various societies, and the degree of political opposition. Such complexity means that patterns of Internet censorship do not lend themselves readily to pat characterizations but require a more detailed, case-by-case analysis. The uneven landscapes of Internet censorship reflect the complex intersections between the growth of cyberspace and a large variety of regional, national, and local political and cultural contexts. Decisions of whether and how to regulate Internet access reflect the degree of centralization of political control, cultural attitudes toward dissent, and geopolitical concerns, particularly for states seeking to attract foreign investment. For example, countries seeking to promote development of an information technology sector or international exports of services (e.g., Malaysia), including tourism, are often concerned that Internet censorship can diminish the revenues from such efforts. This section explores Internet censorship using the levels of severity denoted by Reporters Without Borders, as depicted in Table 1 and Fig. 2.

Worst censors (RWB scores 80–115)

China

In a country with more than 420 million Internet users in June, 2010, Chinese Internet censorship is arguably the world's most severe (Kahn 2002). The Communist Party of China has long exerted strict, centralized control over flows of information within and across the nation's borders, largely through the Ministry of Information Industry (MII), although Internet policing is conducted primarily through the Ministry of State Security. The state has encouraged Internet usage, but only within an environment that it controls, and cyberspace in China remains relatively free compared to the traditional media. In the early phases of Internet development, the state did little to regulate cyberspace, but as chat rooms and blogs pushed the boundaries of allowable dissent with a steady stream of criticism of government officials, it began to tighten control significantly after 2000 (Bi 2001). Indeed, for the first decade the Internet likely strengthened the government's control, although as China's population of netizens grew explosively, it increasingly became a vehicle for challenges to the state's authority (Hachigian 2001), leading to increasingly harsh repression. In 2005, the OpenNet Initiative (2005) declared that "China operates the most extensive, technologically sophisticated, and broad-reaching system of Internet filtering in the world." The Chinese government has been blunt in its justification for censorship, asserting its necessity to maintain a "harmonious society."

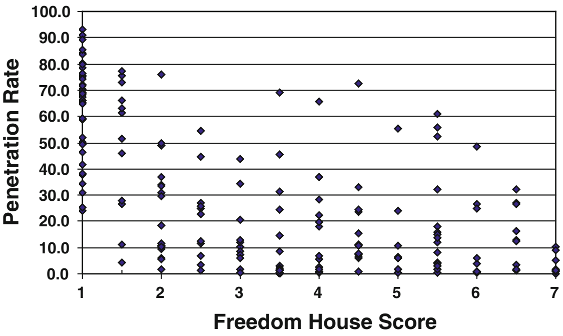

Fig. 4 Scattergram of freedom house score and Internet penetration rates, 2010. *Source*: author

The government deploys a vast array of measures collectively but informally known as the "Great Firewall," which includes publicly employed monitors and citizen volunteers, screens blogs and email messages for potential threats to the established political order. There are numerous components to the Great Firewall that operate with varying degrees of effectiveness. International Internet connections to China are squeezed through a selected group of state-controlled backbone networks. Popular access to many common Web services, such as Google and Yahoo!, is heavily restricted (MacKinnon 2008; Paltemaa and Vuori 2009). The national government hires armies of low-paid commentators, commonly called by the derogatory term the "five-mao party," to monitor blogs and chat rooms, inserting comments that "spin" issues in a light favorable to the Chinese state. Some municipal governments take censorship into their own hands: Beijing, for example, uses 10,000 volunteer Internet monitors (Wines 2010). However, a large share of censorship occurs via Internet companies themselves (MacKinnon 2009), which monitor chat rooms, blogs, networking services, search engines, and video sites for politically sensitive material in order to conform to government restrictions. Websites that help users circumvent censorship like anonymizer.com and proxify.com are prohibited. Users who attempt to access blocked sites are confronted by Jingjing and Chacha, two cartoon police officers who inform them that they are being monitored. Instant messaging and mobile phone text messaging services are heavily filtered, including a program called QQ, which is automatically installed on users' computers to monitor communications. Blogs critical of the government are frequently dismantled, although for the most part the government out-sources this function to blog-hosting companies (MacKinnon 2008). In 2006, for example, Microsoft's MSN Spaces blog-hosting site agreed to conform to government "guidelines" in return for freedom from censorship at the ISP level. In June, 2009, the government attempt to require manufacturers to install filtering software known as Green Dam Youth Escort on all new computers, but retreated in the face of a massive popular and corporate outcry (LaFraniere 2009), a lawsuit from a California firm, Cybersitter, alleging that China stole its software (Crovitz 2010), and the fact that Green Dam inadvertently jammed government computers (Lake 2009). In response, Falun Gong released a program to circumvent it called Green Tsunami.

The Great Firewall system began in 2006 under an initiative known as the "Golden Shield," a national surveillance network that China developed with the aid of US companies Nortel and Cisco Systems (Lake 2009) and extended beyond the Internet to include digital identification cards with microchips containing personal data that allow the state to recognize faces and voices of its 1.3 billion plus inhabitants. The envy of authoritarian governments worldwide, the Golden Shield has been exported to Cuba, Iran, and Belarus. Indeed, many respects, China's state-led program of Internet development serves as a model for other authoritarian governments elsewhere.

The Chinese government has periodically initiated shutdowns of data centers housing servers for websites and online bulletin boards, disrupting use for millions. Email services like Gmail and Hotmail are frequently jammed; before the 2008 Olympics, Facebook sites of critics were blocked. In 2007, the State Administration of Radio, Film and Television mandated that all video sharing sites must be state owned. Police frequently patrol Internet cafes, where users must supply personal information in order to log on, while web site administrators are legally required to hire censors popularly known as "cleaning ladies" or "big mamas" (Kalathil and Boas 2003).

At times government censorship can generate problems with foreign investors. The government for years blocked access to *The New York Times*, until its editors complained directly to President Jiang Zemin, but left the web site for *USA Today* unmolested (Hachigian 2002). In the Chinese case, Google, the world's largest single provider of free Internet services, famously established a separate, politically correct (by China's government standards) website, Google.cn, which censors itself to comply with restrictions demanded by the Chinese state, arguing that the provision of incomplete, censored information was better than none at all (Dann and Haddow 2008). In early 2010, responding to the ensuing international criticism, Google announced it would no longer cooperate with Chinese Internet authorities and withdrew from China. Untroubled, the Chinese government promotes its home-grown search engines such as Baidu, Sohu, and Sina.com, which present few such difficulties.

Finally, the Chinese state has arrested and detained several Internet users who ventured into politically sensitive areas. Although it cannot monitor all websites in the countries, the state pursues the intimidation strategy popularly known as "killing the chicken to scare the monkeys" (Harwit and Clark 2001). Reporters Without Borders reported in 2008 that China had incarcerated 49 cyberdissidents, the most in the world. For example, cyberjournalist Hu Jia, winner of the European Sakharov Prize for Freedom of Thought, was sentenced to 3½ years in prison in 2008 for "inciting subversion of state power." Human rights activist Huang Qi received a similar sentence that same year for posting criticisms of the Sichuan earthquake relief efforts. Librarian Liu Jin received 3 years for downloading information about the organization Falun Gong, which China treats as terrorists. China's best known blogger, Zhou Shuguang, was prohibited from traveling to Germany to judge an international blogging competition. Others have been prosecuted for posting or downloading information about Tibetan independence, Taiwanese separatism, or the Tiananmen Square massacre. No avenue exists to repeal censorship decisions.

Such measures have helped to limit the use of the web by democracy and human rights advocates, Tibet separatists, and religious groups such as Falun Gong. They also help proactively to sway public opinion in favor of the state. However, given the polymorphous nature of the web, such restrictions eventually fail sooner or later. By accessing foreign proxy servers, a few intrepid Chinese netizens engage in *fanqiang*, or "scaling the wall" (Stone and Barboza 2010). Using its programmers in the US, Falun Gong has developed censorship-circumventing software called Freegate, which it has offered to dissidents elsewhere, particularly in Iran (Lake 2009). Chinese censorship and its resistance thus form a continually change front of strategies and tactics: As one Chinese blogger put it, "It is like a water flow—if you block one direction, it flows to other directions, or overflows" (quoted in James 2009).

Vietnam

Vietnam's Leninist state has long pursued a rigid path of Internet censorship (Pierre 2000). The country's sole ISP with a license for international connections, Vietnam Data Communications, is a subsidiary of the government telecommunications monopoly. Domestic content providers must obtain special licenses from the Ministry of the Interior and lease connections from the state-owned Vietnam Post and Telecommunications Corporation. The state uses a complex system of firewalls, access controls, and strenuously encouraged self-censorship. E-mail is regularly monitored by searches for key words. Vietnam has imprisoned those who dare to use the Internet to speak out against the government, such as Pham Hong, a doctor who posted an online article calling for democracy (International Censorship Explorer 2006). Owners of cybercafés who permit searches of unauthorized websites by their clients face fines of 5 million dong, roughly US$330 (Kalathil and Boas 2003). Despite the liberalization efforts known as *doi moi*, the Vietnamese Communist Party keeps a firm grip on cybertraffic, particularly Internet sites considered to be "offensive to Vietnamese culture" (Human Rights Watch 2002). In 2003, the government lashed out at Reporters Without Borders after the organization listed the country as one of the world's 15 worst censors of the Internet.

Burma/Myanmar

The government of Burma/Myanmar, according to the OpenNet Initiative (2005, p. 4), "implements one of the world's most restrictive regimes of Internet control." The ruling junta, the State Peace and Development Council, bars 84% of sites "with content known to be sensitive to the Burmese state" (p. 4). It also excludes email sites such as Hotmail and Yahoo because they cannot be monitored for political criticism, and pornography. The 1996 Computer Science Development Law requires that all network-ready computers be registered with the Ministry of Communications, Posts and Telegraphs. Burma/Myanmar has only two Internet service providers, and both outlets charge high prices for email accounts. To implement its censorship, the government purchases software from the US Company Fortinet to block access to selected websites and servers. At times, the state has resorted to blunter instruments: when it sought to silence demonstrators in 2007, it switched off the country's Internet network altogether for 6 weeks.

Iran

One of the world's more repressive governments in terms of Internet regulation, Iran maintains strict control over cyberspace through its state-owned telecommunications monopoly, Telecommunication Company of Iran, run through the Ministry of Information and Communication Technology, to which all Iranian ISPs are connected. Like many countries, Iran manages its censorship at the level of ISPs, which must agree to prohibit access to "non-Islamic" web sites. As the Internet has emerged as prominent domain in which political dissent, the government's restrictions have grown proportionately. In 2001, the government assumed control over all international traffic entering or leaving the country, and claims to have blocked access to five million websites. Roughly 20 official categories of prohibited websites exist, including those that insult Islam, promote national discord, pornography, and immoral behavior. In 2006, all websites and blogs were required to obtain licenses from the Ministry of Islamic Culture and Guidance or risked being declared illegal. Also in 2006, the government outlawed Internet connections faster than 128 kbps, entailing stiff resistance from business leaders. The government's surveillance of dissidents was abetted by purchases of European spy technology from Siemens and Nokia (Rhoads and Chao 2009), particularly a technique called deep packet inspection, which allows authorities not only to block email and Internet telephony but to identify users' names. Foreign spyware have now been complemented by domestically produced versions (OpenNet Initiative 2009a, b). In 2009, in the face of massive anti-government protests—themselves organized through social networking channels—the Iranian regime cracked down yet again, imprisoning dozens of dissenting bloggers under the aegis of Tehran Prosecutor Saeed Mortazavi.

However, Iran has found Internet censorship increasingly difficult to administer. During the 2009 crackdown, for example, amateur videos of government attacks on demonstrations circulated virally on the Web. In response, the government slowed down the maximum transmission rates on its Internet backbones, making traffic in videos slow and difficult. Using free, downloadable software to circumvent government filters called Freegate and Ultrasurf, which were developed by China's Falun Gong (Lake 2009), Iranian protestors repeatedly resisted government controls over cyberspace at critical political moments. Some observers argue that the Internet has "certainly broken 30 years of state control over what is seen and is unseen, what is visible versus invisible" (Stelter and Stone 2009).

Severe censors (RWB scores 50–79)

Russia and Belarus

The archipelago of countries consisting of Russia and neighboring states—a region long known for many governments that resist transparency, abuse human rights, and rely on state-controlled media—exhibits numerous attempts to restrict access to the Internet as well as govern its contents. In Russia, where the conventional media are already under tight government control, the Putin government gradually sought to extend its influence over the Internet, essentially following the Chinese model of granting the secret service extensive monitoring powers, ostensibly on the grounds of fighting corruption (Troianovski and Finn 2007). As Russia's penetration rate increased, threatening to broaden the sphere of public debate and give rise to autonomous voices, the administration responded by purchasing independent websites, promoting pro-government websites, and fostering a network of government-friendly bloggers. Russia's Internet surveillance law, the System for Operational-Investigative Activities, allows state security services unfettered physical access to ISPs and requires them to report statistics about users, and has been emulated, to one extent or another, by other countries in this region. In Ukraine, where the Internet remains relatively free, the state-owned provider Ukrtelecom is the largest ISP in the country; even here, however, government officials have raided the offices of online newspapers, such as *Obkom*, on national security grounds. In 2003 the Ukrainian Parliament passed the Law on Protection of Public Morals (OpenNet Initiative 2007). Under the guise of combating terrorism, the Ukrainian state has held that censorship is necessary to secure the "national information space".

In Belarus, whose government Reporters Without Borders called one of the world's "bitterest enemies of the Internet," President Lukashenko claimed that he would "put an end to the anarchy" online and would "not allow humanity's great technical achievement to become a news sewer" (Reporters Without Borders 2008). The point was backed up by the presence of government troops at Internet cafes. All Belorussian ISPs are required to connect through Belpak, a subsidiary of the state-controlled ISP Beltelecom. During the 2006 presidential elections the government launched "just-in-time" cyberattacks against opposition party websites, which often mysteriously suffered frequent disconnections.

Pakistan

The Pakistan Telecommunications Authority (PTA) repeatedly filters Internet content deemed to be irreligious, antimilitary, or secessionist. All international traffic to and from the country is routed through three sites owned by Pakistan Internet Exchange, with locations in Islamabad, Lahore, and Karachi. The 2006 Net Café Regulation bill requires Internet cafes to monitor patrons, although its enforcement has been dubious (Reporters Without

Borders 2004). The PTA has banned dozens of URLs that published Danish cartoons ridiculing the Prophet Mohammed; indeed, the Pakistani police attempt to register all websites containing “blasmephous material” (Ahmed 2002). Baluchi nationalist and human rights sites are also blacklisted. The Pakistani cybercommunity responded to these initiatives with a “Don’t Block the Blog” campaign (http://dbtb.org/), which, among other things, has exposed the military’s numerous civil rights violations.

Arab world severe censors

In most of the Arab world, the media are closely monitored and controlled by governments, either through laws and regulations or via direct ownership in state monopolies (Warf and Vincent 2007). Cyber-journalists, editors, and bloggers may face penalties for “slighting the Islamic faith,” blaspheming government officials, promoting political change, or advocating “immoral behavior”. Arab governments typically excuse their censorship on the grounds that they are protecting Islamic values and morality. Sometimes this justification is linked to an alleged onslaught of Western decadence against Islamic values (Fandy 1999). Offensive sites generally are held to include pornography, homosexuality, drugs, gambling, and atheism. However, like autocratic regimes the world over, many Arab governments are afraid of their citizens having access to *any* substantive political information about the outside world. Censorship may also generate profits for the government, including limited potential access of customers to rivals of state-owned telecommunications companies. Nonetheless, despite these restrictions, the Internet has opened myriad spaces of Arab political debate that transcend national boundaries (Ghareeb 2000; McLaughlin 2005; MacFarquhar 2006).

Censorship in the Arab world is most acute in Saudi Arabia. Public access to the Internet in the kingdom was made possible only when the state deemed that it could effectively control it; the entire Internet backbone network is state-owned. Thus, while the kingdom has sought to garner the economic benefits of the web, it has also strenuously tried to prevent it from challenging the highly conservative basis of its rule (Teitelbaum 2002). The Saudi state has erected extensive firewalls to control the flow of digital information. Saudi Internet cafes are required to record the names of the customers and the times they arrive and depart, information that must be delivered to state security upon request; persons under 18 are forbidden unless accompanied by an adult. By royal decree, the King Abdul Aziz City for Science and Technology (KACST), a government-owned research center, is the only portal through which ISPs can make international connections (www.unesco.org/webworld). This mechanism operates using commercial software produced in the United States, Secure Computing’s SmartFilter (Lee 2001), which has also been sold to and utilized by the governments of Iran, Yemen, Tunisia, the U.A.E., and Sudan (Villeneuve 2006). Requests from Saudi ISPs to access the outside world must pass through state-controlled servers. According to the OpenNet Initiative (2004), in 2004 more than 400,000 web pages were banned by the Saudi regime (about 2.2% of all sites tested in a sample), the vast bulk of which pertained to adult material but also including some games, recreational sites, on-line shopping, Yahoo, America On-Line, and even medical websites that use words like “breast,” if only in a medical context. Access attempts to banned sites are logged by the state, which understandably encourages widespread self-censorship.

Many Arab states follow the Saudi model to different degrees. In 2006, Bahrain and Jordan blocked access to Google Earth and Skype, respectively, citing national security concerns (BBC News Online 2002). In Syria, the government blocks access to Kurdish-language news websites overseas and any domain ending in “.il,” i.e., Israel. In Tunisia, the government forbids access to services such as Hotmail and human rights websites; in addition, every ISP must submit a monthly list of subscribers to the state censorship agency. In 2002, a Tunisian court sentenced cyber-activist Zohair Ben Said al Yehiawy to 2½ years in jail for criticizing the judiciary and corrupt police practices (www.hrinfo.net/en/reports/net2004/tunis.shtml). Tunisia’s suppression of freedom of speech led Reporters without Borders to criticize the United Nations’ 2005 World Summit on the Information Society in Tunis as a joke. In Iraq under the regime of Saddam Hussein, Internet access was strictly limited (Ghattas 2002). In 1997, the Iraq government newspaper *al-Jamhuriyya* denounced the Internet as “an American means to enter every house in the world” (Anderson 1997).

Moderate censors (RWB scores 20–49)

Thailand, Malaysia, Singapore, and Indonesia

Many countries in Southeast Asia exhibit multiple forms of Internet censorship. Many governments in the region often justify such intervention on the grounds that they share "Asian values" ostensibly at odds with Western notions of democratic access (Hachigian 2002). In Thailand, the number of blocked websites jumped markedly after the military coup of January, 2006. When YouTube posted a silly 44-s video ridiculing King Bhumibol Adulyadej in 2007, the government temporarily banned the website entirely throughout the country and deported the producer, a Swiss national, back to his country.

Seeking to encourage growth of his country's information technology sector, Malaysian Prime Minister Mahatir Mohamad declared publicly in 1996 that there would be no censorship of the Internet, in part to give his country an edge over neighboring rival Singapore. As a result, "pro-reform websites have matured from a cacophony of accusatory and insulting diatribes into an alternative, independent media" (Abbott 2001, p. 105). However, in 2002, the Malaysian government signaled its intent to require website operators to obtain licenses precisely for the purpose of monitoring content, and has tried to restrict Muslim fundamentalists from publishing on the web. The country's famed Multimedia Corridor, however, designed to attract foreign investors, remains a censorship-free zone, revealing that the geographies of censorship vary not only among countries but within them as well.

The authoritarian government of Singapore, one of the world's best-connected and technologically dynamic countries, also censors the Internet regularly (Rodan 2000). Its primary vehicle in this regard is the Singapore Media Development Authority (MDA), which has regulated Internet content under the guise of monitoring a broadcasting service since 1996. All ISPs are automatically licensed by the Singapore Broadcasting Authority, which routes all Internet connections through government proxy servers. Licensees are required to comply with the 1996 Internet Code of Practice, which includes a definition of "prohibited material," i.e., content that it deems "objectionable on the grounds of public interest, public morality, public order, public security, national harmony, or is otherwise prohibited by applicable Singapore laws" (OpenNet Initiative 2006, p. 3). Moreover, "the government has at times taken unannounced strolls through several thousand personal computers with Internet connections, subsequently explaining such actions as sweeping for viruses or pornography" (Kalathil and Boas 2003, p. 78). Self-censorship is also encouraged as a means to stifle political expression. The use of lawsuits under stringent defamation laws is also common, and can reach well beyond the island's perimeter. For example, Jiahoa Chen, a Singaporean student at the University of Illinois, was forced to shut down his caustic.soda blog under threat from the government-run Agency for Science, Technology, and Research (OpenNet Initiative 2006). As a result of these measures, Singapore's government has achieved near-total control over its Internet environment with minimal loss of political legitimacy. Zittrain and Palfrey (2008), however, argue that Singapore's censorship has been exaggerated and is largely confined to a handful of pornographic websites.

India

India, despite its generally democratic practice of governance, has nonetheless also engaged in moderate Internet censorship. In 2000, the Indian Parliament approved the Information Technology Act to crack down on cybercrime, allowing cybercafes and Internet users' homes to be searched without warrants as part of criminal investigations. It also allowed the government to block access to sites considered pornographic or that "endanger public order, the integrity and security of the nation and relations with other countries." Those setting up "anti-Indian" websites can be jailed for up to 5 years (Reporters Without Borders 2004, p. 1). In 2002, India enacted the Prevention of Terrorism Ordinance Act authorizing the government to monitor electronic communications, including personal email. The Indian cybercafé association, the Association of Public Internet Access Providers, strenuously protested against the measures, which it said would lead to the closure of most of the country's 3,000 or so cybercafés.

Central Asia

Central Asia exhibits a pronounced tendency toward heavy Internet censorship. For example, the same "event-based filtering" practiced by the Belarussian government occurred in Kyrgystan during the 2005 parliamentary elections there. In Uzbekistan, ISP providers must operate under government control, the government's web filter, Uzpak, enjoys a monopoly over international connections, monitors all Internet traffic in the country, and the government often shuts down uzbekistanerk.org and birlik.net, the Web sites belonging to the largest opposition parties (Privacy International 2003). In Kazakhstan, a journalist from the news website kub.kz, Kazis Toguzbayev, was given a 2 year prison sentence in 2008 for posting an article accusing the regime of protecting the killers of opposition leader Altynbek Sarsenbayev. Invoking an older Soviet tradition, Uzbek Internet journalists who publish criticisms of the government are occasionally forced into psychiatric hospitals. The dictator of Turkmenistan, Saparmurat Niyazov, another of Reporters Without Borders's ardent "enemies of the Internet," strove to keep that country hermetically sealed from the outside world via a national intranet, although his successor, Gurbanguly Berdymukhammedov, vowed to open it up to the global Internet. This promise was belied, however, by the presence of government soldiers at the doors of Internet cafes (Eurasianet.org 2007). Cybercafes in which customers attempt to access banned websites are routinely closed.

Azerbaijan seems to have to have taken electronic governance to heart (Hajiyev 2006). While Azeri Internet provision is highly centralized via two state-owned ISPs, the Azeri web remains relatively free from government filtering. Nonetheless, when two Azeri bloggers posted a video ridiculing the government's purchase of high-priced donkeys, they were arrested (Barry 2004).

The Internet has also been used against the state in several such countries. Between 2003 and 2005, Ukraine, Georgia, and Kyrgyzstan all experienced "color revolutions," in which opposition parties utilized the web as an integral part of their strategy and suffered just-in-time blocking by their governments (Warf 2009b). A growing community of Eurasian cyberactivists resists Internet censorship (see Eurasianet.org). The Uzbek "For a Free Internet!" campaign, for example, has monitored bills in the lower house of parliament, the Mazhlis, which attempt to extend the government's censorship. The Tajik government's attempts to criminalize some forms of cyber-speech as libel against the state were met with heated opposition led by Nuriddin Qarshiboev, head of the National Association for Independent Media in Tajikistan. Moreover, Tajik cyber-journalists petitioned the government to abolish the requirement that the president be called "worthy" and "reliable" every time he was mentioned. More recently, those seeking to avoid government censorship can download software designed to help them do so, such as the Canadian "censorship circumvention" program Psiphon.

Arab world moderate censors

The United Arab Emirates (UAE) is often heralded as the Internet star of the Middle East, with relatively a high penetration rate and a government eager to diversify the economy. However, here too censorship is the norm. All telecommunications passes through the government monopoly, Etisalat, which operates the country's only ISP. Filtering of Internet content at cybercafes blocks sites that are blacklisted by the state, although leased lines in businesses and homes are exempt. The UAE Minister of Transportation, Ahmed Hameed Al-Taier, claimed that his government's filtering system "was the main reason behind the spread of the Internet in the country. Many people allowed access to the Internet inside their homes upon the condition that there be some sort of censorship to protect their families from websites offensive to their morality" (Arabic Network for Human Rights Information 2004).

Some Arab countries, such as Egypt, Jordan, and Lebanon, are relatively lenient with regards to Internet regulation. Typically such states are oriented toward the West and at least grudgingly accept the need for democratic access to the Internet (Anderson 2003), such as in Jordan (Cunningham 2002). Morocco is often included in this category, although it assiduously blocks access to web sites promoting independence for the Western Sahara. Egypt is often celebrated for its relative lack of overt censorship, reflective of a regime eager to encourage tourism and court foreign investors. Even so, the Egyptian state created an agency in 2004, the Department to Combat Crimes of Computers and Internet, to censor "subversive" Internet sites, and has arrested programmers, journalists and human rights activists for violating censorship standards. In 2001, Shuhdi Surour, the webmaster for *al-Ahram Weekly* newspaper was arrested for posting a poem online critical of the state (Bahgat 2004). Despite the government's attempts to halt the publication of several books, many authors found alternative outlets on the Web (Gauch 2001). One of the most important political uses of the Internet in Egypt involves the Muslim Brotherhood, which, while technically illegal, engaged in cybercampaigns but whose activities are closely monitored.

Oman and Yemen offer contrasting models of Internet censorship. In Oman, the government-owned OmanTel is the monopoly provider of fixed and mobile telephony services, and facilitated the purchase of PCs through instalment payments. In contrast, Yemen's government ordered all Internet cafes to remove barriers between computers to ensure users lacked privacy when on-line (OpenNet Initiative 2006), leading to a decline in the number of such establishments. Almost all Yemen's efforts, implemented through a product called Websense, are directed against pornography, although some anti-Islamic sites are also blocked.

Israel's enduring confrontation with the Palestinians has also taken the form of Internet censorship. Before the Oslo Accord of 1995, the Israeli military's Order 1,279 forbid Palestinians from using electronic transmissions for political purposes, including leased telephone lines (Parry 1997). In response, Palestinians in the West Bank created a wireless network, PalNet, using microwave transmitters, which has been subject to occasional disruptions by the Israeli army. In 2000, the Israeli government attempted to shut down several Hezbollah websites (Diker 2003), leading to retaliation by Palestinian hackers against the Israeli Foreign Ministry's website, flooding it with spam messages. The Palestinian Authority launched a Hebrew-language version of its Wafa news agency website to circumvent what it called Israel censorship of cyberinformation. The Israeli government has also actively recruited bloggers to combat anti-Zionist websites, including those that deny the Holocaust. Finally, it should be noted that the ultraorthodox community within Israel has attempted to impose Internet censorship as well, efforts directed primarily at preventing access to adult material on-line.

Turkey briefly blocked a YouTube site that insulted the founder of the modern Turkish state, Kemal Ataturk. In 2000, the Ministry of the Interior barred Internet cafes from allowing access to websites that espoused anti-secularist (i.e., Islamicist) or Kurdish nationalist views (*Economist* 2007). In 2007, after the Turkish parliament passed legislation regulating Internet access there in less than 1 h of debate, the number of websites blocked in the country immediately jumped from zero to 2,600 (Anderson 2009).

Subsaharan Africa

In Subsaharan Africa, minuscule Internet penetration rates and an enfeebled civil opposition have done little to curtail censorship efforts. Resisting the global tide of neoliberal deregulation and privatization that has washed over telecommunications markets worldwide, many African governments have retained state monopolies over information services. Levels of censorship vary widely across the continent, of course. At one extreme is Sudan, where Internet usage is almost entirely concentrated in Khartoum, the government openly boasts of censorship; the government's telecommunications monopoly, Sudatel, was blacklisted by the United States as part of a broader strategy to resolve the violence in Darfur (OpenNet Initiative 2009b). The other end of this censorship spectrum is South Africa, which has negligible government interference in cyberspace. Most African states fall in between these poles. In Kenya, the administration used several censorship strategies, such as restricting bandwidth offered to ISPs through the state-owned Internet backbone and demanding that ISPs turn over their subscriber lists (Africa ICT Policy Monitor 2006). In 2000, the Communications Commission of Kenya ordered the closure of the month-old Kenya Internet Exchange Point, ostensibly on the grounds of preventing its use by 'terrorists' but more likely because it infringed upon Telkom Kenya's monopoly. Zimbabwe's government issued numerous laws to limit freedom of expression of the media, including the Broadcasting Services Act, the Zimbabwe Broadcasting Corporation Commercialisation Act, and the Public Order and Security Act (POSA). Its Monitoring and Interception of Communications Centre may compel ISPs to install software to intercept information deemed necessary by the state (Burnett 2005). The government also blocks certain websites using legislation such as POSA: For example, the website of the Movement for Democratic Change (www.mdczimbabwe.com) has been shut down a number of times (http://www.privacyinternational.org).

Latin American moderate censors

Latin American Internet censorship is typically less egregious than that found other parts of the world. The region's most restrictive policies are found in Cuba, where Internet and e-mail access is jealously guarded by the government, which controls the country's only Internet gateway and four national ISPs (Kalathil and Boas 2001). In 1996, the Cuban Executive Council of Ministers initiated Decree Law 209, which governed Internet access in that country. With six competing ministries vying for control, however, it proved to be bureaucratically unfeasible, and in 2000 censorship authority was passed to the Ministry of Computing and Communications. Faced with high prices of computer equipment, partly due to the long standing US trade embargo, Cuba has rejected a market-led model of Internet development in favor of a collective, government-led one that emphasizes institutions, not individuals. As a result, "individual access to the Internet has been essentially prohibited" (Kalathil and Boas 2003, p. 55). Commercial ISPs are allowed to provide individual accounts only to people who have obtained sponsorship from government agencies. Until recently, all Internet accounts had to be registered through the National Center for Automated Data Exchange at the cost of $260 a month (the average Cuban makes $240 per year). Relaxation of this restriction in 2006 helped to fuel the boom in Cuban Internet access. Nonetheless, differential pricing ensures that access to the nation's intranet remains considerably cheaper than international networks. Access to Internet cafes with international connections must be paid for in US dollars, which are scarce among Cubans. Nonetheless, a growing network of *informáticos*, or technologically savvy individuals, has contested these restrictions, and in the US, conservative groups such as the Cuban American National Foundation maintain web sites criticizing the regime.

Light Internet censors (RWB scores = 10–19)

Latin American light censors

Many governments with unsavory human rights records in the past, such as Brazil, now are remarkably open with regard to the Internet, although Brazilian courts have ordered ISPs to block access to certain blogs and YouTube videos that carry material "defamatory" to the state. Similarly, Argentina passed an anti-censorship decree for the Internet. In some countries, including Costa Rica, which is known for its democratic governance, journalists have been harassed by the state when exposing corruption in ruling circles on the Internet (Privacy International 2003).

Less draconian is the attempt of the Chilean Chamber of Deputies, which passed a bill allowing judges to punish Internet users who are "offensive to morals" or the "public order" (Cortés 2000). The order was aimed at websites located within Chile, i.e., with the.cl domain name, and was utterly ineffective against sites located outside the country. An attempt to prohibit access to Alejandra Matus's *The Black Book of Chilean Justice*, an expose of the ineffectiveness of the judiciary, led to its publication on the web and even wider readership.

In contrast with Chile, the Peruvian government passed the Transparency and Access to the Public Information Act, which created public access Internet terminals, and established the Telecommunications Investment Fund, which is responsible for promoting universal Internet access. Peru's Transparency and Access to the Public Information Act includes the creation of public information portals and considers governmental information as accessible to citizens.

Southern and Eastern Europe

Southern European countries generally exhibit less tolerance for Internet dissent than do their northern counterparts. In Italy, the Vatican called for restrictions on the Internet's "radical libertarianism," and the Italian government has shut down websites critical of Catholicism. The government has also attempted to force ISPs from allowing websites that defend or instigate crimes or portray the Mafia in a positive light. Following the assassination of a town councilor in northern Spain, a website for the Basque separatist electronic journal Euskal Herria, based in San Francisco, was shut down by email bombs believed to be initiated by the Spanish government (Conway 2007).

In Eastern Europe, with a long history of censorship under Soviet occupation, attempts to control the

Internet have been more explicit and widespread. In Bulgaria, for example, the government's attempt to license ISPs that included the collection of user names and passwords was defeated by the Internet Society of Bulgaria on the grounds that it served political rather than economic purposes. Moldovan Internet café owners formed the Internet Club Association to lobby against restrictions to access. In the former Yugoslavia, Internet censorship was widespread under the government of Slobodan Milosovic in the 1990s. Cyber-repression included: the arrest and persecution of the journalist Miroslav Filipovic, who wrote about military human rights abuses; politically motivated tampering with websites during the 2000 presidential elections; filtering of academic networks; and ordering some ISPs to close politically "unsuitable" websites. The overthrow of the Milosovic regime in 2000 greatly improved that country's affairs in this regard.

Uncensored (RWB scores 0–9)

Western Europe

While European countries are generally relatively open in terms of Internet access, there too several governments attempt to restrict what is said in cyberspace. Generally, however, censorship in economically developed countries focuses more on social concerns such as pornography or intellectual property than overt attempts to stifle political dissent. Often moves to restrict access are strenuously opposed by privacy advocates and some ISPs. Indeed, most attempts to censor the government in Europe have backfired. In addition to large, mobilized constituencies that advocate Internet liberties, economic integration has reduced European states' room to maneuver on this issue: for example, in 2008, the European Parliament passed a proposal that treats Internet censorship as a free trade barrier. While aimed at EU trade relations with countries such as China, the measure also limits domestic censorship.

Despite these obstacles to censorship, some European countries do engage in mild forms of Internet censorship, to widely varying degrees. Northern Europe tends to be especially mild, with Reporters Without Borders reporting zero interference in Scandinavia. However, in Finland, a nation widely celebrated as a bastion of high tech democracy, when hacker Matti Nikki's website criticized government efforts to regulate the Internet, the government added it to its list of proscribed child pornography sites, blocking access by ISPs. A Finnish government attempt to censor Internet message boards in 2003 was met with stiff resistance from telecommunications and media companies. In the United Kingdom, it is illegal to look at any of a list of websites kept by the Internet Watch Foundation (Anderson 2009). Starting in the mid-1990s, the German government attempted to shut down foreign sites that promoted racial hatred; more recent efforts, led by the Minister of Family Affairs, have focused on child pornography. Similarly, in France, the government in 2000 banned Yahoo! from allowing access to websites that promote racial hatred or sell Nazi memorabilia or those portraying child sexual abuse. In both France and Germany it is impossible to search for Nazi materials on-line using Google (Conway 2007). More recently, government officials have tracked down bloggers who insulted them and filed intimidating legal challenges (Sayare 2009). With some of the world's toughest antipiracy laws, the government now fines persons who repeatedly download illegal material.

United States

Although it often trumpets itself as a paragon of democracy, and although Internet censorship in the US is minimal, there too the state has intervened occasionally in attempts to shape Internet access. Whereas the first attempts to regulate cyberspace were caught up in culture wars between liberals and conservatives, more recent attempts have been more explicitly corporatist in nature.

The most egregious case of American Internet censorship involved the Communications Decency Act (CDA), passed by Congress in 1996 in an attempt to limit children's access to pornography (however loosely defined) on the Internet by facilitating government censorship, particularly the distribution of "patently offensive" materials to minors, essentially catering to the political agenda of the Christian Right. Resistance to the CDA was ferocious, including lawsuits by a coalition of ISPs, leading to the Supreme Court to overturn the law in 1997.

More recent government Internet censorship efforts in the US involve private sector proxy actors

(Kreimer 2006). Thus, Congress has mandated that public schools and libraries install filtering software, and holds ISPs responsible for providing access to child pornography. In this reading, censorship is a means of controlling "negative externalities" such as Internet crime and pornography that the market, left to its own devices, would fail to control. Congress has also initiated incentives for ISPs to block access to websites that infringe on intellectual property rights. Under the USA PATRIOT Act, the Federal Bureau of Investigation has a "good corporate citizen" program that encourages ISPs to censor websites that are not consonant with the public interest and to turn over information about users whose email reveals suspicious intent (Gellman 2005). The administration of George B. Bush enacted legislation encouraging telecommunications companies to engage in data mining on anti-terrorist grounds; indeed, "with respect to online surveillance, the United States may be among the most aggressive states in the world in terms of monitoring online conversations" (Deibert et al. 2008, p. 232). Whereas issues of copyright infringement or child pornography constitute legitimate concerns in this regard, other applications, particularly restrictions on political information, lie at the end of the slippery slope that such measures entail.

Discussion: a Habermasian critique

Many groups in closed societies can view digital information in a manner unavailable in censored print or broadcast media, undermining state monopolies over the media, and enhancing, if slowly and contingently, moves toward democratic governance (Slane 2007). Precisely because cyberspace facilitates relatively easy, unfettered access to information, it has been viewed with alarm by numerous governments. In and of itself, of course, the Internet does not simply produce positive or negative effects, for its information is always filtered through national and local cultures, biases, and predispositions. However, as ever larger numbers of people are brought into contact with one another on-line, cyberspace may expand opportunities for engaging in political activity, some of which challenges or delegitimizes prevailing models of authority by undermining the monopoly of traditional elites over the means of communication. The Internet is relatively low in cost and easy to use, and thus reduces a major obstacle to the participation in public debate by the poor. Because it allows access to multiple sources of information, including films and images, the Internet has facilitated a generalized growth in awareness of foreign ideas, products, and political norms. Indeed, as Yang (2003) suggests, given how widespread digital communications have become, the Internet and civil society have increasingly come to co-evolve, energizing and shaping one another in time and space.

In this way, cyberspace closely resembles Habermas's (1979) famous "ideal speech situation" in which unfettered discourse is central to the "public sphere" and in which discursive truth is constructed in the absence of barriers to communication (Poster 1997). One of the twentieth century's leading social philosophers, Habermas has long maintained that unconstrained communications are mandatory to broader processes of consensus construction, in which people of all backgrounds partake in public, positive and normative interpretations of their worlds. In what is essentially a pragmatist defense of Enlightenment ideals, his notion of communicative rationality, which is central to his critical theory, refers to the procedures of open debate and criticism, which he holds became increasingly widespread with the growth of modern bourgeois society. The "ideal speech situation" is vital to the operation of civil society in which social life is successfully reproduced and transformed. The ideal speech situation never exists in reality, but functions as a Weberian ideal type, a counterfactual yardstick by which to judge real-life contexts and the obstacles that generate distorted communication. In a situation in which all power relations constraining debate have been removed, all participants are free to provide input into the norms of truth production. As Luhmann (1996, p. 885) notes,

> Habermas does not locate the problem at the level of actually occurring communications. … Instead, he employs a theory of how the reasonable coordination of actions can take place if assured of the freely rendered agreement of all involved.

Thus, in this conception, reason, truth, logic, and self-reflexivity are not located in some abstract transcendental realm but are grounded in praxis.

The only criterion that remains for resolving contesting claims is their truth-value, which rests on the "force of a better argument," leading to a consensus theory of truth that rejects absolute foundations for knowledge in favor of procedural ones. Importantly, "the participants in an ideal speech situation [must] be motivated solely by the desire to reach a consensus about the truth of statements and the validity of norms" (Bernstein 1995, p. 50). Later, in *The Structural Transformation of the Public Sphere* (Habermas 1989), he argued that civil society, located between the state and everyday life and with origins in the rise of industrial capitalism and the Enlightenment, had become thoroughly dominated by large corporations, reducing citizens to spectators and consumers of goods (see Kellner 1979, 1990).

Habermas's critics have argued that his view exaggerates the power of reason to obtain consensus and that he obfuscates inequalities in access to public discourse such as class, gender, and ethnicity. Thus, Habermas holds up an ideal that can never be realized in practice (Hohendahl 1979; Calhoun 1992). Despite these objections, it is worth noting that the ideal free speech situation remains the prevailing normative standard against most contemporary conceptions of the political economy of unfettered access to and production of knowledge are compared, particularly with regard to the legitimacy of legal institutions (Froomkin 2003).

Cyberspace in all its diverse forms—chat rooms, blogs, and email, as well as neogeographic practices such as wiki-webs—arguably exemplifies the Habermasian vision of diverse groups engaging in practical discourse more than any other realm today. Enhanced access to information empowers citizens, facilitates debate, and may alter political outcomes. In particular, the Internet allows communities of shared interests to form around common discourses that express identities and foment mutual understandings within a broader, heterogeneous, differentiated civil society. Of course, the reality of unequal digital access is never a perfect reflection of the idealized norm: the digital divide, at multiple spatial scales, signifies that social and spatial inequalities are reproduced inside of cyberspace. That said, at minimal cost and easy to use, the Internet allows for the construction of a negotiated consensus that lies at the heart of legitimate political rule. As Froomkin (2003, p. 856) puts it, "In Habermasian terms, the Internet draws power back into the public sphere, away from other systems." More generally, by shifting the production of meaning from the few to the many, unfettered electronic communication allows truth to be uncoupled from power.

Given this ideal, Internet censorship represents a particularly egregious infringement not only upon democratic norms of liberty, equality, and informed dissent, but upon the discursive capacity of citizens to construct their worlds. Far from challenging existing power relations, censorship of cyberspace thus amplifies them. At risk, when and where censorship succeeds, is the production of reason itself: if, following Habermas, truth is the consensual outcome of reasoned debate, then government limitations on Internet access and attempts to shape the contents of cyberspace fly in the face of peaceful resolutions of differences. Ever since Foucault, social science has concerned itself greatly with the ways in which power and knowledge are hopelessly entwined with one another. Censorship of whatever type is thus an affirmation that rational consensus, and thus truth, is impossible in the face of force.

Concluding thoughts

As the Internet grows by leaps and bounds—the vast bulk of users worldwide began after 2000—its social applications and implications have risen proportionately. Despite the hyperbole exaggerating the Internet's capacity to effect social change, the global diffusion of the Internet has created a growing challenge for many authoritarian regimes and greatly enabled the growth and effectiveness of global civil society. Email petitions, cyberprotests, calls for action, advocacy of various marginalized political causes, and the blogosphere have become an integral part of political action, allowing local social movements to "jump scale" by reaching national and global audiences (Adams 1996). In response, government censorship, ranging from relatively mild steps such as anti-pornography measures to the arrest and execution of cyberdissidents, has become an inescapable dimension of the geographies of cyberspace. One-quarter of the world's netizens live under the harshest forms of censorship, and in most countries self-censorship accomplishes what governments have not.

The information technology revolution, however, has also brought with it promise of economic growth and improved productivity. Many governments, therefore, are caught in a conundrum, wishing to encourage the growth of information technology sectors on the one hand but fearful of its political repercussions on the other. In attempting to manage Internet access and content, states must take care not to alienate investors, tourists, entrepreneurs, and software developers. For some states, such as Myanmar or North Korea, such concerns are irrelevant. But most governments seek to appropriate the economic benefits of information technology without paying the political costs of enhanced democracy. The strategies used to negotiate this predicament are contingent and reflective of a wide constellation of political, economic, and cultural circumstances; thus, censorship and its resistance are geographically specific. Contrary to early utopian predictions, the growth of the much vaulted global "information society" will not necessarily lead to greater democracy worldwide, but, in a more sober view, to enhanced avenues for civil discourse. The Habermasian critique addresses the moral dimensions of this issue from the standpoint of contemporary social philosophy.

A last point concerns electronic governance, or e-government, which takes a variety of forms, ranging from simple broadcasting of information to integration (i.e., allowing user input), in which network integration minimizes duplication of efforts. E-government allows, for example, for the digital collection of taxes, electronic voting, payment of utility bills, applications for permits, passports, and driver's licenses, on-line registration of companies and automobiles, access to census data, and reductions in waiting times in government bureaucracies. While such measures are relatively common in economically advanced countries, even many countries in the developing world have moved in this direction (Wagner et al. 2003). As ever larger domains of social life move on-line, the future is likely to see steady growth in e-government across the planet, leading to greater transparency and accountability in state actions. Clearly, strict censorship and enhanced e-government are incompatible goals. How different political regimes strive to implement such measures, yet still retain control over discourses they perceive to be threatening, will play out in fascinating and unexpected ways in the future.

References

Abbott, J. (2001). Democracy@internet.asia? The challenges to the emancipatory potential of the net: Lessons from China and Malaysia. *Third World Quarterly, 22*(1), 99–114.

Adams, P. (1996). Protest and the scale politics of telecommunications. *Political Geography, 15*(5), 19–441.

Africa ICT Policy Monitor. (2006). http://africa.rights.apc.org.

Ahmed, A. (2002). Pakistan's blasphemy laws: Words fail me. *The Washington Post*, May 19.

Anderson, J. (1997). Globalizing politics and religion in the Muslim world. *Journal of Electronic Publishing*, www.press.umich.edu/jep/archive/Anderson.html.

Anderson, J. (2003). New media, new publics: Reconfiguring the public sphere of Islam. *Social Research, 70*(3), 887–906.

Anderson, K. (2009). Net surveillance and filters are a reality for Europe, too. *The Guardian*, June 24. http://www.guardian.co.uk/technology/2009/jun/24/kevin-anderson-internet-filtering.

Arabic Network for Human Rights Information. (2004). The Internet in the Arab world: A new space of repression? http://www.hrinfo.net/en/reports/net2004/.

Bahgat, H. (2004). Egypt's virtual protection of morality. *Middle East Report, 230*, 22–25.

Barry, E. (2004). In Azerbaijan, a donkey suit leads to laughs, questions and possibly arrests. *New York Times*, July 15, 2009, p. A4.

BBC News Online. (2002). Bahrain blocks opposition websites. March 26. http://news.bbc.co.uk/1/low/world/middle_east/1895005.stm.

Bernstein, J. (1995). *Recovering ethical life: Jürgen Habermas and the future of critical theory*. New York, NY: Routledge.

Bi, J. (2001). The internet revolution in China: The significance for traditional forms of communist control. *International Journal, 56*(3), 421–441.

Brunn, S. (2000). Towards an understanding of the geopolitics of cyberspace: Learning, re-learning and un-learning. *Geopolitics, 5*(3), 144–149.

Burnett, P. (2005). Internet censorship on the rise in Africa? http://www.worldhunger.org/articles/06/africa/burnett.htm.

Cairncross, F. (1997). *The death of distance*. Boston, MA: Harvard Business School Press.

Calhoun, C. (1992). *Habermas and the public sphere*. Cambridge, MA: MIT Press.

Castells, M. (2001). *The internet galaxy*. Oxford: Oxford University Press.

Conway, M. (2007). Terrorism and internet governance: Core issues. http://www.unidir.ch/pdf/articles/pdf-art2644.pdf.

Cortés, M. (2000). Internet censorship around the world. http://www.isoc.org/inet2000/cdproceedings/8k/8k_4.htm.

Crampton, J. (2003). *The political mapping of cyberspace*. Edinburgh: Edinburgh University Press.

Crampton, J. (2007). The biopolitical justification for geosurveillance. *Geographical Review, 97*(3), 389–493.

Crovitz, G. (2010). China's web crackdown continues. *Wall Street Journal*, January 11. http://online.wsj.com/article/SB10001424052748703948504574649021577882240.html.

Cunningham, K. (2002). Factors influencing Jordan's information revolution: Implications for democracy. *Middle East Journal, 56*(2), 240–256.

Dann, D., & Haddow, N. (2008). Just doing business or doing just business? Google, Microsoft, Yahoo! and the business of censoring China's Internet. *Journal of Business Ethics, 79*(3), 219–234.

Deibert, R., Palfrey, J., Rohozinski, R., & Zittrain, J. (Eds.). (2008). *Access denied: The practice and policy of global internet filtering*. Cambridge, MA: MIT Press.

Diker, D. (2003). Should Israel now send a new message to the Arab world? *Jerusalem Letter*, May 1. http://www.jcpa.org/jl/vp497.htm.

Dobson, J., & Fisher, P. (2007). The panopticon's changing geography. *Geographical Review, 97*(3), 307–323.

Dodge, M., & Kitchin, R. (2000). *Mapping cyberspace*. London: Routledge.

Dunn, M. (2000). The information revolution and the Middle East: An overview of the early literature. *Middle East Journal, 54*(3), 465–476.

Elmer-Dewitt, P., Jackson, D., & King, M. (1993). First nation in cyberspace. *Time*, December 6, pp. 62–64.

Eriksson, J., & Giacomello, G. (2009). Who controls what, and under what conditions? *International Studies Review, 11*(1), 206–210.

Eurasianet.org. (2007). In *Turkemenistan*. Internet access comes with soldiers. http://www.eurasianet.org/departments/insight/articles/eav030807.shtml.

Fandy, M. (1999). Cyberresistance: Saudi opposition between globalization and localization. *Comparative Studies in Society and History, 41*, 124–147.

Froomkin, A. (2003). Habermas@Discourse.net. Toward a critical theory of cyberspace. *Harvard Law Review, 116*(3), 740–873.

Gauch, S. (2001). Effects of Arab censorship blunted by the Internet. *Christian Science Monitor*, January 29, p. 1.

Gellman, B. (2005). The FBI's secret scrutiny: In *Hunt for terrorists, bureau examines records of ordinary Americans*. *Washington Post*, November 6, p. A1.

Ghareeb, E. (2000). New media and the information revolution in the Arab world: An assessment. *Middle East Journal, 54*(3), 395–418.

Ghattas, K. (2002). Surfing the net in Iraq. BBC News, May 1. http://news.bbc.co.uk/1/hi/world/middle_east/1959481.stm.

Goldsmith, J. (1998). Against cyberanarchy. *University of Chicago Law Review, 1199*(fall), 1217–1222.

Goldsmith, J., & Wu, T. (2006). *Who controls the internet? Illusion of a borderless world*. New York, NY: Oxford University Press.

Habermas, J. (1979). *Communication and the evolution of society*. Boston, MA: Beacon Press.

Habermas, J. (1989). *The structural transformation of the public sphere: An inquiry into a category of bourgeois society*. Oxford: Blackwell.

Hachigian, N. (2001). China's cyber-strategy. *Foreign Affairs, 80*(2), 118–133.

Hachigian, N. (2002). The internet and power in one-party East Asian states. *Washington Quarterly, 25*(3), 41–58.

Hajiyev, Y. (2006). Azerbaijan. http://ec.europa.eu/information_society/activities/internationalrel/docs/pi_study_rus_ukr_arm_azerb_bel_geor_kaz_mold/5_azerbaijan.pdf.

Harwit, E., & Clark, D. (2001). Shaping the internet in China: Evolution of political control over network infrastructure and political content. *Asian Survey, 41*(3), 377–408.

Hohendahl, P. (1979). Critical theory, public sphere and culture: Habermas and his critics. *New German Critique, 16*(winter), 89–118.

Human Rights Watch. (2002). Human Rights Watch: World report 2001, Vietnam. http://www.hrw.org/wr2k/asia/Vietnam.html.

Inglehart, R., & Welzel, C. (2005). *Modernization, cultural change, and democracy: The human development sequence*. Cambridge: Cambridge University Press.

International Censorship Explorer. (2006). Vietnam strikes back. http://ice.citizenlab.org/?p=150.

James, R. (2009). A brief history of Chinese internet censorship. *Time*, March 18. http://www.time.com/time/world/article/0,8599,1885961,00.html.

Kahn, J. (2002). China has world's tightest internet censorship, study finds. *New York Times*, December 4, p. 1.

Kalathil, S., & Boas, T. (2001). The Internet and state control in authoritarian regimes: China, Cuba, and the counterrevolution. *Carnegie Endowment global policy program work*, paper no. 21. Washington, DC: Carnegie Endowment for International Peace.

Kalathil, S., & Boas, T. (2003). *Open networks, closed regimes: The impact of the internet on authoritarian rule*. Washington, DC: Carnegie Endowment for International Peace.

Katyal, N. (2001). Criminal law in cyberspace. *University of Pennsylvania Law Review, 1003*, 1100.

Kellerman, A. (2002). *The internet on Earth: A geography of information*. Hoboken, NJ: Wiley.

Kellner, D. (1979). TV, ideology, and emancipatory popular culture. *Socialist Review, 45*(May–June), 13–53.

Kellner, D. (1990). *Television and the crisis of democracy*. Boulder, CO: Westview Press.

Kreimer, S. (2001). Technologies of protest: Insurgent social movements and the First Amendment in the era of the Internet. *University of Pennsylvania Law Review, 150*(1), 119–171.

Kreimer, S. (2006). Censorship by proxy: The First Amendment, internet intermediaries, and the problem of the weakest link. *University of Pennsylvania Law Review, 155*(11), 11–101.

LaFraniere, S. (2009). Censors put tighter grip on internet in China. *New York Times*, December 18, p. A. 14.

Lake, E. (2009). Hacking the regime. *The New Republic*, September 3. http://www.tnr.com/article/politics/hacking-the-regime.

Lee, J. (2001). Companies compete to provide Saudi internet veil. *New York Times*, November 19, p. A1.

Luhmann, N. (1996). Quod omnes tangit: Remarks on Jurgen Habermas's legal theory. *Cardoso Law Review, 17*(4–5), 883–900.

MacFarquhar, M. (2006). In tiny Arab state, Internet is tool to fight rulers. *New York Times*, January 15, p. A1, 11.

MacKinnon, R. (2008). Flatter world and thicker walls? Blogs, censorship and civic discourse in China. *Public Choice, 134*, 31–46.

MacKinnon, R. (2009). China's censorship 2.0: How companies censor bloggers. *First Monday*, 14(2). http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2378/2089.

Malecki, E., & Moriset, B. (2008). *The digital economy: Business organisation, production processes, and regional developments*. London: Routledge.

McLaughlin, W. (2005). The use of the Internet for political action by non-state dissident actors in the Middle East. *FirstMonday*. http://www.firstmonday.org/issues/issue8_11/mclaughlin.

Murdoch, S., & Anderson, R. (2008). Tools and technology of internet filtering. In R. Deibert, J. Palfrey, R. Rohozinksi, & J. Zittrain (Eds.), *Access denied: The practice and policy of global internet filtering* (pp. 57–72). Cambridge, MA: MIT Press.

O'Brien, R. (1992). *Global financial integration: The end of geography*. New York, NY: Council on Foreign Relations Press.

OpenNet Initiative (2004). Internet filtering in Saudi Arabia in 2004. http://opennet.net/studies/saudi. Accessed 18 Nov 2010.

OpenNet Initiative (2005). Internet filtering in China 2004–2005. http://opennetinitiative.net/studies/china.

OpenNet Initiative (2006). Singapore. http://opennet.net/research/profiles/Singapore.

OpenNet Initiative (2007). Commonwealth of Independent States. http://opennet.net/research/regions/cis.

OpenNet Initiative (2009a). Internet filtering in Iran. http://opennet.net/sites/opennet.net/files/ONI_Iran_2009.pdf.

OpenNet Initiative (2009b). Internet filtering in Sudan. http://opennet.net/sites/opennet.net/files/ONI_Sudan_2009.pdf.

Paltemaa, V., & Vuori, J. (2009). Regime transition and the Chinese politics of technology: From mass science to the controlled internet. *Asian Journal of Political Science, 17*(1), 1–23.

Parry, N. (1997). The past and future of information technology in Palestine. www.nigelparry.com/mideastinternet/unitednationspaper.html.

Pierre, A. (2000). Vietnam's contradictions. *Foreign Affairs, 79*(6), 69–86.

Poster, M. (1997). Cyberdemocracy: Internet and the public sphere. In D. Porter (Ed.), *Internet culture* (pp. 202–214). London: Routledge.

Privacy International. (2003). Silenced—Costa Rica. http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-103752.

Quirk, M. (2006). The web police. *Atlantic Monthly*, May. http://www.theatlantic.com/magazine/archive/2006/05/the-web-police/4818.

Reporters Without Borders. (2004). *Pakistan annual report 2004*. http://www.rsf.org/article.php3?id_article=10794.

Reporters Without Borders. (2008). Belarus. http://www.rsf.org/article.php3?id_article=25496. 2008.

Reporters Without Borders. (2009). Internet enemies. http://www.rsf.org/en-ennemi26106-Turkmenistan.html.

Rhoads, C., & Chao, L. (2009). Iran's web spying aided by Western technology. *The Wall Street Journal*, June 22. http://online.wsj.com/article/SB124562668777335653.html.

Rodan, G. (2000). Singapore information lockdown: Business as usual. In L. Williams & R. Rich (Eds.), *Losing control: Freedom of the press in Asia* (pp. 66–81). Canberra: Asia Pacific Press.

Sayare, S. (2009). As web challenges French leaders, they push back. *New York Times*, December 13, p. 26.

Slane, A. (2007). Democracy, social space, and the internet. *University of Toronto Law Journal, 57*(1), 81–104.

Steinberg, P., & McDowell, S. (2003). Mutiny on the bandwidth: the semiotics of statehood in the internet domain name registries of Pitcairn Island and Niue. *New Media & Society, 5*(1), 47–67.

Stelter, B., & Stone, B. (2009). Web pries lid of Iranian censorship. *New York Times*, June 22, p. A1. http://www.nytimes.com/2009/06/23/world/middleeast/23censor.html.

Stone, B., & Barboza, D. (2010). Scaling the digital wall in China. *New York Times*, January 16, p. B1.

Taylor, P. (1994). The state as container: Territoriality in the modern world-system. *Progress in Human Geography, 18*(2), 151–162.

Teitelbaum, J. (2002). Dueling for 'Da'Wa': State vs. society on the Saudi internet. *Middle East Journal, 56*(2), 222–239.

Tilly, C. (2007). *Democracy*. Cambridge, MA: Cambridge University Press.

Troianovski, A., & Finn, P. (2007). Kremlin seeks to extend its reach in cyberspace. *The Washington Post*, October 28, p. 1. http://www.washingtonpost.com/wp-dyn/content/article/2007/10/27/AR2007102701384_pf.html.

Villeneuve, N. (2006). The filtering matrix: Integrated mechanisms of information control and the demarcation of borders in cyberspace. *First Monday, 11*(1–2). http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1307.

Wagner, C., Cheung, K., Lee, F., & Ip, R. (2003). Enhancing e-government in developing countries: Managing knowledge through virtual communities. *Electronic Journal on Information Systems in Developing Countries, 14*(4), 1–20. http://www.ejisdc.org.

Warf, B. (2009a). Diverse spatialities of the Latin American and Caribbean internet. *Journal of Latin American Geography, 8*(2), 125–146.

Warf, B. (2009b). The rapidly evolving geographies of the Eurasian internet. *Eurasian Geography and Economics, 50*(5), 564–580.

Warf, B., & Grimes, J. (1997). Counterhegemonic discourses and the internet. *Geographical Review, 87*(2), 259–274.

Warf, B., & Vincent, P. (2007). Multiple geographies of the Arab internet. *Area, 39*(1), 83–96.

Wines, M. (2010). China's censors tackle and trip over the Internet. *New York Times*, April 8, p. 1, 4.

Wriston, W. (1997). Bits, bytes, and diplomacy. *Foreign Affairs, 76*(5), 172–182.

Yang, G. (2003). The co-evolution of the internet and civil society in China. *Asian Survey, 43*(3), 405–422.

Zittrain, J., & Palfrey, J. (2008). Internet filtering: The politics and mechanisms of control. In R. Deibert, J. Palfrey, R. Rohozinksi, & J. Zittrain (Eds.), *Access denied: The practice and policy of global internet filtering* (pp. 29–56). Cambridge, MA: MIT Press.

Zook, M. (2003). Underground globalization: Mapping the space of flows of the Internet adult industry. *Environment and Planning A, 35*(7), 1261–1286.

Zook, M. (2005a). *The geography of the Internet industry*. Oxford: Wiley-Blackwell.

Zook, M. (2005b). The geography of the internet. *Annual Review of Information Science and Technology, 40*(1), 53–78.

Zook, M., & Graham, M. (2007). The creative reconstruction of the Internet: Google and the privatization of cyberspace and DigiPlace. *Geoforum, 38*(6), 1322–1343.