JOURNAL OF
DEMOCRACY

April 2011, Volume 22, Number 2 $12.00

Paradoxes of the New Authoritarianism
Ivan Krastev

Brazil After Lula
Amaury de Souza

The Freedom House Survey for 2010
Arch Puddington

Eric Kramon & Daniel Posner on Kenya's New Constitution
Neil DeVotta on Sri Lanka
Ellen Lust & Sami Hourani on Jordan's Elections
Greg Michener on FOI Laws
Omar Encarnación on Gay Rights in Latin America
Roukaya Kasenally on Mauritius

Liberation Technology?
Rebecca MacKinnon ▪ *Xiao Qiang* ▪ *Evgeny Morozov*

WHITHER INTERNET CONTROL?

Evgeny Morozov

Evgeny Morozov *is a Bernard L. Schwartz Senior Fellow at the New America Foundation and a contributing editor of* Foreign Policy, *where he runs the "Net Effect" blog* (http://neteffect.foreignpolicy.com). *He is the author of* The Net Delusion: The Dark Side of Internet Freedom *(2011).*

Leading liberal democracies such as the United States have begun promoting "Internet freedom" and, by extension, opposing "Internet control." But what exactly is this control, and how best may it be combated? As a category, it is broad, encompassing both censorship (which violates the right to free expression) and surveillance (which violates the right to privacy). This dual character of control explains why it is often so hard to assess innovations such as social networking in the abstract: They work in favor of freedom of expression by making it easier for us to express ourselves, but at the same time they also tend to work in favor of surveillance by making more of our private information public.

In addition to its ability to manifest itself as both censorship and surveillance, "Internet control" has a technological dimension and a sociopolitical dimension that often overlap in practice even though they are analytically distinct from each other. A good example of the technological control would be a national-level scheme in which government-sanctioned Internet filters automatically banned access to all sites whose URLs contained certain sensitive keywords. A good example of sociopolitical control would be a law that treated blogging platforms such as WordPress or LiveJournal as mass-media organs and made them screen all user-submitted online content prior to publication. In the former case, a government would be using technology to chill the freedom of expression directly; in the latter case, the sought-after effect would be the same, but would be indirect and mediated through the power of law rather than sought through the direct application of technology alone.

Most talk of "liberation technologies" as ways of weakening "Internet control" turns out to be about the technological rather than the sociopolitical dimension. But what if success in that area is met with larger and more sophisticated efforts at exerting sociopolitical control? Scholars still know little about the factors that influence the dynamics and the distribution of the two kinds of control. As technological methods lose efficacy, sociopolitical methods could simply overtake them: An authoritarian government might find it harder to censor blogs, but still rather easy to jail bloggers. Indeed, if censorship becomes infeasible, imprisonment may become inevitable.

Thus, if the technological dimension of Internet control were one day to be totally eliminated, the upshot could be a set of social and political barriers to freedom of expression that might on balance be worse—not least because "liberation technologies" would be powerless to overcome them. It would be a cruelly paradoxical outcome indeed should liberation technology's very success spur the creation of a sociopolitical environment in which there would be nothing for technology to "liberate."

But suppose that we could set such concerns aside. What are the ways to minimize the technological dimension of Internet censorship? On first sight, this looks like a mere engineering challenge. It may even be tempting to reframe this question as follows: Given what we know about how the Internet works, what can we do to help bypass such technological restrictions as authoritarian governments might put in place?

The proliferation of numerous censorship-circumvention technologies over the last decade suggests that even the most sophisticated Internet-filtering schemes are not immune to the ingenuity of the engineering community. The porousness and decentralization that are basic to the Internet's design make it hard to come up with a firewall that works 100 percent of the time. Unless they are forced to deal with a national Intranet featuring a fixed number of government-run websites, those with the requisite know-how will always be able to circumvent government bans by connecting to third-party computers abroad and using them to browse the uncensored Internet.

It might seem, then, that the only outstanding problems are technological in nature: making sure that tools deliver on their promises—including promises to keep their users safely undetected and anonymous—and that they remain cheap and easy to use. It might also seem that money and engineering talent would be all that is needed to solve such problems. For example, Shiyu Zhou, the founder of a Falun Gong technology group that designs and distributes software for accessing sites banned by the Chinese government, says that "the entire battle over the Internet has boiled down to a battle over resources."[1]

This is a misleading view. The sociopolitical environment will always affect the scope and intensity of technology-based efforts to get around Internet controls. Some of the constraints on the use and proliferation of such tools are anything but technological in origin, and are not traceable to resource scarcity. A tool that can help dissidents in authoritarian states to access websites that authoritarian governments have banned may also allow terrorists or pedophiles to access online resources that democratic governments have placed off-limits in keeping with their own laws and systems of due process. Similarly, any tool that allows dissidents to hide their digital doings from the prying eyes of an unfree regime's secret police may also be used by criminals to evade the legal monitoring efforts of legitimate law-enforcement agencies in liberal-democratic states. Technology and engineering, in other words, do not operate in a vacuum. The social and political environment will inevitably have much to do with determining how, where, how quickly and widely, and to what ends they are brought to bear, as well as what the public thinks about them and their uses.

Considering that many such tools are developed by activists (often working as volunteers) who have a stake in many different projects—not all of them viewed altogether favorably by governments or publics—it is unsurprising that the going can be tough. When we consider that at least one of the key people doing work on Tor—a much-celebrated system of servers and software that is designed to ensure users' online anonymity and that enjoys U.S.-government funding—has also collaborated with WikiLeaks,[2] we are not shocked to learn that the U.S. government may be having some second thoughts about this particular surveillance-evading tool. Although this has not so far had a tangible impact on the level of support that the U.S. government has been giving to Tor, that may change in the future—especially as competing projects acquire powerful backers and lobbyists eager to defend their cause in Washington.

At a minimum, any policy initiative that aims to address the technological dimension of "Internet control" needs to find a way to model the sociopolitical environment—including the tricky human element—in which such tools are designed and distributed. At this point, it is hard to predict how Western governments will react if Tor solves its functionality problems and suddenly becomes more user-friendly and faster. Nor do we know how upcoming legislation aimed at forcing Internet companies to create "backdoors" through which U.S. law-enforcement and intelligence agencies can secretly access online services such as Skype and Gmail may impede the wider deployment of a tool such as Tor, which would probably help to keep these "backdoors" closed.[3] This is not only, or even mainly, a battle for resources; there are many unresolved political issues involved here. The U.S. State Department, as Hillary Clinton announced in a widely publicized January 2010 speech,[4] may back an Internet-freedom agenda, but can the same be said for all arms of the U.S. government?

One possible solution would be to design specialized tools that would tackle Internet censorship only in particular countries such as China, Iran, or Kazakhstan. Such tools would not abet the terrorists and criminals that worry U.S. authorities—unless, of course, the bad actors managed to set up shop in one or more of those countries. Another disadvantage is that any tool with a particular geographic focus will end up becoming far more politicized than would any generic solution such as Tor.

The focus on abetting censorship circumvention in a particular country may only result in the government aiming sharper scrutiny at such tools and those who wield them. A case in point is Haystack, an anticensorship tool that U.S. "hacktivists" devised for Iranian dissidents to use in the wake of their country's 2009 "Green Wave" postelection protests. Since Haystack's users were presumed to be dissidents downloading Human Rights Watch reports rather than illegal online pornography (a common use of general-purpose tools such as Tor), the Iranian government had a particularly strong incentive to monitor them. (Haystack shut down in September 2010 after proving to be less reliable than its inventors had claimed.)

The further segmentation of this market, with the appearance of tools specific to Fiji and Tajikistan, for instance, would also make it hard to vouch for the security of each tool. Ideally, any effort to create a new country-specific tool would conform to appropriate standards and procedures, so that its technical merits could be independently assessed by third parties and subjected to peer review. The Haystack debacle suggests the pitfalls that lie in wait if such rigorous protocols are ignored.

The Sociopolitical Dimension

Internet-filtering is just one of the many options available to governments. It is also the one that is easiest to document. Moreover, it lends itself nicely to straightforward assessments by Freedom House, the OpenNet Initiative, and Herdict Web, a Harvard-based initiative that seeks input from Internet users worldwide in order to "crowdsource" real-time data regarding Internet control. Because of this relative transparency, and because being known for Web-filtering looks bad (few countries want to be spoken of in the same sentence with phrases such as the "Great Firewall of China"), governments are now experimenting with more sophisticated ways of exerting control that are harder to detect and document. These include:

Distributed denial-of-service attacks. Although reliable statistical data is scarce, anecdotal evidence suggests that politically motivated "distributed denial-of-service" (DDoS) attacks are on the rise.[5] These target individuals or entire organizations by flooding their websites with crippling volumes of artificially generated Internet traffic. This effectively shuts down the targeted site for a time and denies access to legitimate users.

The publishers of a site that comes under DDoS attack must not only scramble for ways to keep content available (especially if the assault comes at a sensitive moment such as during a period of postelection protests), but must also cope with the anger of the Internet-hosting companies that are often the ones left dealing with the consequences of such attacks. Repeated DDoS attacks on a site may eventually make it "unhostable"—no hosting company will touch it for fear of the costly cyber-assaults that it will draw.

For content producers, DDoS attacks could have far worse consequences than would attempts to filter their websites in a given jurisdiction. First, a successful DDoS attack makes content unavailable anywhere and everywhere, not just in this or that place with a Web-filtering system in place. Second, DDoS assaults put heavy psychological pressure on content producers, suddenly forcing them to worry about all sorts of institutional issues such as the future of their relationship with their Internet-hosting company, the debilitating effect that the unavailability of the site may have on its online community, and the like.

From the perspective of those ordering the attacks—it is a fair assumption that in some cases this means authoritarian governments—DDoS assaults beat censorship by virtue of being far harder to trace to their source. Indeed, it can sometimes be hard to say if a DDoS attack has taken place at all. Websites go down all the time for a variety of reasons: legitimate spikes in traffic, server failures, power outages, and numerous other causes that have nothing to do with cyber-attacks. Among other things, this means that there are still no reliable ways to gauge the frequency and intensity of DDoS attacks. They might be a worse threat to global freedom of expression than we currently realize.

Unfortunately, things will probably get worse, as there has already emerged a black market in DDoS attacks (you can go to eBay to "rent" the ability to launch one). This seems to be happening mainly because DDoS attacks can also be used to target businesses for the purposes of cyber-extortion. Yet a recent survey by the computer-security firm Symantec indicates that 53 percent of critical-infrastructure providers report experiencing what they perceive as politically motivated cyber-attacks against their networks. Those who reported having been attacked further reported an average of ten incidents over the preceding five years, with an average total cost across all five years of US$850,000.[6]

Deliberate erosion of online communities' social capital. Among the things about the Internet that make authoritarian rulers uneasy are its powers to boost civic associations of all kinds and to connect previously unconnected people and organizations with one another. Governments fearful of Internet-enabled "connectivity" have learned that censorship is too blunt an instrument to be their best weapon against communities that begin online and remain outside the state's control. Censorship can be too easily circumvented and it can backfire if the presence of a threat from the state ends up strengthening rather than weakening a target community's internal bonds. There are numerous ways to weaken community ties more effectively.

One option may be the launching of DDoS attacks as a means of shutting sites down periodically and, worse, forcing them to find a way to pay for better hosting services. Even simpler methods may include trolling or dispatching new members to create artificial splits within the community as well as intentionally provoking community administrators to take harsh and unpopular measures. These last two stratagems are labor-intensive and costly ways to hamstring and manipulate online communities, but they are more likely to prove effective than censorship.

The Chinese government has become notorious for its "fifty-centers"—people who are paid piece rates to post progovernment comments on message boards and other widely read online forums. Their work is plainly meant to influence the intellectual dynamics of online communities and sow doubts within their ranks. Vladimir Putin's Russia, likewise, has plenty of Kremlin-friendly youth movements whose members will defend the government and its policies online, including on the websites of critics.

The "nationalization" of cyberspace. In the months since Hillary Clinton's speech on Internet freedom, many governments seem to have woken up to the possibility that the United States might be keen to exploit its existing dominance of cyberspace in order to promote a certain political agenda. Whether or not their concerns are justified, the governments of China, Iran, Russia, and many other countries have suddenly realized the degree to which their own citizens are dependent on Internet services offered by U.S. companies. Editorials in their state-owned newspapers increasingly speak of "informational sovereignty," by which they mean the ability of their digital economies to function independent of foreign service providers.

In keeping with this, these governments have begun bolstering their domestic Internet enterprises at the expense of foreign competitors. Turkey made the first move into this space with its late-2009 launch of the Anabena project, which is meant to create a national search engine that better caters to "Turkish sensibilities," with a national e-mail system to follow. Iran quickly followed suit, banning Gmail in February 2010 and announcing its own national e-mail system. Later in the same year, Russia announced plans similar to Turkey's, including the establishment of a national e-mail service and the allocation of $100 million to explore the feasibility of a national search engine.

It would not be surprising to see the Chinese, Russian, and other governments declare that Internet-search services are a "strategic industry" like energy and transport and move to block foreign companies in this area. If the impression that Twitter and Facebook can facilitate political revolutions continues to gain currency, social-networking and microblogging services may end up in the "strategic" category as well. This will almost certainly be bad news for users, since local alternatives to Google, Facebook, and Twitter are likely to have more restrictive attitudes toward freedom of expression and privacy. Even if we see no new national search engines, existing local competitors to Google (China's Baidu and Russia's Yandex, for instance) may grow stronger as a result.

The outsourcing of Internet control to third parties. One way for governments to avoid direct blame for exercising more Internet control is to delegate the task to intermediaries. At a minimum, this will involve making Internet companies that offer social-networking sites, blogging platforms, or search engines take on a larger self-policing role by holding them accountable for any content that their users post or (in the case of search engines) index and make available.

Being able to force companies to police the Web according to state-dictated guidelines is a dream come true for any government. The companies must bear all the costs, do all the dirty work, and absorb the users' ire. Companies also are more likely to catch unruly content, as they are more decentralized and know their own online communities better than do the state's censors.

It would be a mistake to think that only authoritarian governments harbor such ambitions. The Italian government has been holding YouTube accountable for the videos that are published on its site. This creates an enabling environment in which authoritarian governments can justify their actions by referring to similar developments in democratic societies.

Other ways in which third parties abet Internet control are appearing as well. Thailand's strict laws against *lèse majesté* ban the publication of anything (even a Twitter post) that may offend the country's royal family. When the Thai blogosphere's rapid expansion began outstripping the authorities' monitoring capacities, a member of parliament proposed a solution in early 2009. A site called ProtectTheKing.net was set up so that Thai users could submit links to any website that they deemed offensive to the monarchy. According to the BBC, the government blocked five-thousand submitted links in the first twenty-four hours. Not surprisingly, the site's creators "forgot" to provide a way in which to complain about sites that were blocked in error.[7]

Similarly, Saudi Arabia allows its citizens to report to the Communications and Information Technology Commission any links that they find offensive; citizens do so at an average rate of about 1,200 times per day. This allows the Saudi government to achieve a certain efficiency in the censorship process. According to *Business Week,* in 2008 the Commission's censorship wing employed only 25 people, although many of them were graduates of top Western universities such as Harvard and Carnegie Mellon.[8] But many similar efforts are also emerging and flourishing organically, without any apparent state involvement. Thus, a well-coordinated group of two-hundred culturally conservative volunteers that calls itself "Saudi Flagger" regularly monitors all Saudi Arabia–related videos uploaded to YouTube. Their practice is to complain *en masse* about any videos that they do not like—mostly these contain criticisms of Islam or Saudi rulers—by "flagging" them for YouTube's administrators as inappropriate and misleading.[9] A member, Mazen Ali Ali, described this in 2009 as "perform[ing] our duty towards our religion and homeland."[10]

Private-sector innovations. The Internet-control activities of secret-police officials in authoritarian states are increasingly getting a boost from breakthroughs in data analysis that the Web itself is making cheaper to obtain. It is not only text-messaging traffic that is becoming easier to search, organize, and act on: Video footage is moving in that direction as well, thus paving the way for even more video surveillance. This explains why the Chinese government keeps installing video cameras in its most troubling cities. Not only do such cameras remind passers-by about the panopticon that they inhabit, they also supply the secret police with useful clues. In mid-2010, there were 47,000 cameras scanning Urumqi, the capital of China's restive Xinjiang Province, and that number was projected to rise to 60,000 by the end of the year.[11]

Such an expansion of video surveillance could not have happened without the involvement of Western partners. Researchers at UCLA, funded in part by the Chinese government, have managed to build surveillance software that can automatically annotate and comment on what it sees, generating text files that can later be searched by humans, obviating the need to watch hours of video footage in search of one particular frame.[12] (To make that possible, the researchers had to recruit twenty graduates of local art colleges in China to annotate and classify a library of more than two-million images.) Such automated systems are crucial in order for video surveillance to be massively "scaled up" in a useful way, since it makes sense to add new cameras only if their footage can be rapidly indexed and searched.

The maddening pace of innovation in data analysis is poised to make surveillance far more sophisticated, with new features that seem straight out of science fiction. Digital surveillance will receive a significant boost as face-recognition techniques improve and enter the consumer market. The trade in face-recognition technologies is so lucrative that even giants such as Google cannot resist getting into the game as they feel the growing pressure from smaller players such as Face.com, a popular tool that allows users to find and automatically annotate unique faces as these appear throughout their photo collections. In 2009, Face.com launched a Facebook application that first asks users to identify a Facebook friend in a photo and then proceeds to search the entire social-networking site for other pictures in which that friend appears. By early 2010, the company was boasting of having scanned nine-billion pictures and identified 52-million individuals.

Imagine censorship systems that are as detailed and as fine-tuned to their "users" (targets) as the behavioral ads that we now see every day.

Applications go far beyond finding photos of one's friends on Facebook. Imagine advanced face-recognition technology in the hands of the Iranian Revolutionary Guards as they seek to ferret out the identities of people photographed during Tehran street protests. That said, governments had been using face-recognition technologies (the legitimate law-enforcement applications are obvious) for some time before these tools became commercially viable. What is most likely to happen in the case of Iran is that widely accessible face-recognition technologies will empower various solo agents, cyber-vigilantes who may not be on the payroll of the Islamic Republic, but who would like to help its cause. Just as Thai royalists surf the Web in search of sites criticizing the monarchy or progovernment Chinese go on the lookout for problematic blog posts, so we can predict that Islamist hard-liners in Iran will be checking photos of antigovernment protests against those in the massive commercial photo banks, populated by photos and names harvested from social-networking sites, that are sure to pop up, not always legally, once face-recognition technology goes fully mainstream. The cyber-vigilantes may then continue stalking the dissidents, launch DDoS attacks against their blogs, or simply report them to authorities.

Search engines capable of finding photos that contain a given face anywhere on the Internet are not far off. For example, SAPIR, an ambitious project funded by the European Union, seeks to create an audiovisual search engine that would automatically analyze a photo, video, or sound recording; extract certain features to identify it; and use these unique identifiers to search for similar content on the Web. An antigovernment chant recorded on the streets of Tehran may soon be broken down into individual voices, which in turn can then be compared to a universe of all possible voices that exist on amateur videos posted on YouTube.

Or consider Recognizr, the cutting-edge smartphone application developed by two Swedish software firms that allows anyone to point their mobile phone at a stranger and immediately query the Internet about what is known about that person (or, to be more exact, about that person's face). Its developers are the first to point to the tremendous privacy implications of their invention, promising that strict controls would eventually be built into the system.[13] Nevertheless, it is hard to believe that once the innovation genie is out of the bottle, no similar rogue applications would be available for purchase and download elsewhere.

The rise of online "publicness." If there is a clear theme to much of the Internet innovation of the last decade, it is that being open to sharing one's personal information can carry big benefits. More and more of our Internet experience is customized: Google arranges our search results in part based on what we have searched for in the past, while our Facebook identity can now "travel" with us to different sites (for example, those who visit music-streaming sites such as Pandora while logged into Facebook will be able to see what music their Facebook friends like and recommend).

When Jeff Jarvis, a professor of new media at the City University of New York and a leading Internet pundit, points out the benefits of publicness, he is right: There are, indeed, tremendous advantages to sharing our location, favorite music, or reading lists with the rest of the world.

The problem is that a world where such publicness can be turned against us is not so hard to imagine—and Internet pundits are usually the last to point out that all the digital advantages come at a price. Just as Amazon recommends books to us based on the books that we have already purchased, it is not hard to think of a censorship system that makes decisions based on the pages that we have visited and the kinds of people whom we list as our friends on social-networking sites. Might it be possible that in the not-so-distant future, a banker who peruses nothing online but Bloomberg News and the *Financial Times,* and who has only other bankers as her online friends, will be left alone to do anything she wants, even browse Wikipedia pages about human-rights violations? In contrast, a person of unknown occupation, who occasionally reads the *Financial Times* but who is also linked to five well-known political activists through Facebook and who has written blog comments containing words such as "democracy" and "freedom," will only be allowed to visit government-run websites (or, if he is an important intelligence target, he will be allowed to visit other sites, with his online activities closely monitored).

If online advertising is anything to judge by, such behavioral precision is not far away. Google already bases the ads that it shows us on our searches and the text of our e-mails; Facebook aspires to makes its ads much more fine-grained, taking into account what kind of content that we have previously "liked" on other sites and what our friends are "liking" and buying online. Imagine censorship systems that are as detailed and as fine-tuned to their "users" (targets) as the behavioral advertising that we now see every day. The only difference between the two is that one system learns everything about us in order to show us more relevant advertisements, while the other one learns everything about us in order to ban us from accessing relevant pages.

By paying so much attention to the most conventional and blandest of Internet-control methods (blocking access to particular URLs), we risk missing more basic shifts in the field. Internet censorship is poised to grow in depth, looking ever more thoroughly into what we do online and even offline. It will also grow in breadth, incorporating more and more information indicators before the "censor or do not censor" decision is made. Arguably, Green Dam Youth Escort—the Chinese software that made a lot of noise in mid-2009—was a poor implementation of an extremely powerful and dangerous concept: Green Dam analyzed the kinds of activities that the user was engaged in and made a decision about what to block or not based on such analysis rather than on a list of banned sites. A censorship scheme that manages to marry artificial intelligence and basic social-networking analysis would not only be extremely powerful; it would also help to limit the threat that censorship currently poses to economic development, thereby removing one of the major reasons that currently impels governments to avoid censorship.

The Future of Internet Control

The forces that are shaping the future of Internet control come from the realms of politics, society, and business. In the political realm, the U.S. government and its initiatives will be the biggest single force shaping the actions of other governments. Among the key developments to watch will be those concerning the future of the "Internet freedom" agenda and the evolution of the U.S. State Department's approach to the Internet. Hillary Clinton's speech was ambitious and idealistic, but also highly ambivalent. It is unclear how far the State Department is prepared to go in speaking up on behalf of bloggers who are jailed in countries whose rulers serve U.S. interests. Nor is it clear what the broader "Internet freedom" strategy is to be or which projects will receive priority funding. (Some vocal activists from the Middle East have already expressed concerns about the increased U.S.-government funding in this space.)

It remains to be seen whether "Internet freedom" means primarily defending the "freedom of the Internet" (that is, ensuring that governments and corporations avoid increasing censorship and surveillance) or promoting "freedom via the Internet" (that is, using the Internet and new media to facilitate anti-authoritarian movements such as Iran's "Green Wave"). Many governments around the world worry that the latter approach will predominate. Clinton's references to the role that technology played in the protests in Iran (and earlier in Moldova) did nothing to allay those fears.

The tight relationship between the State Department and U.S. technology companies may also prove problematic for both sides, and its future looks uncertain. As European governments and the UN take on "Internet freedom" issues, the State Department may find itself fighting on too many fronts, as those other governments and organizations would probably push to establish new treaties and laws, moves on which Washington is not very keen.

While the State Department promotes a vague notion of "Internet freedom" abroad, a number of domestic law-enforcement and intelligence agencies plus the Commerce Department are pushing for significant changes that amount to "Internet control" initiatives. Taken together, concerns in the areas of cyber-warfare and cyber-crime, electronic wiretapping, and Internet piracy and copyright reform may drive the U.S. government toward seeking significant sway over the Internet.

Whatever the democratic merits of such government initiatives, they will have the drawback of creating an enabling environment for authoritarian governments that are keen on passing similar measures, mostly for the purpose of curbing political freedom. In addition, concerns about cyber-crime may lead to the proliferation and legitimization of practices such as "deep packet inspection" (when network operators scrutinize the the contents of data packets that pass through their networks), driving down the costs for tools and services associated with it. This, in turn, may abet authoritarian governments (such as Iran's) that are already relying on technology supplied by European companies such as Nokia-Siemens to analyze the traffic passing through national networks.

It is possible that social attitudes toward "publicness" and privacy may become more cautious over time. So far, however, all the indicators are that Internet companies will continue to promote the practice of sharing more and more private data online. Short of U.S. and European policy makers passing new privacy-related legislation—though a few proposals are already in the pipeline—it is unrealistic to expect wider social and cultural shifts away from "publicness." In the business realm, some Internet service providers (ISPs) in Germany and the Netherlands are moving to make DDoS attacks costlier and more difficult to mount by informing any customer whose computer has become infected by a "botnet" (the mass of hijacked computers that makes a DoS attack "distributed"), by requiring corrective measures whenever a botnet infection is detected on a customer's machine, and by urging preventive measures to stop such infections before they start. Absent such interventions, the cost of DDoS attacks will continue to decline as botnets proliferate. Whether all ISPs will accept the potentially expensive task of fighting botnets remains to be seen, however.

Similarly, the software used for analyzing and "mining" data is becoming more powerful as businesses and intelligence agencies demand it. Whether the use of such software could be limited only to democratic states and business contexts remains to be seen; in the worst-case scenario, such tools may end up strengthening the surveillance apparatus of authoritarian states.

Authoritarian governments control the Internet through the combination of technological and sociopolitical means. It is unclear what the most potent combination of those types is; an Internet-control system that wields mainly the sociopolitical means may end up being more draconian than one that relies on technological means only. The great paradox is that the rising profile of "liberation technology" may push Internet-control efforts into nontechnological areas for which there is no easy technical "fix."

Both types of control are made possible by a number of social, political, and technological factors, many of which have their roots in the economies and government policies of democratic states. Any ambitious effort to promote "Internet freedom" should therefore begin by generating a typology of those factors as well as outlining some strategies for dealing with them. The U.S. government's current "Internet freedom" policy has yet to face this challenge, though it needs to do so.

NOTES

1. John Markoff, "Iranians and Others Outwit Net Censors," *New York Times,* 30 April 2009.

2. Virginia Heffernan, "Granting Anonymity," *New York Times Magazine,* 17 December 2010.

3. Charlie Savage, "U.S. Tries to Make It Easier to Wiretap the Internet," *New York Times,* 27 September 2010.

4. Hillary Rodham Clinton, "Remarks on Internet Freedom," 21 January 2010, available at *www.state.gov/secretary/rm/2010/01/135519.htm.*

5. Erica Naone, "Political Net Attacks Increase," *Technology Review,* 13 March 2009.

6. See "Politically Motivated Cyber Attacks," Help Net Security, 6 October 2010, available at *www.net-security.org/secworld.php?id=9957.*

7. "Thai Website to Protect the King," BBC News, 5 February 2009, available at *http://news.bbc.co.uk/2/hi/asia-pacific/7871748.stm.*

8. Peter Burrows, "Internet Censorship, Saudi Style," *Business Week,* 13 November 2008.

9. Soren Billing, "Saudi Campaign to Clean Up YouTube," ITP.net, 13 August 2009, available at *www.itp.net/564689-saudi-campaign-to-clean-up-youtube.*

10. Billing, "Saudi Campaign to Clean Up YouTube."

11. Michael Wines, "In Restive Chinese Area, Cameras Keep Watch," *New York Times,* 2 August 2010.

12. Tom Simonite, "Surveillance Software Knows What a Camera Sees," *Technology Review,* 1 June 2010.

13. Maija Palmer, "Face Recognition Software Gaining a Broader Canvas," *Financial Times,* 22 May 2010.