Technology Review
PUBLISHED BY MIT

May/June 2009

Dissent Made Safer

How anonymity technology could save free speech on the Internet.

By David Talbot

"Sokwanele" means "enough is enough" in a certain Bantu dialect. It is also the name of a Zimbabwean pro-democracy website whose bloggers last year published accounts of atrocities by Robert Mugabe's regime and posted Election Day updates describing voter intimidation and apparent ballot stuffing. You can visit Sokwanele's "terror album" and see photographs: of a hospitalized 70-year-old woman who'd been beaten and thrown on her cooking fire (she later died, the site says); of firebombed homes; of people with deep wounds carved into their backs. You can find detailed, frequently updated maps describing regional violence and other incidents. You will be confronted with gruesome news, starkly captioned: "Joshua Bakacheza's Body Found."

Because this horrific content is so readily available, it is easy to overlook the courage it took to produce it. The anonymous photographers and polling-station bloggers who uploaded the Sokwanele material remain very much in danger. In a place like Zimbabwe, where saying the wrong thing can get you killed or thrown in prison on treason charges, you take precautions: you're careful about whom you talk to; you're discreet when you enter a clinic to take pictures. And when you get to the point of putting your information on the Internet, you need protection from the possibility that your computer's digital address will be traced back to you. Maybe, at that point, you use Tor.

Tor is an open-source Internet anonymity system--one of several systems that encrypt data or hide the accompanying Internet address, and route the data to its final destination through intermediate computers called proxies. This combination of routing and encryption can mask a computer's actual location and circumvent government filters; to prying eyes, the Internet traffic seems to be coming from the proxies. At a time when global Internet access and social-networking technologies are surging, such tools are increasingly important to bloggers and other Web users living under repressive regimes. Without them, people in these countries might be unable to speak or read freely online *(see "Beating Surveillance and Censorship (http://www.technologyreview.com/computing/22427/page4/) ").*

Video (http://link.brightcove.com/services/player/bcpid263777539?bctid=19532032001)

Unlike most anonymity and circumvention technologies, Tor uses multiple proxies and encryption steps, providing extra security that is especially prized in areas where the risks are greatest. Paradoxically, that means it's impossible to confirm whether it's being used by the Zimbabwean bloggers. "Anyone who really needs Tor to speak anonymously isn't going to tell you they use Tor to speak anonymously," says Ethan Zuckerman, cofounder of Global Voices, an online platform and advocacy organization for bloggers around the world. "You can't tell if it's happening, and anyone who is actively evading something isn't going to talk about it." That said, the Sokwanele journalists "are extremely sophisticated and use a variety of encryption techniques to protect their identity," he says.

Anonymity aside, Internet users in dozens of countries--whether or not they are activist bloggers--often need to evade censorship by governments that block individual sites and even pages containing keywords relating to forbidden subjects. In 2006, the OpenNet Initiative--a research project based at Harvard and the Universities of Toronto, Oxford, and Cambridge that examines Internet censorship and surveillance--discovered some form of filtering in 25 of 46 nations tested, including China, Saudi Arabia, Iran, and Vietnam.

In a new and still-evolving study, OpenNet found that more than 36 countries are filtering one or more kinds of speech to varying degrees: political content, religious sites, pornography, even (in some Islamic nations) gambling sites. "Definitely, there is a growing norm around Internet content filtering," says Ronald Deibert, a University of Toronto political scientist who cofounded OpenNet. "It is a practice growing in scope, scale, and sophistication worldwide."

Tor can solve both problems; the same proxies that provide anonymous cover for people posting content also become portals for banned websites. When it officially launched five years ago, the Tor network consisted of 30 proxies on two continents; now it has 1,500 on five continents, and hundreds of thousands of active users. And its developers are trying to expand its reach, both abroad and in the United States, because digital barriers and privacy threats affect even the free world. In the United States, for example, libraries and employers often block content, and people's Web habits can be--and are--recorded for marketing purposes by Internet service providers (ISPs) and by the sites themselves. "The Internet is being carved up and filtered and surveilled," says Deibert. "The environment is being degraded. So it's up to citizens to build technologies to [counter these trends]. And that is where I see tools like Tor coming into play. It preserves the Internet as a forum for free information."

Neutral Nodes

The product of a small nonprofit organization with eight paid developers and a few dozen volunteer security professionals around the world, Tor takes advantage of the fact that Internet traffic consists of two-part packets. The first part contains data--pieces of a Web page you are viewing, or of the photo file or e-mail you are sending. The other consists of the Internet protocol (IP) address of the sending and receiving computer (plus other data, such as the size of the file). Tor uses the latter portion--the addressing information--to build a circuit of encrypted connections through relays on the network (*see "Dodging Spies, Data Miners, and Censors (http://www.technologyreview.com/computing/22427/page3/) " next page*). The requisite relays (which collectively serve as proxies) are operated on a volunteer basis at universities such as Boston University and a few corporations, and by computer-security professionals and free-speech advocates around the world. (Many Tor users also use existing technologies, such as HTTPS--a protocol for encrypting and decrypting a user's page requests and the pages that are returned--to protect the content they are sending and receiving.)

Tor, like the Internet itself, emerged from military research--in this case at the U.S. Naval Research Laboratory in Washington, which built a prototype in the mid-1990s. The military interest was clear: without a way to make Internet traffic anonymous, an agent's cover could be compromised the minute he or she visited .mil domains using the Internet connection of, say, a hotel. Even if the data were encrypted, anyone watching traffic over the hotel network could quickly figure out that the guest might be associated with the U.S. military. And the problem is hardly limited to hotel networks; IP addresses can be linked to physical locations by a variety of means (ISPs correlate such data with phone numbers, data miners can piece together clues from Internet traffic, and someone outside your house can confirm that you are the source of specific kinds of Internet traffic by "sniffing" data traveling over Wi-Fi). As a Tor presentation puts it, chillingly, what might an insurgent group pay to get a list of Baghdad IP addresses that get e-mail from a .gov or .mil account?

The navy project never emerged from the lab, but it attracted the interest of Roger Dingledine, a cryptographer concerned about a different aspect of Internet privacy: the way ISPs and websites amass databases on people's browsing and search history. In 2000, at a conference where he was presenting his MIT master's thesis on anonymous distributed data storage, he met a Naval Research Lab mathematician, Paul Syverson. The two men saw that tools for protecting military agents and tools for protecting Web surfers' privacy could be one and the same, and together they revived the project with funding from the Defense Advanced Research Projects Agency (DARPA) and the navy.

The first public version of Tor, which came out in 2003, was available for anyone who cared to install it. But it worked only on open-source operating systems, and using it required at least some technical knowledge. The Electronic Frontier Foundation, the digital civil-liberties organization, funded development of a version for Windows, and soon a wider variety of users emerged. "Originally one of my big reasons for working on Tor was to provide tools for people in the West--Americans and Europeans--to let them keep their information safe from corporations and other large organizations that generally aren't very good at keeping it to themselves," says Dingledine, now 32, who is Tor's project leader. But now, he says, some police agencies use Tor to make sure that an investigation of an online scam won't be compromised by tipping the scammer off to regular site visits from a police department's computers. And some companies, he says, use it to help them prevent competitors from figuring out, say, who is scouring their online product sheets.

It quickly became clear that this diversity was crucial to the technology's success. "It's not just safety in numbers; there is safety in variety," Dingledine says. "Even if there were 100,000 FBI agents using Tor, you would know what it's for: 'You are using the FBI's anonymity system.' Even from the very beginning, part of the fun and the challenge was to take all of these different groups out there who care about what Tor provides, and put them all into the same network." To help promote wider use, its developers made Tor far easier to install. And in 2006, they developed a new feature, the Torbutton, which allows Tor users to easily turn Tor on and off while they browse with the Firefox Web browser (turning it off speeds up Internet access but removes the protections).

Global spread

Syria is an all-purpose Internet repressor. It hunts down some bloggers; a Syrian named Tariq Biasi, for example, was recently sentenced to three years in prison for "dwindling the national feeling"; he allegedly posted a comment critical of the state's security service online. Beyond going after online critics, Syria also blocks many websites--including Facebook, YouTube, and Skype--from all Web users in the nation. I spoke about Syrian censorship with another blogger, Anas Qtiesh; he sat in an Internet café in Damascus as I messaged him from my living room. Qtiesh isn't worried that he'll be tracked down, because he tends to blog about pan-Arab politics, not about criticisms of the regime. But he wants access to more of the Internet than the government permits, so the Firefox browser on his laptop sports the Torbutton. Click the button, and presto--the same Internet that everyone in America sees. To access blocked sites, his computer negotiates a series of proxies, eventually connecting to an IP address somewhere else in the world. This intermediary fetches the blocked material. "Tor brings back the Internet," he wrote.

Qtiesh has plenty of company: Tor was always of interest abroad, but word of mouth and the introduction of the easy-to-use Torbutton have helped accelerate its global spread. Zuckerman has been actively promoting Tor through his Global Voices network. So have other advocates of online free speech in Asia, China, and Africa. And these efforts have been working. Wendy Seltzer, who teaches Internet law at American University and founded Chilling Effects, a project to combat legal threats against Internet users, saw that firsthand when she traveled to Guangzhou, China, for a blogger conference last year. China is generally acknowledged as the most sophisticated Internet filterer in the world; it employs a variety of techniques, including blocking IP addresses, domain names (the text name of a website, such as www.google.com), and even Web pages containing certain keywords (*Falun Gong*, for example). According to one report, Chinese security forces have arrested several hundred Internet users and bloggers in the past 10 years. Seltzer says that many bloggers she met in Guangzhou were using Tor. And when she went to an Internet café there, she reports, the computers were automatically configured to run the software.

In China, Tor is one weapon in a large arsenal. But in Mauritania, Tor appears to have single-handedly overwhelmed state censorship. Nasser Weddady is a Mauritanian-born son of a diplomat, now living in the Boston area. He is a civil-rights activist who seeks to call attention to the slavery still practiced in his native country, where black Muslims work in servitude for Arab and Moorish farms and households, far from the international spotlight. In 2005, in response to Internet filtering in Mauritania, he translated a guide to using Tor into Arabic and arranged for its distribution to owners of cybercafés. The effect was stunning: the government stopped filtering. Officials "didn't know we were using Tor," says Weddady. "I'm not sure they know what Tor is. But they noticed that our communications were not disrupted, so the filtering was useless."

Such successes can be short-lived, of course, and Weddady predicts that the regime will regroup and resume filtering. "The Middle East in general is a civil-rights desert; it has some of the most sophisticated filtering operations in the world," he says. "Plenty of people I personally know are using Tor in that region." Users know that to any snooper, the messages they post appear to originate from a Tor relay somewhere else in the world, so cybercafé owners can't rat them out even if they want to. "Tor doesn't say, 'Just trust us not to give out your information'--it says, 'We have a design where nobody is in a position to give up your information, because no one person has it,'" says Seltzer, who volunteers on Tor's board. "I do believe Tor is the best solution for people who are trying to get access to blocked matter, or are trying to speak anonymously."

Bridging Tor's Gaps

Neither Tor nor any other tool is a perfect solution to Internet spying and censorship. As an open-source project, Tor publishes everything about its workings, including the addresses of its relays. That doesn't betray the actual source and destination of users' information, but it does mean that a government could obtain this list of addresses and block them. (So far, nobody has taken this step, though Iran, Saudi Arabia, and the United Arab Emirates did find a way to block Tor for a few months in 2008.) Second, using Tor can make Internet access painfully slow; online activities can take more than 10 times longer when using Tor, according to a study by Harvard's Berkman Center for Internet and Society. "It turns out the speed of light isn't so fast after all," Dingledine deadpans. And this problem is getting worse; in the past year, the number of users has increased faster than Tor's developers can add relays.

But the biggest limitation is simply that all these tools still reach only a narrow slice of the world's Internet users. Yes, if you're a business traveler in China and have technical savvy and bandwidth--or you hire someone to set you up--you can circumvent government filters. (It's generally understood that state security forces will rarely move to shut down circumvention tools unless they're publicly embarrassed by being outsmarted online.) But a recently released Berkman report by Zuckerman, faculty codirector John Palfrey, and researcher Hal Roberts has concluded--on the basis of data supplied in 2007 by makers of circumvention software--that only a few million people use the major circumvention tools worldwide. It's true that usage has grown since then--and this estimate doesn't count everybody who has figured out a way to use proxies. Still, China alone has 300 million Internet users, and the researchers believe that most of them aren't equipped to fight censorship. Meanwhile, the list of nations that censor is only growing. Two years ago, Turkey piled on, with particular zeal for stamping out criticism of the nation's founding father, Kemal Atatürk.

Tor is preparing for the fight against relay blocking by creating a system of "bridge nodes"--a constantly changing list of IP addresses through which people can reach the main network of relays. A user can simply send an e-mail asking for a bridge address. Of course, an Iranian censor could also request and block such addresses, but the idea is to defeat such efforts by generating ever more bridges, donated by a wide range of Internet users. And Jonathan Zittrain, a Berkman cofounder and Harvard Law School professor, envisions going even further. "The next big moment that the Tor people haven't implemented--something in the background, something that would be huge--would be if your use of Tor, by default, makes you a Tor node yourself," he says. "At that point, it totally scales. The more people use it, the more people can use it."

As part of a three-year effort to improve the software and expand its use, Tor's staff and volunteers will step up appeals for Tor users to let their computers serve as bridges to individual users elsewhere. But taking the next step--becoming a relay, or node, potentially available to any Tor traffic--would massively increase the traffic flowing through a user's computer. If users became nodes by default, it could defeat the purpose of using Tor to remain low key: once a user wandered into a cybercafé to blog anonymously, that terminal would soon stand out as a hub of Internet traffic. What's more, such a system "sets off an arms race with all the network providers and network administrators," says Andrew Lewman, Tor's executive director. "It increases traffic, and we become something they might block, because that's their job." Tor would ultimately like to find safe ways to enlist distributed help, but for now, developers are pursuing intermediate goals, such as limiting bulk data transfers and improving the flow among existing Tor relays.

One criticism leveled against Tor is that it can be used not only for good purposes but for bad--protecting distributors of child pornography, for example. Dingledine's response is that Tor's protections help law enforcement catch criminals, too, while criminals may find it more effective to use neighbors' or public Wi-Fi links, or hacked computers, to mask their identities.

Another concern is that circumvention tools--especially those that only use a single proxy, which holds information about who is talking to whom--can create privacy and security worries of their own. Earlier this year, Hal Roberts discovered that certain tools used widely in China--DynaWeb Freegate, GPass, and FirePhoenix--appeared to be offering to sell users' browsing histories. While there's no evidence that any individual's privacy was compromised, the point was made: in many cases, using anonymity or circumvention systems still means trusting an organization with your information--and trusting that its privacy policies can and will be honored. (With Tor, it's a bit different; since no single relay ever holds the information about the complete route, you must trust the integrity of algorithms that obscure connections between origins and destinations.) "I don't doubt the dedication of the people hosting these tools, but what I'm concerned about is whether they will protect your data," Roberts says. "The biggest takeaway is: they have that data."

Dingledine thinks events will push people to seek the protections that Tor and other tools provide. In 2006, for example, AOL gave away millions of users' search terms for research purposes. Although the searchers were identified only by random numbers, bloggers and reporters were quickly able to identify individual users from clues based on the search terms. (Since Tor uses a different router pathway for each user each time, it's impossible to amass such aggregate data about even an anonymously identified Tor user.) Dingledine reasons that each time a national censor blocks news sites and YouTube, or an ISP or website loses or sells or gives away user data, people will seek solutions. "The approach we've taken so far is to let the bad guys teach people about it," he says. "Let the AOLs and the China firewalls screw up. Let everybody read about why they want privacy on the Internet." More and more people might just decide that enough is enough.

David Talbot is *Technology Review*'s chief correspondent.

Cambridge, MA
Friday, April 24, 2009
http://sustainabilitysummit.mit.edu/ (http://sustainabilitysummit.mit.edu/)

The Front End of Innovation (http://www.iirusa.com/feiusa/fei-home.xml)
Boston, MA
Monday, May 18, 2009 - Wednesday, May 20, 2009
http://www.iirusa.com/feiusa/fei-home.xml (http://www.iirusa.com/feiusa/fei-home.xml)

MIT Sloan CIO Symposium: Sustaining CIO Leadership in a Changing Economy (http://www.mitcio.com/)
Cambridge, MA
Wednesday, May 20, 2009
http://www.mitcio.com/ (http://www.mitcio.com/)

TieCon East (http://www.tieconeast.org/2009/)
Boston, MA
Thursday, May 21, 2009 - Friday, May 22, 2009
http://www.tieconeast.org/2009/ (http://www.tieconeast.org/2009/)

2009 Medical Innovation Summit (http://www.ClevelandClinic.org/innovations/summit)
Cleveland, OH
Monday, October 05, 2009 - Wednesday, October 07, 2009
http://www.ClevelandClinic.org/innovations/summit (http://www.ClevelandClinic.org/innovations/summit)