International Bloggers and Internet Control

Hal Roberts, Ethan Zuckerman, Jillian York, Robert Faris, and John Palfrey

Berkman Center for Internet & Society

August 2011

Each co-author is affiliated with The Berkman Center for Internet & Society at Harvard University. Hal Roberts is a fellow; Ethan Zuckerman is a senior researcher; Jillian York was a Berkman Center staff member at the time of this report; Robert Faris is the director of research; and John Palfrey is a faculty co-director of the Berkman Center. We gratefully acknowledge support for this research from the US Department of State via a subgrant through Internews Network (USA).

We are grateful for the participation of Global Voices Online and for the work of those who translated our blogger survey into more than a dozen languages. We offer our special thanks to the bloggers that participated in the survey.

OBJECTIVE

The Internet is an increasingly contested space, particularly in countries with repressive governments. Infringements on Internet freedom, particularly through Internet filtering and surveillance, have inspired activists and technologists to develop technological counter-measures, most notably circumvention tools to defeat Internet filters and anonymity tools to help protect user privacy and avoid online surveillance efforts. The widely heralded role of online activism in the Arab spring and the increasing incidence of Internet filtering around the world have spurred greater interest in supporting the development and dissemination of these tools as a means to foster greater freedom of expression online and strengthen the hand of activists demanding political reform. However, despite the perceived importance of this field, relatively little is known about the demand for and usage patterns of these tools.

In December 2010, we surveyed a sample of international bloggers to better understand how, where, why, and by whom these tools are being used.

From previous research, we know that circumvention tools are effective in evading national Internet filtering, though they can be slow, insecure and difficult to use.[1] We also know that worldwide circumvention tool usage is limited. In our recent report on circumvention tool usage,[2] we found that at most (and likely far fewer than) 3% of Internet users in countries that engage in substantial filtering use circumvention tools once a month or more. Through this survey, we aim to better understand usage of these tools by a specific community of politically- and internationally-oriented bloggers.

The full, aggregated results of the survey are available online.[3]

KEY FINDINGS

- *A small majority of respondents in all surveyed countries, and 79% of respondents in heavily filtering countries, use circumvention tools at least occasionally.*

[1] Hal Roberts, Ethan Zuckerman, and John Palfrey, "2007 Circumvention landscape report: methods, tools, uses," The Berkman Center for Internet & Society, March 2009, http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/2007_Circumvention_Landscape.pdf.

[2] Hal Roberts et al., "2010 Circumvention Tool Usage Report," The Berkman Center for Internet & Society, October 2010, http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/2010_Circumvention_Tool_Usage_Report.pdf.

[3] "International Bloggers and Internet Control: Full Survey Results," The Berkman Center for Internet & Society, August 2011, http://cyber.law.harvard.edu/publications/2011/International_Bloggers_Internet_Control_Full_Survey_Results.

- *Tor and HTTP/Socks/CGI proxies were the most popular tools among our respondents.*
- *Respondents report that privacy is the most important aspect of circumvention tools.*
- *Most respondents rated speed as the most poorly performing aspect of circumvention tools.*
- *Many respondents that do not use circumvention tools report that they have no need to access blocked content.*
- *Respondents broadly but not universally disagree with national Internet filtering of content for adults.*
- *Respondents broadly but not universally report that they believe that their online activity is monitored by a range of actors.*
- *Most respondents believe that posting content critical of their governments online poses significant legal and physical risks, and most selectively self-censor in response to those risks.*

METHODOLOGY AND SAMPLE

Studying the usage of circumvention tools is hard because most circumvention tool users are almost by definition trying to avoid notice and because, according to our previous research, usage of these tools is rare among the general population of Internet users even in countries that aggressively filter the Internet. Instead of focusing on the general Internet population, we focused this survey on a specific community of politically- and internationally-oriented bloggers from a wide variety of countries, including countries with substantial national Internet filtering and a few without. We think that this sample is more likely to use circumvention tools and that respondents' use of the Internet to circulate news and opinion content means their behavior is highly informative for discussions of political freedom on the Internet.

Working in conjunction with Global Voices Online—an aggregator of blogs and citizen media from around the world—we created a sample of 1,080 individual bloggers referenced in 2010 by Global Voices Online (GVO). We built this sample by running a crawler to pull out every blog linked from at least one post published on GVO over the past year and subsequently generated a subsample of these blogs corresponding to a set of target countries. Most posts on GVO focus on some combination of politics, political freedom, Internet freedom, and international community. Compared to the general population of Internet users and even the general populace of bloggers, this GVO sample is likely to be more politically active, more internationally connected, more active in posting content, and more interested in issues of Internet freedom. We believe this sample therefore represents a set of people much more likely to use circumvention tools than the general Internet population, and specifically to use them for political purposes.

We worked in cooperation with Global Voices also because the organization is a widely trusted leader in online freedom of speech issues. We believed that we would increase cooperation with a sensitive study by involving the organization in the process. The subset of blogs referenced by GVO that we studied included only blogs tagged by the referencing GVO posts as relevant to one of the following countries: Bahrain, Brazil, Burma (Myanmar), China, Iran, Kazakhstan, Morocco, Pakistan, Russia, Saudi Arabia, South Africa, South Korea, Syria, Thailand, Tunisia, Turkey, United Arab Emirates, and Vietnam. These countries were chosen based on prevalence of filtering and on geography. We sought to include nations where Internet filtering is pervasive, but we also sought geographic diversity and inclusion of nations with large and active blogging populations. Of this sample, only Brazil, Russia, and South Africa have not been documented by the OpenNet Initiative as imposing substantial Internet filtering on their citizens.

This sampling strategy is only capable of producing a set of blogs that are included within blog posts that reference the target countries; many blogs cited within a post tagged as relevant to a particular country are only marginally relevant to the country; i.e. a post substantively about Tunisia might mention Syria in passing, and both countries would be included in GVO's tags. This country tagging data only represents the country discussed in the blog post and does not always reflect the country of residence for the blogger. While some bloggers may indicate their country of residence on their blog, we are only able to ascertain the country of residence for the full sample based on their responses in the survey.

We administered the survey and survey invitations in English and in the 12 primary languages represented by the target sample countries: Arabic, Persian, Burmese, Vietnamese, French, Turkish, Urdu, Chinese, Korean, Russian, Thai, and Portuguese.

In addition to questions about circumvention tool usage, we asked questions about the respondent's views of Internet filtering and surveillance and about the risks of posting content online.

RESPONDENTS

Of the sample of 1,080, 244 individuals responded, for a response rate of 22.4%. The set of respondents was heavily biased toward males, college graduates, and young people. 74% of respondents were male. 77% of respondents reported having undergraduate or graduate university degrees, and 100% reported having high school degrees. 42% of respondents were between the ages of 20-30; 31% were aged 31-40; 17% were aged 41-50, 6% were aged 51-60, 3% were aged 61-70, and a single respondent was over 71 years of age.

The demographics of our respondents may be atypical for the general Internet population; however, there is evidence to suggest that the blogospheres in many of our target countries fit similar demographics. For example, the Berkman Center's study of the Arabic-language blogosphere—which overlaps with six countries in this study—found that three-quarters of the bloggers in the study were under 35 years old, the majority were in the 25-35 year-old range, and 60% were male.[4] Similarly, the Berkman Center's study on the Iranian blogosphere found that the majority of bloggers in that blogosphere were male.[5]

Respondents were asked in which country they currently reside; as a result, we received responses from a number of countries outside of our initial target countries, including a large number of responses from bloggers living in the United States. These countries of residence vary widely in their approaches to filtering. For some—such as China, Tunisia, and Iran—the OpenNet Initiative has documented pervasive filtering across several categories of content. For others—such as Brazil, the United States, and South Africa—the OpenNet Initiative has found no evidence of national Internet filtering.

FINDINGS

A majority of respondents have used circumvention tools at least occasionally.

Among all respondents, we found that 58% reported ever having used a circumvention tool. For this and for many subsequent results, we divided respondents into two sets: those reporting residence in a country documented by ONI to practice substantial national Internet filtering, and those reporting residency in a country documented by ONI to practice no or minimal national Internet filtering.

For the resulting filtered and non-filtered respondents, we found that regular circumvention tool usage is much more common among respondents in filtered countries, with 78.7% of respondents in heavily filtering countries using a circumvention tool at least occasionally:

FREQUENCY OF TOOL USAGE BY LEVEL OF FILTERING

	NEVER	ONCE PER WEEK OR LESS	MORE THAN ONCE PER WEEK
NO OR MINIMAL FILTERING	52.2%	38.2%	9.6%
HEAVY FILTERING	21.3%	36.1%	42.6%
TOTAL	42.6%	37.6%	19.8%

[4] Bruce Etling et al., "Mapping the Arabic Blogosphere: Politics, Culture, and Dissent," June 2009, http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/Mapping_the_Arabic_Blogosphere_0.pdf.

[5] John Kelly and Bruce Etling, "Mapping Iran's Online Public: Politics and Culture in the Persian Blogosphere," April 2008, http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/Kelly&Etling_Mapping_Irans_Online_Public_2008.pdf.

Tor and HTTP/Socks/CGI proxies were the most popular tools

Of the 118 respondents who reported ever having used a circumvention tool, 87 specified the tool or tools they used either by name or by type of tool. These respondents reported using the following tools or types of tools:

WHICH CIRCUMVENTION/PROXY/ANONYMITY TOOL DO YOU USE MOST OFTEN FOR BROWSING THE WEB AND OTHER ONLINE ACTIVITIES?	
TYPE OF TOOL	PERCENTAGE OF USERS
HTTP/Socks/CGI Proxies	33.3%
Tor + I2P	28.7%
Popular Desktop Tools	19.5%
Virtual Private Networks (VPNs)	18.4%
Other	16.1%
Not sure	4.6%
Note: Total percentages add up to more than 100%, as respondents were allowed to specify more than one tool.	

Within these broad tool types, the 87 respondents listed 32 different specific individual tools. Tor had the highest name recognition of the tools with 24 mentions, followed by Hotspot Shield with 8 mentions. The full list of tools mentioned by respondents can be found in the appendix.

WHICH CIRCUMVENTION/PROXY/ANONYMITY TOOL DO YOU USE MOST OFTEN FOR BROWSING THE WEB AND OTHER ONLINE ACTIVITIES?		
TYPE OF TOOL	PERCENTAGE OF USERS IN COUNTRIES THAT FILTER	PERCENTAGE OF USERS IN COUNTRIES THAT DO NOT FILTER
HTTP/Socks/CGI Proxies	34.9%	31.8%
Tor + I2P	14.0%	43.2%
Popular Desktop Tools	25.6%	13.6%
Virtual Private Networks (VPNs)	27.9%	9.1%
Other	23.3%	9.1%
Not sure	2.3%	6.8%
Note: Total percentages add up to more than 100%, as respondents were allowed to specify more than one tool.		

Respondents report that privacy is the most important aspect of circumvention tools.

We asked users to rate on a scale of 1–5 the importance of various aspects of circumvention tools when choosing which tool to use and found that users rated privacy highest, with operating platform compatibility and speed also ranking highly:

HOW IMPORTANT IS EACH ASPECT OF THE TOOL YOU USE MOST OFTEN?	
	IMPORTANCE (4-POINT SCALE)
Privacy	3.62
Compatibility with my computer/operating system	3.49
Speed	3.39
Functionality of specific websites	3.23
Cost	3.16
Ease of installation	3.10
Ease of discovery	3.07

We further asked respondents whether they primarily use tools to access blocked content or to protect their privacy. We found respondents almost evenly split between access (54%) and privacy (46%). Breaking the results down into regions, we found that respondents in Russia (where there is no national Internet filtering) use tools mostly but not solely to protect their privacy (68%), while respondents in the Middle East (72%) and China (90%), where filtering is generally pervasive, use tools mostly but not solely to access blocked content. Note that even in countries like Russia with no national Internet filtering, there is filtering at a variety of other levels, including in homes, workplaces, schools, libraries, and cyber cafes; many people use circumvention tools to circumvent these types of more local filtering.

Most respondents rated speed as the most poorly performing aspect of circumvention tools.

We asked users to rate the performance of circumvention tools for the same aspects listed above. We found speed to be rated the most poorly, with specific site functionality and ease of discovery also rating relatively poorly:

HOW DOES THE TOOL YOU USE MOST OFTEN PERFORM IN EACH OF THE FOLLOWING AREAS?	
	PERFORMANCE (5-POINT SCALE)
Speed	3.28
Functionality of specific websites	3.62
Ease of discovery	3.75
Privacy	3.95
Ease of installation	3.99
Cost	4.15
Compatibility	4.33

This finding correlates with our 2007 evaluation of circumvention tools, which found that the speed of circumvention tools ranged from fair to very poor. It also echoes conversations we have conducted with circumvention tool developers, who report that speed and site compatibility, along with economic sustainability, are their most difficult challenges to address.

Breaking this data down into specific tools, we found speed to be the lowest rated aspect of performance of every type of tool except VPNs, for which cost received the lowest rating and speed the second lowest:

TOOL PERFORMANCE BY TYPE OF TOOL (5-POINT SCALE)

	DISCOVERY	INSTALLATION	SPEED	PRIVACY	SPECIFIC SITES	COST	COMPATIBILITY
DESKTOP	3.75	4.00	3.47	3.94	3.47	4.67	4.36
PROXIES	4.09	4.14	3.64	4.15	4.00	4.44	4.68
TOR/I2P	3.87	3.96	2.78	3.91	3.19	4.62	4.32
VPN	3.94	4.13	3.38	4.23	3.87	3.27	4.31

Note that the speed of Tor rated particularly poorly, and its privacy received the lowest rating among its users compared to the ratings given to other tools by their users. This is a puzzling finding because Tor is almost universally regarded as having the strongest privacy protections of any circumvention tool. Tor's privacy rating may reflect a higher level of sensitivity to and skepticism of tool privacy in general by users of Tor, which would explain why Tor is the most popular tool among our respondents despite its very low speed rating. Tor was also much more popular in countries that do not filter compared to countries that filter, likely indicating use the tool for its privacy properties and despite its slow performance.

Many respondents that do not use circumvention tools report that they have no need to access blocked content.

Of the respondents who indicated that they had never used a circumvention tool, the most common primary reasons for not having used a circumvention tool were lack of national Internet filtering, no need to access blocked content, and lack of knowledge of tools. In countries with national filtering, most users who do not use circumvention tools choose not to do so because they have no need to access blocked content.

WHAT IS THE PRIMARY REASON YOU DO NOT USE THESE TOOLS?

	PERCENTAGE OF RESPONDENTS
There is no filtering in my country	32.1%
I have no need to access blocked content	31.0%
I do not know how/I lack the proper tools to circumvent	20.2%
Other	9.5%
Fear of incrimination by government or government agencies	3.6%
I am using a public computer	1.2%
I agree with filtering policy	1.2%
Fear of incrimination by employer	1.2%
Fear of incrimination by non-government paramilitary or other threatening groups	0%

Removing the respondents who indicated that they have no filtering, this finding indicates that fully 45% of respondents who choose not to use circumvention tools do so for lack of relevant content, versus 32% who lack the knowledge necessary to use the tools.

It is notable that relatively few respondents that do not use circumvention tools report the risk of incrimination as the primary reason.

Respondents broadly but not universally disagree with national Internet filtering of content for adults.

75% of respondents who reported Internet filtering in their countries either disagreed or disagreed strongly that national Internet filtering was beneficial to society, with the remainder having either no opinion, agreeing, or agreeing strongly that national Internet filtering is beneficial:

"NATIONAL FILTERING IN MY COUNTRY IS BENEFICIAL TO SOCIETY"

	PERCENTAGE OF RESPONDENTS
Strongly agree	2.2%
Agree	8.7%
Neither agree nor disagree	13.0%
Disagree	22.8%
Strongly disagree	52.2%

Broken down further into types of content, there is almost universal agreement that filtering of political content for adults is not acceptable. There is much more, though still minority, support for filtering of sexual, gambling, and copyrighted, and hacking content for adults. A small majority of respondents think that filtering either is or might be acceptable for hacking or copyrighted content.

IN YOUR OPINION, IS NATIONAL FILTERING FOR ADULTS ACCEPTABLE IN THE FOLLOWING CATEGORIES?

	YES	NO	MAYBE
Sexual content	17.9%	59.9%	22.2%
Gambling sites	23.7%	61.6%	14.7%
Religious content	3.4%	83%	13.6%
Political content	4.8%	89.9%	5.3%
Downloading of copyrighted media	26.1%	48.3%	25.6%
Social networking	4.4%	88.8%	6.8%
Dating sites	5.8%	85.9%	8.3%
Hacking content	27.1%	48.6%	24.3%
Circumvention / proxy / anonymity tools	6.8%	77.2%	16.0%

Respondents broadly but not universally believe that their Internet activity is monitored by a range of actors.

51% of respondents believe that their governments are definitely capable of monitoring their online activities, and 59% believe that their Internet service providers are definitely capable of monitoring their online activities.

HOW CAPABLE DO YOU THINK EACH OF THE FOLLOWING PEOPLE OR ORGANIZATIONS ARE OF MONITORING YOUR ONLINE ACTIVITIES?

	DEFINITELY	PROBABLY	PROBABLY NOT	DEFINITELY NOT	NOT SURE
Government	51.4%	25.7%	8.1%	12.4%	2.4%
Internet Service Provider (ISP)	59.1%	25.5%	4.3%	8.2%	2.9%
Websites visited or search engines	35.8%	39.1%	11.1%	10.6%	3.4%
Family/spouse	14.1%	22.8%	23.3%	36.9%	2.9%
Employer/company	25.7%	33.5%	13.6%	22.3%	4.9%
Cybercafé	19.3%	43.7%	15.5%	15.9%	5.3%
Advertisers	19.3%	39.6%	16.4%	17.9%	6.8%

Respondents are less confident that various actors are currently monitoring their online activities, with only 35% believing that their governments are monitoring them and 25% believing that their Internet service providers are monitoring them.

WHICH OF THE FOLLOWING PEOPLE OR ORGANIZATIONS DO YOU BELIEVE ARE CURRENTLY MONITORING YOUR ONLINE ACTIVITIES?

	DEFINITELY	PROBABLY	PROBABLY NOT	DEFINITELY NOT	NOT SURE
Government	35.3%	29.4%	22.6%	4.9%	7.7%
Internet Service Provider (ISP)	25.4%	32.2%	28.8%	5.4%	8.3%
Websites visited or search engines	27.9%	48.5%	15.2%	1.5%	6.9%
Family/spouse	2.5%	4.1%	24.4%	65.5%	3.6%
Employer/company	11.1%	12.6%	25.8%	43.4%	7.1%
Cybercafé	5.0%	20.1%	32.7%	29.2%	13.1%
Advertisers	22.9%	42.0%	18.5%	8.8%	7.8%

Most respondents believe that there are significant legal and physical risks for them in posting content critical of their governments online, and most selectively self-censor in response to that risk.

74% of respondents think that there is some risk of detention, arrest, or criminal investigation in posting material critical of their governments online, and 59% think that there is some risk of violence directed at themselves or their families.

WHAT DO YOU THINK ARE THE RISKS IN POSTING MATERIAL CRITICAL OF THE GOVERNMENT IN YOUR COUNTRY?

	HIGH RISK	LOW RISK	NO RISK	NOT SURE
Detention, arrest, or criminal investigation	39.7%	34.2%	21.1%	5%
Monetary fine	23.1%	35.4%	32.3%	9.2%
Violence directed at self or family	26.8%	32.3%	32.8%	8.1%
Public reporting of Internet activity	23.6%	32.3%	35.4%	8.7%
Loss of employment or demotion	32.2%	27.6%	29.7%	10.6%

59% of respondents have chosen not to post content because of possible risks, 35% have not refrained from posting content, and 6% are not sure. Of those who have refrained from posting risky content, 68% posted some risky content and 32% posted no risky content.

Overwhelmingly, the content that respondents refrained from posting was political in nature:

"I HAVE DECIDED NOT TO POST THE FOLLOWING TYPE OF CONTENT BECAUSE OF THE RISKS INVOLVED"

	PERCENTAGE OF RESPONDENTS
Politics and current events	89%
Religion	31%
Copyrighted media	23%
Sexuality	18%
Social networking	14%
Hacking	7%
Circumvention/proxy/anonymity tools	6%
Gambling	5%
Dating	5%

DISCUSSION

Our 2010 report on overall circumvention tool usage found that a very small percentage of the general Internet population uses circumvention tools. This finding does not mean that circumvention tools are unimportant in making the Internet accessible as a civic space for nations that filter the Internet. Supporters of circumvention tools often point out that the impact of the tools can be greatly magnified if core populations of highly connected and influential people use the tools and distribute the information they gather or post through the tools to a much wider audience. While there may be only a couple of circumvention tool users in a small town in China, those users might be highly influential and may be able to communicate what they learn online to their friends and neighbors. Similarly, while we might see only a small number of Tunisians using circumvention tools to post content to blogs and video sites, it's possible that their content is highly influential to populations in the Diaspora around the world.

Our finding in this survey that a majority of our respondents—who we believe are likely to be the sort of influencers described above—at least occasionally use circumvention tools. This result is consistent with the argument that there could be significant community effects from circumvention tool use. However, another key finding of this survey—that a majority of those who do not use the tools in filtered countries choose not to use them because of lack of relevant blocked content—challenges the theory that if circumvention tools were more easily and widely available and performed better that this would lead to widespread use. If the value of the circumvention tool to influential users comes from the ability to access forbidden information, for instance, information from foreign newspapers about global or local crises, the fact that a significant number of users do not see the utility of blocked information is an intriguing finding.

One possible interpretation of the relative lack of demand for access to blocked content, which is striking given the educational level and evidence of political involvement in our sample, is that in filtered countries there is less pent up demand for access to political information published outside the country than we might expect. Much more research is necessary to understand better more precisely how people are using these tools, what information they are using them to access, and their forms of influence in their local and global communities.

Another key finding of this research—that the respondents mostly perceive significant risks in posting political content online and mostly respond by selectively self-censoring themselves—shows that Internet censorship may not be solely, or even primarily, about blocking access to international content. Instead, a major purpose may be suggesting that Internet connections are subject to surveillance, which may be intended to encourage the sort of self-censorship we've seen in this survey.

For these bloggers (many of whom bravely continue to publish in the face of substantial legal and physical risk) the most important mechanisms of censorship are traditional tools like arrest, detention, and physical violence. Combined with the finding that many of our respondents see no value in accessing blocked content, this finding of self-censorship offers support to the theory that the most effective forms of censorship are offline ones, through traditional forms of knock-on-door enforcement, on the local content that is generally in more demand than filtered international content.

APPENDIX: CIRCUMVENTION TOOLS MENTIONED BY RESPONDENTS BY CATEGORY

HTTP/SOCKS and CGI Proxies

- AOL proxy
- Bind2
- CiteBite
- Cooloo
- FoxyProxy
- garak.surfersafe.com
- Glype
- Google Chrome's one-click proxy
- Hide IP
- hideymyass.com
- kyproxy
- Opera Turbo
- Peacefire Circumventor
- PHProxy

Popular Desktop Tools

- Anonymizer
- Freegate
- Hotspot Shield
- Ultrasurf

TOR + I2P

- I2P
- Tor

VPN

- 12vpn
- Freedur
- vpnod.com
- Witopia
- Your Freedom

Other

- https
- Incognito
- Psiphon
- Safari private browsing
- SSH
- Zip