The New York Times
ROOM FOR DEBATE
A Running Commentary on the News

JANUARY 15, 2010, 7:18 PM

Can Google Beat China?

By THE EDITORS

Liu Jin/Agence France-Presse — Getty Images Google headquarters in Beijing.

Updated, Jan. 16, 9:40 a.m. | Ross Anderson of Cambridge University joins the discussion. He says the growing complexity and volume of Web traffic will only make government censorship harder.

When Google made the surprising announcement on Tuesday that it would no longer censor search results in China, it was applauded by human rights advocates around the world. Since China isn't likely to allow unfiltered results, which would bring up banned topics, Google would have to quit operating google.cn, its Chinese search engine.

But that may not be the end of the story. The very tech savvy are starting to work around the government's filters. Is it just a matter of time before the technologists defeat censorship broadly? What kinds of technological advances would that involve? Or will governments like China be able to maintain strong censorship control with ever more advanced technology on their side?

- Jonathan Zittrain, Harvard Law School
- Steven M. Bellovin Columbia University
- Timothy B. Lee, Princeton's Center for Information Technology Policy
- Mikko Hypponen, F-Secure Corporation
- Tyler Moore, Center for Research on Computation and Society
- Ron Deibert, University of Toronto
- James Andrew Lewis, Center for Strategic and International Studies
- Ross Anderson, Cambridge University

What Web Sites Can Do

***Jonathan Zittrain**, a professor of law at Harvard Law School and co-founder of the Berkman Center for Internet and Society, is the author of "The Future of the Internet — And How to Stop It."*

Most ways to get around filtering are on the demand side: the user has to do some work. I'd like to see some work done on the supply side, by Web sites themselves — and not just because of political censorship, but because of the many other reasons a site can become inaccessible, from a cyberattack to poor network connectivity.

We can design new protocols so that participating Web sites can share information with one another, and in the event one goes down, others can mirror what had been there, in exchange for similar help should they be the next victims.

We need a mutual aid treaty for the Internet, opted in one Web site at a time.

It's a kind of mutual aid treaty for the Internet, opted in one Web site at a time — creating a more robust infrastructure against all sorts of blockages. Already, we're building an infrastructure with sites like Herdict so that users can report when they can't get to a given site — something that web site operators are keen to know. As a public early warning system develops for network trouble, the next logical step is to help patch them up as they happen.

Read more...

A Matter of Cost

Steven M. Bellovin *is a professor of computer science at Columbia University, where he specializes in networks, security, and why the two don't get along.*

There's a saying in the security business: "amateurs worry about algorithms; pros worry about economics." There's no doubt that China — or any government so-minded — can censor virtually everything; it's just that the cost — cutting most communications lines, and deploying enough agents to vet the rest — is prohibitive. The more interesting question is whether or not "enough" censorship is affordable.

How much effort are people and companies outside China willing to expend on anti-censoring measures?

There are a variety of techniques that dissidents can use to evade the censors, ranging from obvious things like encryption to assorted anonymous networking techniques to breaking messages up into separate pieces that are nonsensical individually but turn into a real message when enough pieces are combined.

They can even use pictures, either normal ones with hidden messages embedded (a technique known as "steganography") to screen shots of Web pages the government wouldn't like. Of course, there are some obvious countermeasures the government could employ, but they're costly — optical character recognition from pictures is possible but not easy to do efficiently. China currently has more than 300,000,000 Internet users; using heavyweight censorship techniques on all international connections is probably not affordable.

Read more...

Making Freedom Inconvenient

Timothy B. Lee *is an adjunct scholar at the Cato Institute and a member of the Center for Information Technology Policy at Princeton University. He blogs at Bottom-Up.*

Censorship is not primarily about technology. Human beings are much smarter than computers, and they inevitably find ways to circumvent filters to get the content they want. Rather, the basis of effective censorship in China, like all government power, is the ability to punish people in "real life" when they do something online the government doesn't like.

There is no purely technological solution because censorship is not primarily a technological problem.

The Chinese government knows that the "Great Firewall of China" won't stop all attempts to access disfavored foreign Web sites. That is not its goal. The government simply seeks to make disfavored foreign Web sites inconvenient enough that most Chinese users will switch to homegrown alternatives that are under the government's thumb. This allows the government to focus its human resources on the small minority of people who persist in circumventing the Great Firewall.

Google can do a lot of good by investing in improved circumvention technologies. A worldwide network of proxy servers helped dissidents in Iran communicate with the outside world in the weeks after last year's disputed election. Google could certainly invest in the creation of a more extensive, robust, and user-friendly network of proxy servers.

Read more...

Not a War, a Stalemate

***Mikko Hypponen**, an authority on cybercrime who has tracked down several online criminals, is the chief research officer at F-Secure Corporation in Helsinki, Finland.*

I don't see how Google could win against China.

Google could be pushed out of China and the great firewall of China could block access to google.com and other global versions of Google.

For the Chinese end user, bypassing the great firewall isn't hard if you know what you're doing. However, the vast majority of the hundreds of millions of Chinese Internet users would not know how to do it.

For the Chinese end user, bypassing the great firewall isn't hard, but that's not the issue.

I don't think Google and China will end up in an all-out war. Here's what I think will happen: Google or the U.S. State Department will make more accusations against China. China won't respond at all or will respond with their usual confused statements. Google will lift some, but not all of the censorship they have in place on google.cn. The Chinese government won't respond. Time will pass and this whole event will soon be forgotten.

Meanwhile, the targeted Trojan attacks carry on as they have for several years.

Choices Made for Business

***Tyler Moore** is a postdoctoral fellow at the Center for Research on Computation and*

Society at Harvard University.

Online censorship will keep working so long as repressive governments continue to carry it out. I say this not because I expect governments to maintain the upper hand technologically.

Computer scientists have long known that perfect censorship is practically impossible — holes in the great firewall can be found and filters remain incomplete. However, the goal of censorship is merely to control most, not all, of a population. Because the technologies available to fight censorship are unlikely to be adopted at a large scale, censorship will continue to be effective.

There are technical solutions to censorship, but they may never be scalable.

Technical solutions for defeating censorship were proposed and implemented a decade ago. These systems are still used today by tech-savvy activists. However, most targets of censorship — like Twitter, Facebook, and YouTube — can be successfully blocked because of architectural choices made for business reasons.

Read more...

More Than a Tech Problem

Ron Deibert *is the director of the Citizen Lab at the University of Toronto's Munk Centre for International Studies, a principal investigator of the OpenNet Initiative and Information Warfare Monitor projects, and the vice president of policy for Psiphon Inc.*

For years, innovative solutions to sidestep Internet filters have plagued Internet censors. Rebellious kids, hoping to sneak a peek around parental controls, have come up with some of the best of these ideas. Others are highly sophisticated open-source systems tended to by brainy PhD.'s and caffeine-fueled programmers.

Will Google now devote some of its formidable engineering resources to the problem of censorship circumvention? Will the people behind Google mail, Google wave and Google docs bring us something like Google Free? Surely a company as powerful as Google can invent an app that guarantees Internet freedom.

We need a worldwide movement of citizens and policymakers to protect the Internet as an open global source of information.

The problem is that circumventing Internet censorship is at least as much a social and political problem now as it is technological. And that's because the nature of controls exercised in this domain are changing.

Read more...

China May Succeed

James Andrew Lewis *is a senior fellow at the Center for Strategic and International Studies and directs its technology and public policy program.*

A few years ago I worked on a C.I.A. study on how information technology would change the politics of nondemocratic countries. There is clearly a political effect from access to information and the ability of regime opponents to coordinate and plan, but one country in the world has spent billions on technology to defeat this: China. We concluded that for now, the Chinese government would be able to control the political effects of information technology.

China is in a good position to succeed. As manufacturing moves to Asia, it will be easier to build controls into the technologies China's citizens use. China wants its own IT industry and has been investing for decades in the people and plants it will need to get one. The policy has two goals: expanding the ability to control IT and ending the dependence on Western technology.

As manufacturing moves to Asia, it will be easier for China to build controls into the technologies its citizens use.

Read more...

The Dictator's Dilemma

Ross Anderson *is Professor of Security Engineering at Cambridge University, England, and author of The Snooping Dragon, as well as the standard textbook Security Engineering.*

Governments have always tried to control information, but the game is changing fast. Globalization is shifting the real power from national post offices, press censors and police forces to private companies. Overall, that's a good thing; it's easier to set up a new company than a new country.

It's technically possible to filter the Internet but it's getting ever harder in practice because of the growing volume and complexity of traffic, and because of the growing use of encryption. And the consolidation of services in large "Web 2.0" firms like Google, Microsoft and Facebook poses a new dilemma for dictators.

Filtering is becoming ever harder, and blocking entire sites now has serious side effects.

If you want to block some content on YouTube, the only practical ways to do that may be to get YouTube to cooperate, or to block the whole site: you "block it all, or not at all." But blocking it all can have serious side effects. If you block all of YouTube (as Thailand and Pakistan have tried), your schools will suffer and your population, deprived of entertainment, might get restive.

Read more...