COLLATERAL FREEDOM

A Snapshot of Chinese Internet Users Circumventing Censorship

April 2013

Version 1.0

This study was conducted by David Robinson, Harlan Yu and Anne An. It was managed by OpenITP, and funded by a grant from Radio Free Asia's Open Technology Fund.

Audience

This report is intended primarily for developers and funders of censorship circumvention technology projects. It is also designed to be accessible for non-technical policymakers who are interested in Internet freedom, and for China specialists without technology background.

We have included explanations of technical terms, and translations of Chinese phrases. These additional notes are highlighted in **blue** throughout the report. Our sources are documented in the endnotes.

OVERVIEW

This report documents the experiences of 1,175 Chinese Internet users who are circumventing their country's Internet censorship—and it carries a powerful message for developers and funders of censorship circumvention tools. We believe these results show an opportunity for the circumvention tech community to build stable, long term improvements in Internet freedom in China.

The circumvention tools that work best for these users are technologically diverse, but they are united by a shared political feature: the collateral cost of choosing to block them is prohibitive for China's censors. Our survey respondents are relying not on tools that the Great Firewall can't block, but rather on tools that the Chinese government does not want the Firewall to block. Internet freedom for these users is **collateral freedom**, built on technologies and platforms that the regime finds economically or politically indispensable.

The most widely used tool in our survey—GoAgent—runs on Google's cloud hosting platform, which also hosts major consumer online services and provides background infrastructure for thousands of other web sites. The Great Firewall sometimes slows access to this platform, but purposely stops short of blocking the platform outright. The platform is engineered in a way that limits the regime's ability to differentiate between the circumventing activity it would like to prohibit, and the commercial activity it would like to allow. A blanket block would be technically feasible, but economically disruptive, for the Chinese authorities. The next most widely used circumvention solutions are VPNs, both free and paid—networks using the same protocols that nearly all the Chinese offices of multinational firms rely on to connect securely to their international headquarters. Again, blocking all traffic from secure VPNs would be the logical way to make censorship effective—but it would cause significant collateral harm. Instead, the authorities steer a middle course, sometimes choosing to disrupt VPN traffic (and commerce) in the interest of censorship, and at other times allowing VPN traffic (and circumvention) in the interest of commerce. The Chinese government is implementing policies that will improve its ability to *segment* circumvention-related uses of VPNs from business-related uses, including heighten registration

requirements for VPN providers and users.

Respondents to our survey were categorically more likely to rely on these commercially widespread technologies and platforms than they were to use special purpose anti-censorship systems with relatively little commercial footprint, such as Freegate, Ultrasurf, Psiphon, Tor, Puff, or simple web proxies. Many of our respondents have used these non-commercial tools in the past—but most have now stopped. The most successful tools today don't make the free flow of sensitive information harder to block—they make it harder to separate from traffic that the Chinese government wishes to allow.

Reading our own findings alongside earlier research, we believe there are three distinct groups of censorship circumventors in China, defined by three different critical needs: **versatility**, **privacy**, and **simplicity**. Of course, each user would ideally have tools that are private, provide versatile connectivity, *and* are simple to use. But in today's environment, Chinese users cannot have everything—and given their diverse needs, different users are drawn to different solutions. In particular, specialized tools are essential for the small but critically important group of users who put privacy first.

We find that most users of circumvention software are in what we call the "versatility-first" group: they seek a fast and robust connection, are willing to install and configure special software, and (perhaps surprisingly) do not base their circumvention decisions on security or privacy concerns. To the extent that circumvention software developers and funders wish to help these users, we find that they should focus on leveraging business infrastructure hosted in relatively freedom respecting jurisdictions, because the Chinese government has greater reason to allow such infrastructure to operate.

We conclude this report with five practical suggestions:

1. Map the circumvention technologies and practices of foreign businesses in China.
2. Engage with online platform providers who serve businesses in censored countries.
3. Investigate the collateral freedom dynamic in other countries.
4. Diversify development efforts to match the diversity of user needs.
5. Make HTTPS a corporate social responsibility issue.

CONTENTS

1 INTRODUCTION

In mainland China, the government blocks its citizens' access to some parts of the global Internet—a policy often referred to as the **Great Firewall** (GFW). This term, although useful and memorable, is misleading, because the firewall is not a fixed, immovable obstacle. It is a dynamic, constantly changing patchwork of technological barriers. For Chinese users, the firewall often seems like static, or fog: particular resources are intermittently blocked or slowed down, with blockages varying from page to page, moment to moment, and place to place inside the country.[1] The Great Firewall, unlike its physical analogue, reshapes itself as censors deploy a growing variety of techniques and continuously fine-tune their efforts. This creates a cat-and-mouse game with circumvention tool providers and with users.

For Chinese users, much more is at stake than just their ability to access foreign news and information. Inside the firewall, the core tools of online life—search engines for finding all kinds of information, social media and email for communicating with others—are engineered for censorship. (The Chinese term **Golden Shield** refers to this combination of a national firewall with a censored domestic Internet.[2]) On Chinese microblogging (**weibo**) sites, politically sensitive posts are often deleted after they are published.[3] Sometimes, the service will secretly censor a post, hiding the deletion from the post's author, so that the author sees his post but no one else does.[4] Or a user's sensitive post may be rejected, and the user asked to revise it.[5] E-mails are subject to surveillance. Web searches omit relevant results.[6] The Chinese companies behind these platforms work hand in hand with China's government to implement censorship, with specialized software development effort and dedicated staff. Technologies play a crucial role in circumventing this censorship, but the most common anti-censorship technology of all may be the Chinese language itself,

---

Great Firewall 防火长城 Users also refer to being "walled" (被墙) or "shielded" (屏蔽).

Golden Shield 金盾工程

weibo 微博 The term weibo has become a generic one for Chinese-language microblogging services, of which the leading two are Sina Weibo and Tencent Weibo.

whose many homophones provide at least a fleeting opportunity to stay ahead of the censors (until these homophones, too, are blocked).[7]

In deciding to **jump over the wall**, as the Chinese phrase puts it, users are often seeking a better way to exchange information with others in China. On foreign sites and platforms, they can connect socially (and exchange information) with other mainland Chinese.

The country's stated policies on Internet censorship have also been changing, suggesting an overall shift toward greater information control. In particular, the national government in late 2012 passed a law which will require providers of "information publication services" and "website access services" (including VPNs) to collect the real name of each user who registers, a policy known in China and elsewhere as **real-name registration**.[8]

Real-name registration rules will (among other consequences) give the Chinese authorities a basis to monitor and regulate the consumer-facing VPNs that are popular for circumvention, while potentially leaving business-facing VPN services undisturbed. Such policies match the theory that we draw from our survey results: China is seeking to segment circumvention-related VPN traffic from business-related VPN traffic. In the future, it may become politically feasible for the government to block all but a "white list" of corporate VPNs and compliant consumer-facing ones, so that only business services and censor-friendly consumer services will be available. There has already been some amount of protocol-level blocking of VPN connections across the GFW, affecting popular consumer-facing VPNs and likely causing some collateral harm to small businesses that use them.[9] Once the authorities learn which users are business users and which ones are consumers (now registered as such, under the new real names policy), it becomes feasible to single out consumer traffic for additional restrictions.[10]

There is a robust research literature on the technical aspects of Internet censorship and circumvention in China,[11] but the user's expe-

---

jump over the wall 翻墙

real-name registration means a government policy requiring online services not to allow pseudonymous registrations, but instead to collect and verify the real name of each user who signs up.

rience with these tools is relatively little studied and little understood. One reason for this gap is the difficulty of gathering information about user experiences, either indirectly or from the users themselves.

To give a taste of the complexity and variety of experiences that even a single user may encounter, we can offer a composite: The median person described by our survey results is a young man, perhaps a university student. His campus network is censored even more heavily than most mainland Chinese Internet connections. He finds that he can use the `google.com.hk` search engine briefly each morning—but the connection to Google usually goes dead after a few minutes. There is a rule of thumb among his friends on campus: it seems each person is permitted up to five searches per day, before losing access to the site. On some days, shortly after connecting to Google he finds that his Internet connection totally stops working for 15-20 minutes, an experience he describes in English as being put "in the penalty box." For a while, he was able to use Hong Kong-based VPN services to circumvent the GFW, though he had to switch VPN servers 2 or 3 times per day. More recently, he has been totally unable to connect to a VPN from the university. A friend's residential Internet connection, in a different part of town, seems to be less heavily censored (universities appear to be more censored than other networks).[12] By bringing his laptop to a friend's home, this user is able connect to a VPN and access the rest of the Internet. He does most of his academic research from her living room. He isn't afraid of being caught circumventing—he simply finds himself traveling to wherever the Internet works best.

Our overall goal in this study is to build an evidence base, turning stories like these into a robust quantitative dataset that can inform circumvention software developers and funders about how the Great Firewall works in practice for Chinese users, and what those users want and need. Who are the people using circumvention technologies in China? How do they learn about Internet censorship, and about their circumvention options? What goals drive them to use these tools? How well or poorly do the tools work, and what does it feel like when trying to use them? Is circumvention technology hard for users to obtain—or is it easy to obtain, and hard to use?

We couldn't interview a thousand users personally—but we could, and did, learn about them through a structured online survey, allowing them to participate directly in a conversation that too often subordinates human factors to technical ones.

2 SURVEY FINDINGS

We conducted an anonymous online survey of a diverse sample of circumvention tool users on the Chinese mainland. We gathered our sample by reaching out to a group of 51 "seed" respondents, Chinese circumvention tool users who were personally known to members of the research team. We encouraged each respondent to share the survey with his or her contacts. In the end, 17 people distributed the survey to their contacts, and we received 1,175 valid responses. Most of our seeds recruited a small number of survey respondents, but in two instances we had a seed respondent succeed in recruiting several hundred contacts to take the survey. For purposes of analysis, our results are partitioned into three groups: The first two groups are from these two high-traffic seeds, and the third combines all remaining responses recruited by our remaining seeds. (Appendix A provides a detailed description of our methodology and survey design.)

- **Group 1** is seeded by a technology entrepreneur in Hangzhou, and this group includes 554 respondents.
- **Group 2** is seeded by an entrepreneur and technology activist in Shanghai, and this group includes 352 respondents.
- **Others** includes all of the remaining respondents, gathered by the remaining 15 seeds. It totals 269 respondents.

Our sample was far from gender parity: nearly 90% of respondents were male. This figure is startling when compared to the overall population, but it is also on par with a 2010 study by Jason Ng, described below. The median respondent age was 26 years old, and nearly two-thirds of our sample were either working professionals in the information technology sector, or students. Our sample is also highly educated: almost 80% have a university degree. (A detailed demographic breakdown of our sample groups is provided in Appendix B.)

TOOL USAGE

Figure 2.1, combining results from all three seed groups, encapsulates our study's most important finding. We asked each respondent

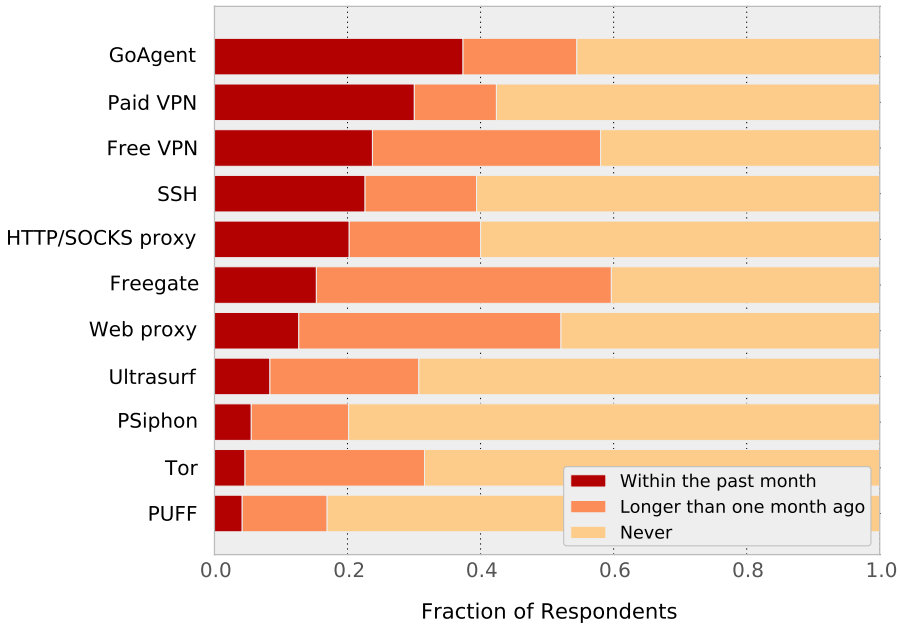

FIGURE 2.1 **How recently have you used each type of software to bypass the Great Firewall?**

whether he had used each type of tool within the last month, longer than a month ago, or never. The chart lists the tools in descending order, based on what portion of our respondents had used each type of tool within the last month. We use the term "current" user as a shorthand for those who have used a particular tool within the last month. The middle interval of each bar shows the fraction of users who, although they have used a particular type of tool before, have not used it within the last month—an answer that leads us to consider the respondent a "former" user of a particular tool.

Each of these tools, in one way or another, connects Chinese users with an uncensored **proxy** server. The most widely used tool is a personal proxy server called **GoAgent**, which relies on Google's cloud infrastructure. GoAgent proxies run on Google servers and can be

---

proxy is a general term for a server in a freedom-respecting environment, that sends and receives information on behalf of one or more users in an unfree environment.

GoAgent is an open source software tool created by Chinese developers. An individual Chinese Internet user can upload a copy of GoAgent onto Google's App Engine servers.

accessed through the same handful of **IP addresses** as Google's own services, including services that the Chinese government chooses not to block such as Gmail, Google Analytics, and Google Apps for Businesses. Technologically speaking, the GFW could use **IP blocking** against those addresses. But that step would block access not just to GoAgent proxies, but to *all* the tools at these addresses—including ones that the regime knows businesses need. A large number of companies that rely on Google Apps for Businesses might find themselves unable to use their corporate infrastructure inside China, and business travelers would lose access to Gmail. Instead of IP blocking, the GFW attempts to censor GoAgent and other uses of Google Apps (without blocking Maps or Gmail) through **DNS poisoning** of the domain names used for Google App Engine sites—domains ending in `appspot.com`. This strategy has limited effectiveness, however, because GoAgent can connect itself directly to the same (unblocked) IP addresses on which so many businesses rely, bypassing the altered DNS information. The **HTTP (or HTTPS)** connections that businesses need will be difficult to separate from the connections made by

---

Once uploaded to Google's system, the GoAgent software functions as a personal proxy server for the particular user who uploaded it, and also for anyone else with whom that user chooses to share the server.

IP addresses (such as `64.233.191.255`) are the unique numbers that identify each computer connected to the Internet. Many different web sites or services—reachable through different domain names—may be hosted by the same computer or system, sharing a single IP address.

IP blocking means discarding all the traffic that is destined for a particular IP address. This is a powerful but blunt technique—a server run by Google, for example, hosts many web domains, and blocking the IP address of that server will block all those different domains at once.

DNS poisoning The Domain Name System (DNS) is a distributed Internet infrastructure that translates human-readable domain names into numeric IP addresses. DNS information is spread throughout many servers, a design that makes the system more resilient but also enables intermediaries to tamper with the results in a local area. "Poisoning" means providing the wrong numeric address for a particular domain name, thus either making the domain inaccessible or, at worst, directing users to a forged version of the server they seek, potentially containing disinformation or malicious software. This can be a finer-grained tool than IP blocking, because it can impact just one of the several domain names that share a particular IP address. A security standard called DNSSEC helps to address this problem by empowering users' computers to automatically verify the authenticity of DNS information. The circumvention technology community should continue to encourage a move toward DNSSEC.

HTTP (or HTTPS) HTTP and HTTPS are the two primary protocols used to share web pages over the Internet (the "S" stands for secure and refers to an encrypted version of the protocol).

GoAgent users. This core Google infrastructure was blocked for a day at the start of the 18th Party Congress,[13] but remains generally accessible throughout China.

The next most used tools, **VPNs**, reflect a similar dynamic: collateral Internet freedom, riding on the coattails of business. Fully 30% of our sample had used paid VPNs within the past month. Some users noted (via the "other" box, on our list of circumvention tools) that they used a workplace VPN, a group we categorized as "free VPN" since the connection likely carries no cost to the end user. VPN traffic has been disrupted in early 2013, causing some harm to business.[14] But that disruption is less than total—businesses, and circumventing Internet users, still find these networks operational.

The purpose-built platforms for censorship circumvention are known to many of our respondents, but currently used by relatively few. **Freegate**, for example, has three times as many former users as it does current ones in our sample: 44.3% of our respondents had used it more than a month ago, but only 15.3% in the last month. **Tor**, which China's censors are free to block without penalty, has indeed been blocked (through tailor-made technical countermeasures added to the GFW) and has lost approximately 85% of its users within the country.[15]

MOBILE CIRCUMVENTION

Unsurprisingly, nearly all of our respondents have used circumvention tools on their desktop computers. In fact, just *two* (out of 1175) respondents reported that they had only used mobile circumvention tools, and never desktop tools. But overall, mobile circumvention is widespread—59.8% of all respondents have used circumvention tools

---

VPNs (Virtual Private Networks) are systems that encrypt all a user's Internet traffic, and route all of it through the VPN server; this in principle makes all the user's activities secure and surveillance-resistant, at least until the traffic leaves the VPN server. VPN servers are typically located outside of the GFW, where they can reach the rest of the Internet without restriction.

Freegate is a purpose-built circumvention tool that automatically and rapidly switches among proxy servers organized by its developers, Dynamic Internet Technology.

Tor (`torproject.org`) is a purpose-built peer to peer technology that encrypts users' communications in transit and provides some of the strongest privacy protection available among today's circumvention technologies.

on their mobile phones, and 41.8% of all respondents have done so in the past month.

The majority of respondents have used circumvention tools on their mobile phones, and many are current users. In the mobile context, a centralized infrastructure keeps track of which information is routed to or from each individual device. This difference could make it easier for the Chinese regime to *segment* business versus consumer mobile traffic, compared to the challenge of segmenting wireline traffic. Usability and interface concerns are also different (and often more challenging) in the mobile context. This suggests that user experiences (and technology risks) related to mobile devices should be a focus area in future studies.

Similarly, our qualitative data collected from various social media platforms, including the GFW Blog[16]—a popular and trusted source for censorship circumvention information—shows strong unmet demand for effective circumvention tools for mobile devices, including iPhone, iPad, Android, and Windows mobile devices. Our survey did not focus on specific mobile user experiences, but this could be a fruitful area for future work.

WHY USERS CIRCUMVENT

In all three seed groups, the same three reasons for wall-jumping were most often cited, in the same order of frequency (Figure 2.2). (These findings are also consistent with the Ng survey described on page 16 below.) First, to access Google or other search engines blocked in China; second, to use Twitter, Facebook or other blocked social networking sites (often to reach other mainland Chinese users); and third, to read foreign news sources such as the New York Times. These results suggest that the role of circumvention tools may be far broader than simply helping people access particular censored content—the tools are also useful (perhaps mostly useful) for people making apolitical uses of the platforms and services that are blocked.

Interestingly, the two options related to private communications placed last on our list of user motivations. Many tools rely on encryption to circumvent censorship controls, and such encryption incidentally provides privacy benefits. However, our survey suggests that the vast majority of users adopt circumvention tools in order to gain access to blocked or filtered websites, and are not acting primarily

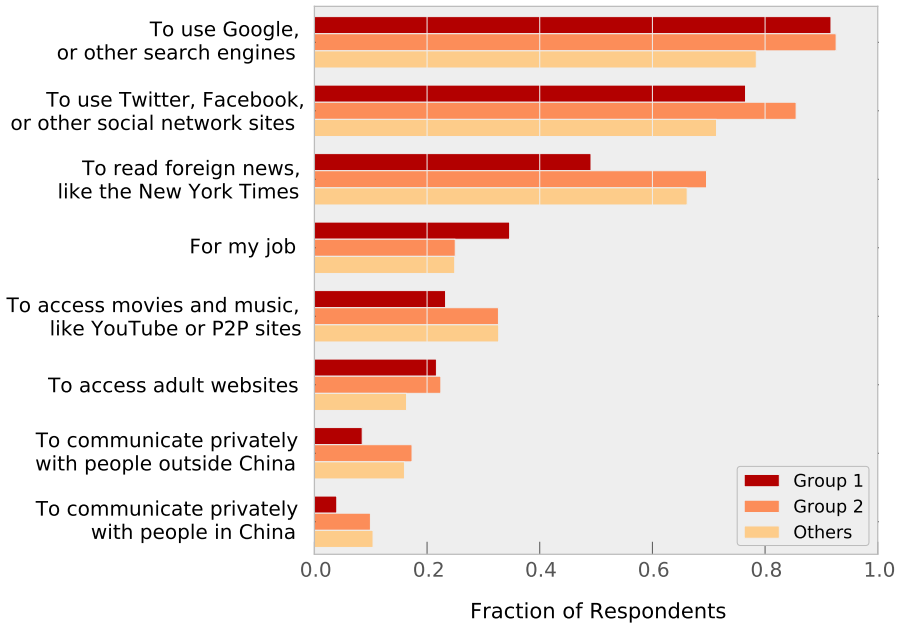

FIGURE 2.2 **What are your main reasons for bypassing the Great Firewall?** *(Select any that apply.)*

out of privacy concerns. Communications on social media may, in fact, be private, but our results suggest that users' primary goal is to use social media, rather than to communicate privately. We believe there is an important group of high-risk users (such as journalists, dissidents, and activists) who require strong security and privacy in their circumvention tools—a group that may be underrepresented in our sample because they are less likely to take surveys like ours. But we also believe, as described below, that these users likely make up a small fraction of all circumvention tool users in China.

COMMON PROBLEMS

Asked what was the most important problem in general with circumvention tools, our respondents were roughly equally likely to pick reliability and speed (Figure 2.3). But when asked what factor motivated them to choose the particular circumvention tool they use most often, our respondents cited reliability more often than any other factor, more often even than speed (Figure 2.4). This suggests that for users of today's tools, differences among tools in reliability are

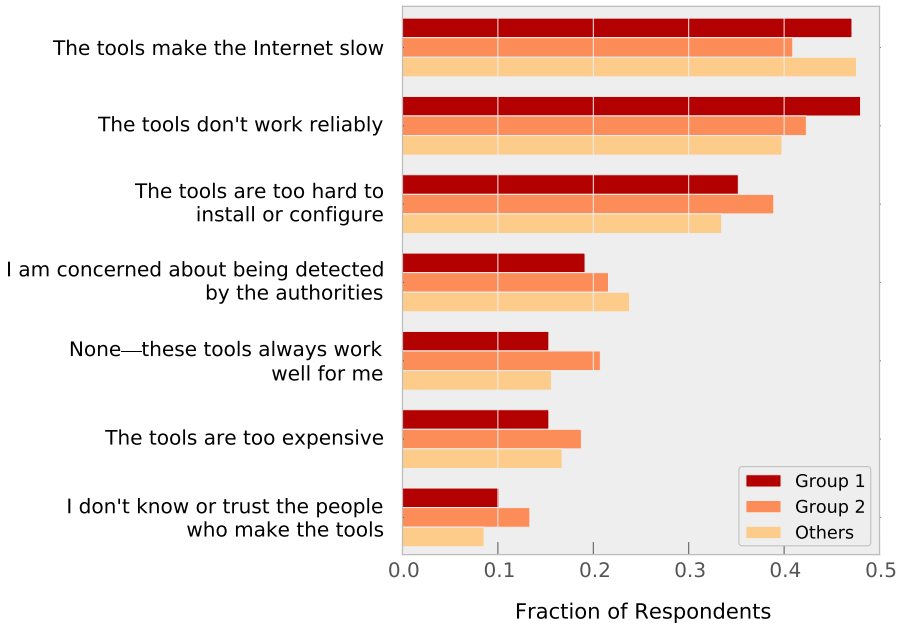

FIGURE 2.3 **In your experience, what is the most important problem with circumvention tools in general?** *(Select any that apply.)*

slightly more important than differences in speed. After reliability, the next two most common reasons for preferring a favorite tool were the speed of the tool, and its ease of configurability.

Few respondents indicated that they base their choice of tools on which toolmaker they trust the most, or on which tool their friends use. The relatively low importance of trust as a factor in choosing tools matches our other findings: Most respondents are concerned with speed and reliability, seek to use the uncensored web for purposes that may be unlikely to attract government attention, and do not cite private communication as a motivating goal. One possibility consistent with these answers is that users may understand that surveillance is a pervasive part of life in China—and may believe they are still subject to surveillance when they use circumvention tools to access the global Internet. There is some basis for such a belief—a topic mostly beyond the scope of this report. As one example, it became clear in 2008 that the Chinese version of Skype (distributed with the help of a Chinese joint venture partner, TOM),[17] retained logs

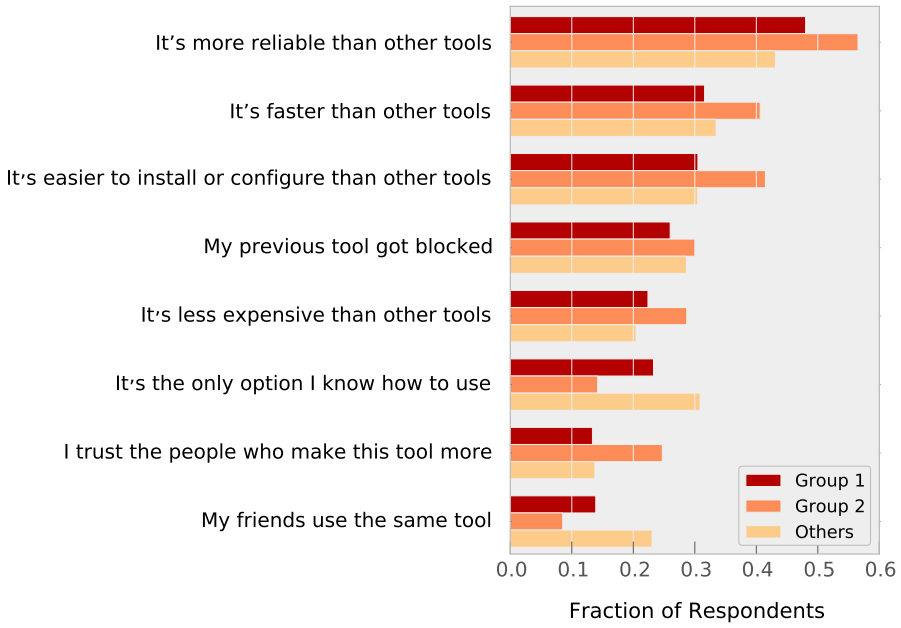

FIGURE 2.4 **Think about the tool you use most often. Why did you choose this tool?** *(Select any that apply.)*

of user text messages on politically sensitive topics, presumably for the benefit of the authorities.[18]

We gave users a freeform "other" box to provide details about the problems they've experienced, and reliability was a recurring theme. One wrote that "the tools are constantly being blocked and therefore I need to change tools frequently;"[19] another complained that "the tools are frequently being disconnected";[20] another that "VPNs are being constantly and easily disconnected—there are no reliable tools."[21]

HOW USERS LEARN ABOUT TOOLS

Since online information related to circumvention tools can be censored by the government,[22] we imagined that users in China would have difficulty finding out about tools, and resolving problems with the tools they use, via the Web. We hypothesized that many people would learn about circumvention tools through word-of-mouth, from their more tech savvy friends, family members or co-workers. But

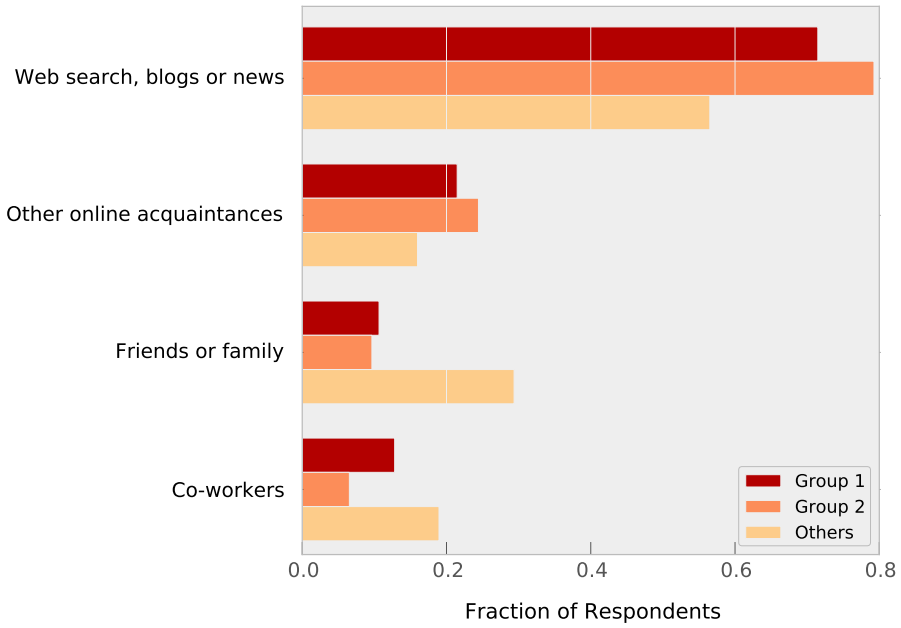

FIGURE 2.5 **How did you learn about the first tool you ever used?** *(Select any that apply.)*

these notions were not supported by our survey results. We asked users two questions: how they learned about the first tool they ever used, and where they turn when they encounter problems with the tools they use.

A wide majority of our respondents said they found their first circumvention tool through web search, blogs or news (Figure 2.5). Once they had their first tool, most respondents continued to use these online media to resolve ongoing configuration issues (Figure 2.6). So despite the efforts by the government to block information about circumvention tools,[23] Internet users in China are still widely able to perform self help, and find useful information independently online. This may mean that the censorship blocks are incomplete, and prohibited information is still leaking through the Firewall. Or it may mean that users have access to multiple avenues of circumvention, allowing them to use one tool to diagnose the problems they are facing with a different tool. Users in our sample have certainly used a range of tools: the median respondent has used four different types of circumvention tools. In any event, these results suggest that

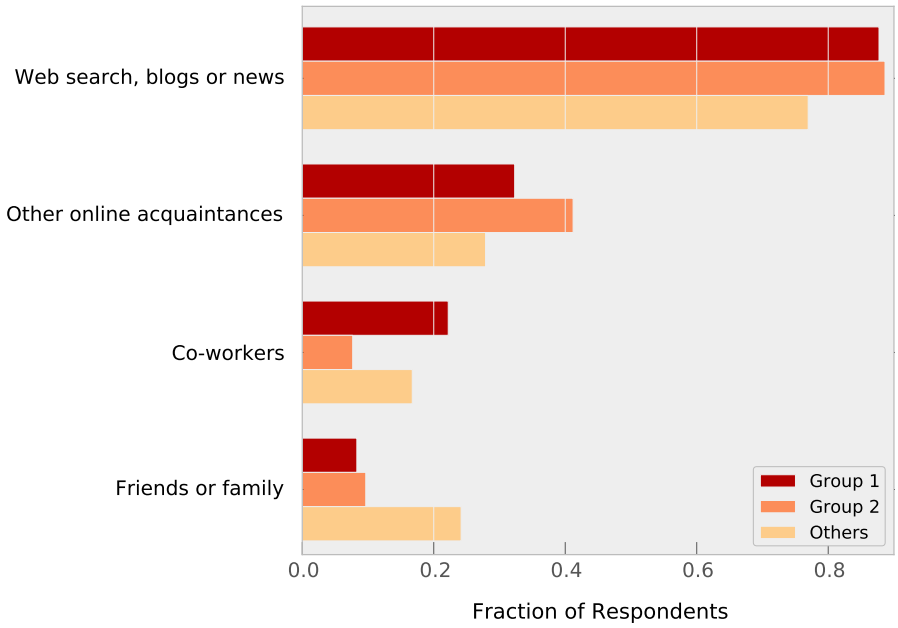

FIGURE 2.6 **Where do you turn for help when you have problems with circumvention tools?** *(Select any that apply.)*

circumvention software (and guidance about how to use it) is, and ought to remain, widely distributed on the Chinese-language Internet.

POLICY PREFERENCES

At the outset of this project, many of the sources and experts we consulted pointed to what they described as a common American misconception about the GFW. Americans, they told us, often imagine that the GFW simply blocks Chinese peoples' access to foreign media—but in fact, the main impact of the firewall is to make it harder for Chinese users to communicate with each other, by trapping them on a censored domestic Internet, and the main reason they circumvent the firewall is to communicate with one another.

We hoped to shed light on this issue by asking our respondents about their priorities: If they could decide either to end the GFW's blocking of foreign sites, or else choose to remove the censorship controls on domestic Chinese sites (but could not do both), which change would be more valuable? We hypothesized that if users cared mostly about

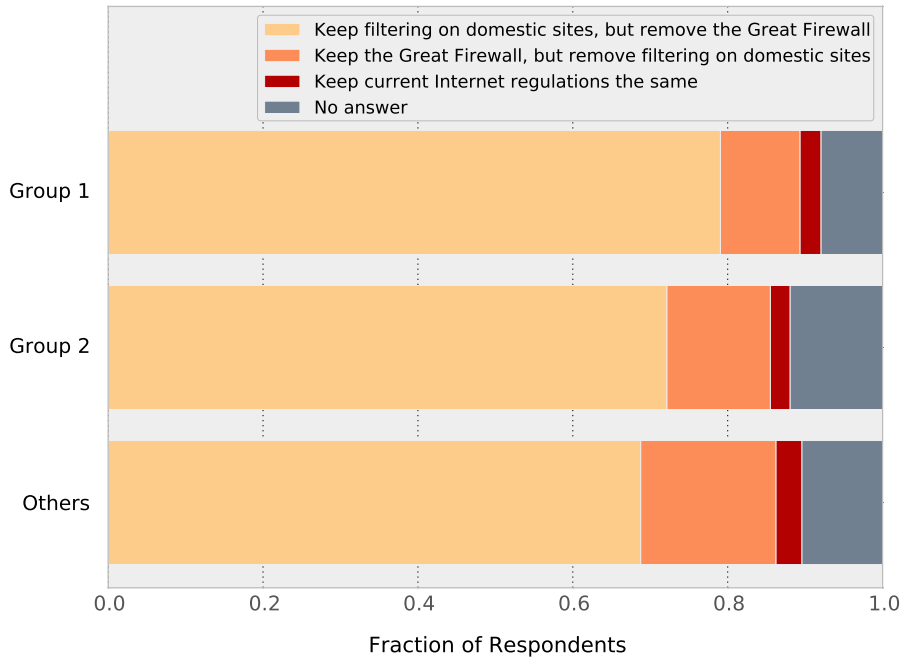

FIGURE 2.7 **Of the following three policies, which option would you most agree with?** *(Select one.)*

communicating with each other, they would sooner see domestic controls ended than see the GFW removed. We purposely did not offer a fourth option of removing both the Great Firewall and filtering on domestic sites, because we wanted to find out which of these two policy changes was more important to users.

In fact, an overwhelming majority (74.6%) of our respondents said they would prefer an end to the firewall, rather than an end to controls on domestic social media. As shown in Figure 2.7, this was consistent across all three response groups.

We see two potential explanations for this initially surprising finding. First, our framing of the question reflected an incorrect assumption: If a user's main goal, in circumventing the GFW, were to communicate freely with others in China, then (we assumed) the user's top policy goal would be an end to domestic censorship rather than an end to the GFW. We thought users would be particularly eager to see the leading

Chinese social media platforms shed their censorship, since this would allow free communication with the broad Chinese Internet population, and not just the handful of other Chinese who have circumvented the GFW to get to Twitter or Facebook. But users may already be comfortable with their level of access to social networking, *e.g.*, holding both a censored account on Sina Weibo and an uncensored one on Twitter.

Second, the data may mean exactly what it says—perhaps Chinese users of circumvention tools do not want domestic controls removed. This finding, if accurate, would match the results of the Jason Ng survey described in the next section, in which a plurality of respondents said the GFW should be maintained through official, open policy rather than in secret, but that it should still exist. Mr. Ng himself, in explaining his results, publicly identified with this group, writing that "personally, I was among the 50% of respondents who felt that the policy should have clear public standards, and not be based on the emotions of Chinese authorities."[24]

This question proved confusing to users, however, and was the only one on which we received significant feedback outside of the survey responses themselves (via e-mail and social media commentary on our survey). A number of users complained that the question did not allow them to register their preference for both the GFW and domestic social media controls to be ended. Typical of these responses was one user who wrote that "I have just completed the survey, but I'm not happy with one of the survey questions on China's Internet censorship policy. The question was asked if China should keep the Great Firewall or keep filtering on domestic sites, but I strongly believe that [Chinese government] should remove both [the Great Firewall and filtering on domestic sites]!"[25]

COMPARING OUR FINDINGS WITH EARLIER RESULTS

Earlier China Findings. We found two previous surveys of Chinese users' experience with censorship circumvention tools, one conducted by Freedom House in 2011 and the other by Chinese blogger Jason Ng in 2010.[26]

The Freedom House study surveyed users in several countries, including China, and asked them to rate their experiences with particular circumvention tools on a number of different dimensions, including

speed, security and ease of use.[27] We have only a limited ability to evaluate this study's conclusions or compare them with our own, because the published report offers limited insight into what data was gathered and how it was analyzed.[28] The report does share two overall findings about the worldwide user experience of circumvention tools, both of which are consistent with our findings in China. First, "users generally indicated a preference for speed of operation over security and anonymity of the[ir] communication."[29] And second, "the majority of users appeared to receive their circumvention tools through websites."[30]

More detailed results are available from a 2010 project by Jason Ng, an entrepreneur and activist in Beijing.[31]. He reported his findings in a Chinese-language blog post that did not receive extensive attention from Western audiences—although its core findings were translated and blogged in English by Global Voices.[32] Mr. Ng sought respondents for his study via social media, drawing about 5,400 responses. In describing his results, he was careful to point out that his effort (like our own) cannot claim to be a representative sample. Half of his respondents were students and another 15% were employed in the technology industry. Fully 92% were men. 77% of his respondents were between the ages of 19-28, and 73% already have a university degree (implying that at least a quarter were current graduate students).

The central finding of that study, consistent with our own results, was that the three leading reasons for users to circumvent the firewall were for web search, social media, and foreign news, in that order. Eighty percent of respondents said that they circumvented the firewall in order to use uncensored search engines such as Google, and 75% said they used circumvention to access social media sites such as Twitter. 72% of those in his sample used circumvention technology to access foreign news sources—a greater fraction than in our own results.

Most of his respondents—71%—said that they use a dedicated cir-

cumvention tool such as Freegate, **UltraSurf** or **PUFF**. 37% said they used **web proxies**, 24% used **SSH**, and only 16% used personal VPN service (while only 5% reported that they used their company's VPN). 15% used an option not listed—many of those, Mr. Ng reported, were using GAppProxy, a predecessor of the GoAgent tool that dominated our own survey results.

These results, gathered in April 2010, notably do not conform to the collateral freedom pattern we found in our own survey. Instead, Mr. Ng's respondents relied heavily on purpose-built circumvention tools. Time may be part of the answer: just a month before Mr. Ng's survey, Tor reported that the Chinese authorities were "getting better at blocking Tor," and noted a steep decline in China-based usage.[33] Similar changes may have impacted other dedicated tools around the same time.

Two thirds of these users said they relied on circumvention technology every day, 8% every other day, and 17% 1-3 times per week. Most (52%) had been using circumvention tools for less than three years. Only 12% paid more than 10 yuan per month ($1.61) for their access—the 88% who paid 10 or fewer yuan may have been dominated by users who rely on free services.

One concern of Mr. Ng's was how few people in mainland China even know about the existence of the GFW, let alone knowing or caring about ways around it. In his survey, he found that nearly all of those 2010 respondents, 85%, reported that they had taught friends about the existence of the GFW and the availability of circumvention

---

UltraSurf (`ultrasurf.us`) is another purpose-built circumvention tool produced by the same team as Freegate (a group of primarily Falun Gong practitioners called the Global Internet Freedom Consortium).

PUFF offers free and commercial "secure proxy software & service" that uses either the SSH or VPN protocol. It is produced by an entity called erights.net.

web proxies are web sites—which users can visit with any web browser—that have not *themselves* been blocked, but that automatically retrieve and republish whatever censored content a user requests. If `proxy.com`, for example, were the address of a web proxy—and Radio Free Asia's `rfa.org` the address of a blocked web site—then a user might be able to reach RFA by browsing to `proxy.com/rfa.org`.

SSH or Secure Shell is a cryptographic protocol most widely used for direct access to the text-based command prompt of a remote computer system. It can, however, also be used to encrypt and carry other traffic, such as web traffic, if the user's computer and the server are specially configured to allow this.

technologies.

The survey also asked its users for an overall opinion of China's Internet policy. A near-majority 48% said that censorship was acceptable if carried out in accordance with published regulations or laws, rather than "behind closed doors." 38% favored total removal of the Great Firewall, and 8% were in between, expressing the view that moderate censorship would be acceptable but the GFW goes too far. Just two percent of respondents favored the status quo.

Global Experiences with Circumvention Tools. For the global state of Internet censorship and of circumvention tools, the most useful research comes from Harvard's Berkman Center on Internet and Society. This work grows out of Berkman's OpenNet Initiative, which is the leading observer of Internet censorship policies and technologies across the world.[34] Rather than focusing on direct interaction with Internet users, these studies have sought information primarily from other sources, such as field tests by researchers, surveys of the tool developers themselves, and some indirect indicators (such as the relative popularity of different search terms in different jurisdictions). The Berkman team's series of investigations of how well circumvention tools work around the world—including, specifically, how well such tools work in China—have generally confirmed the impression that circumvention tools are frustrating and do not work reliably.[35]

The key insights from these Berkman studies are how *few* people actually use censorship circumvention technologies of any sort, and among such users, how few install special-purpose circumvention software. A 2010 analysis attempted specifically to gauge the usage rates of particular circumvention tools around the world, including not only purpose-built tools like Tor, but also more general-purpose tools such as VPNs and simple web proxies.[36] The usage estimates in this study were created using a heterogeneous mixture of different methods, including 134 survey responses from the makers of various VPN services and other tools, an analysis of Google AdPlanner traffic estimates, and an analysis of search traffic using Google Insights.[37] The analysis found that "even given the large margin of error for our estimates, usage of all of the tools described here is very small compared to . . . the population of users in countries that aggressively filter the Internet,"[38] and said the overall number was "likely considerably less" than three percent of the Internet users in heavily filtered countries.[39] The team's most recent report, in 2011, concluded that

"the percentage of Internet users in less open societies using these tools could be as low as 1%."[40]

A second major finding from the Berkman studies is that across the world, including in China, "[m]any more users use simple web proxies than use either blocking-resistant tools or VPN services."[41] This estimate of simple web proxy usage comes from two sources—Google AdPlanner estimates of the traffic to each site, and search trends data about the large number of users who search for "proxy" and related terms using Google. [42]

Berkman's finding implies that after all the users of more complex circumvention technology are accounted for, there remains a very large group of simple web proxy users who must not be employing other tools. In fact, only 15 respondents—out of the 1,175 circumvention tool users in our sample—told us that web proxies were the *only* circumvention tool that they had ever used. Likewise, the 2010 Ng survey did not find many such respondents. Most of the users in both survey groups had used a variety of tools.

We believe this is most likely a sampling effect, and that it points to a core ambiguity in the community's discussions—it may be confusing to describe every user of a simple web proxy as a "circumvention tool user." Simple web proxies can be accessed by browsing to a specified web page, without any special software and perhaps without even a deliberate plan to use a proxy—web links may automatically send users through a proxy to get to a site outside the GFW. There may be a large number of Chinese Internet users who know that the GFW exists, do not bother with or feel comfortable using special circumvention software, and who (when they seek to access something they believe is blocked) respond by searching for a simple web proxy. But a still larger group may simply be following proxied links to censored content, without even knowing that they are engaged in circumvention. These users are simplicity-first users—they will circumvent only if the circumvention process is trivially easy (or even invisible) to them. These users are unwilling to install or use special software, unlike the IT industry workers and younger, tech-savvy students so heavily represented in both our survey and Jason Ng's.

At the same time, a separate Berkman study of a particularly high priority group—244 Global Voices bloggers, many of whom are high profile citizen journalists in filtered countries—found that 79 percent

of the group relied on circumvention tools.[43] These bloggers rated privacy as the most important aspect of circumvention tools (a stark difference from our sample), and speed as the worst performing aspect.[44] They are what we would term privacy-first users.

Why are usage numbers so low? Berkman in 2011 wrote that one reason for low uptake may be the user experience—the Internet as a whole is much slower and less reliable when using such a tool than when not—but "[a]n alternative explanation for relatively low use of circumvention tools is that the tools do not meet one of the major needs of users: creating content on local platforms for local audiences."[45] In our own view, it is the local *audiences* that are likely the most important factor—reaching them, via whatever platform, appears to be a key motivation for many users.

3 IMPLICATIONS FOR INTERNET FREEDOM IN CHINA

Key Questions for Funders

1. What is the collateral cost to China of choosing to block this tool?
2. Who is this tool for—users who put *versatility* first, those who put *simplicity* first, or those who put *privacy* first?

The Internet freedom community faces a fundamental question in China, as it does around the world: What are the human needs of censored users, and how can we best meet those needs?

This study helps answer both parts of that question. Our results suggest there are three distinct groups of Chinese circumvention technology users, each with its own defining need—versatility, simplicity, or privacy. For most of these users, Internet freedom is collateral freedom, available when and where it is inseparable from China's economic growth. Collateral freedom is a pattern that helps explain many recent events, and—once recognized—it suggests promising new approaches for supporting Chinese Internet freedom.

COLLATERAL FREEDOM MATTERS **Most Chinese users need circumvention tools that are hard to *segment* from economically valuable activity, not necessarily tools that are hard to block.**

The conflict between China's censors and the circumvention community is, on its face, technological: Circumvention tech developers find new ways around the GFW, and censors adapt in response.

But China's strategic economic interests play a crucial role in moderating its censorship tactics. In contexts where Internet freedom is inseparable from commerce, the authorities most often allow a measure of both: they tolerate some circumvention as the price

of doing business. The censors are at their most aggressive when censorship carries low economic cost—and they are relatively more constrained when censorship entails economic damage.

Just as the authorities work to separate and censor civic and personal communication while allowing a free flow of business information, the circumvention community could work to do the opposite, integrating these uses so that China (and other Internet censoring countries) cannot have one without the other.

Earlier writers have highlighted the overall tension between authoritarian control and Internet-driven economic growth. For example, Daniel Anderson has written that although the regime cares about censorship, "economic development is equally critical (if not more so) to the stability of the Chinese government. It cannot cut off the physical link to the Internet completely lest it block business traffic (such as HTTPS or VPN)."[46]

Based on direct evidence from users, we are able to strengthen and sharpen these earlier claims. The correspondence between censorship circumvention and business goes beyond just using the same Internet, or even the same protocols. It extends to using the same platforms and services. The more closely a circumvention tool, technique, or practice integrates itself with business traffic, the better it is likely to fare in China.

The collateral freedom dynamic helps explain a number of recent developments in Chinese Internet freedom. For example:

- GoAgent's use of Google's platform makes commerce and Internet freedom a package deal for the Chinese authorities.[47] Chinese censorship of Google's platform—although far from complete—has increased in recent months, possibly in part as a reaction to GoAgent. A recent Wall Street Journal report highlighted the toll on business: "increasingly unreliable connections to Google in recent months have hindered downloads and sharply reduced the effectiveness of [its] instant-messaging service . . . Unstable connections to Google's Gmail service have forced [one executive] to set up a system that forwards his email to multiple services to ensure its delivery."[48] These concerns are widespread: A 2012 survey of 325 American executives in Hong Kong found that 72% believed "slow or unstable Internet access

impede[s their] ability to efficiently conduct business in China."[49] Degraded service and "instability" are hallmarks of the GFW, side effects of an infrastructure that examines nearly all Internet traffic crossing the country's border. Sixty-two percent of the executives agreed more specifically that the blocking of search engines has a negative impact on their "company's ability to conduct business normally" in China.[50]

- The Chinese government's intermittent disruption of VPNs appears to be a balancing act between censorship and commerce. In late 2012 (around the start of China's 18th Party Congress), several of the leading consumer-facing VPN providers began to report protocol-level blocking of VPN services, which made VPNs less reliable, at least for non-business users.[51] The government has shown that it can block these networks at the protocol level, but chooses to disrupt them only intermittently. The blockages, which have reportedly increased in the last few months, are taking a toll on international businesses.[52]
- New government policies will help censors separate circumvention-related VPN usage from business usage. For example, a new real name registration requirement for consumer-facing online businesses (including consumer-facing VPNs) will make it easier for the authorities to identify consumer-oriented VPN services, and filter them while continuing to allow unfiltered VPNs for business use. At the same time, the authorities have reportedly pressured some multinational firms to install police-controlled monitoring and filtering equipment inside their corporate VPNs.[53]
- Tor, a powerful tool with minimal commercial impact, has a distinctive network signature and is blocked throughout China. The Tor team's next move is a tool that will make it harder for censoring regimes to single out Tor traffic.[54] Another project, called **Telex**, uses a similar strategy, by making sensitive connections look innocuous to the censor.
- GitHub, a secure and widely used web site where programmers work together on source code, was briefly blocked in China in late January of 2013, likely because of one or more specific users who had posted unwelcome information on the site.[55] This caused an outcry among Chinese programmers, who rely on access to

---

Telex (`telex.cc`) is a research project from the University of Michigan. The project's approach is to build anti-censorship technology into the network infrastructure, with the cooperation of large intermediary ISPs in freedom-respecting jurisdictions. It uses a technique called *public key steganography* to hide Telex traffic in plain sight.

the site for local (and worldwide) collaboration.[56] In the end, the authorities backed down, restoring access to the site.[57] Because `github.com` is secured with HTTPS, the Chinese were unable to block the particular page that they were concerned about. Chinese officials had to allow all or none of GitHub through the GFW—and they chose to allow all of it.

CHINESE USERS ARE DIVERSE **Different Chinese users of circumvention tools have different needs: versatility, simplicity, or privacy.**

Considering our survey results alongside the earlier Berkman and Ng studies, we conclude that there are **three distinct groups** of circumvention tool users in China:

Versatility-first users are a young, motivated, technology-savvy population, including the respondents to our survey. They want to take advantage of the full range of Internet technologies—using globally popular social media tools and video streaming sites, and doing other complex tasks that require a technologically versatile connection to the global Internet. Copies of censored static content, even if widely available, would not meet their needs. They will install special software and learn new skills in order to obtain Internet freedom that is as reliable and fast as possible, so they can conveniently access social networking and rich media such as video. But their purposes are not expressly political, and they are for the most part unafraid of being surveilled.

Simplicity-first users are the lion's share of people who ever access censored content in China. They do not rely on special-purpose tools, and may not even consider themselves "circumvention tool users." For them, circumvention is worthwhile only if it is as simple as browsing to a different web page.[58] People in this group (and similarly situated people in other censored countries) account for the Berkman team's finding that "in aggregate . . . usage of simple web proxies is at least an order of magnitude larger than use of blocking-resistant proxy tools but is still a very small portion of all Internet users."[59] Many in this group may not even realize that they are browsing through a web proxy (if, for example, they arrived at the proxy by following a link to a particular piece of content).

Privacy-first users are the smallest group, though a very important

one. This category includes journalists, bloggers and dissidents who are doing politically sensitive work and have reason to be concerned about official reprisal. This group simply cannot enjoy Internet freedom unless their circumvention tools afford them strong privacy guarantees.

These categories are not absolute, and they do not describe everyone. But we believe they are a helpful framework when thinking about how best to meet user needs. Users in each of these three groups will go without Internet freedom unless their defining need is met. Each group *requires* one of these three traits—simplicity, versatility, or privacy. To evaluate a China-focused circumvention tool, or a policy strategy, one should first understand which users—and which needs—are being targeted.

To the extent that our results are indicative of the large versatility-focused group of circumvention tool users (who represent most of those willing to install circumvention software), it appears that purpose-built anti-censorship platforms lacking a significant commercial footprint are not the right solution for this group. Such platforms often must sacrifice versatility in order to evade censorship and protect privacy. (Tor, for example, provides strong privacy guarantees, but relies on techniques that also make the Internet connection much slower.) Commercial platforms like VPNs or the cloud infrastructure under GoAgent, on the other hand, not only need to exist, but need to function well, in order for China to prosper.

AREAS FOR FUTURE WORK

1. Map the circumvention technologies and practices of foreign businesses in China. For international business, some amount of circumvention is mission critical—and the commercial mission is one the Chinese authorities do not want to disrupt. This points to a range of circumvention-enabling tools, platforms, and services that are partly insulated from censorship for economic reasons, such as corporate VPNs, uncensored cloud hosting platforms, and secure mobile devices for employees in the field. Which tools do businesses rely on for uncensored, secure communication, who provides those tools, and how well do they work? Can more circumvention technologies be enabled on or through them? As cloud services become more common, are there more emerging opportunities analogous to

GoAgent—situations where an individual user can access business-class IT infrastructure?

2. Engage with online platform providers who serve businesses in censored countries. There are a number of global online platforms, based in relatively freedom-respecting jurisdictions, that have become indispensable for a growing range of business users around the world—including, in some instances, local businesses in Internet-censoring countries. Google's cloud infrastructure, on which the GoAgent software relies, is one example, and GitHub is another. Neither of these companies has an operational presence on the ground in mainland China, but both have something more important: business users there (both local and foreign), whose connectivity the Chinese government has reason not to disrupt. Circumvention technology developers might be well advised to seek out such platforms, and look for ways to enlist them as forces for Internet freedom.

3. Investigate the collateral freedom dynamic in other censored countries. China is not the only country that maintains an unfree Internet while seeking investment from Internet-reliant global businesses. Vietnam, in particular, "continues to expand and strengthen [a] pervasive regime[] of Internet controls"[60] even as it competes with its regional neighbors (and other developing countries around the world) for foreign investment. The same dynamic may apply there: whatever else the regime does, it *must* allow robust Internet connectivity for foreign businesses. Other Internet-censoring countries that undervalue economic growth (like Cuba or North Korea), or that have major reserves of strategic natural resources (such as Iran or the Persian Gulf states), may be insulated from this dynamic.

4. Diversify development efforts to match the diversity of user needs. Much of today's circumvention project funding is tailored to the needs of privacy-first users. These investments are valuable, but our survey also suggests that other important needs may now be under-funded. Anti-censorship solutions that provide connectivity fast and reliable enough for the versatility-first group of users could powerfully enhance Internet freedom in China, even if such tools did not provide their users with enhanced privacy or a simple installation experience. Not every tool in the circumvention ecosystem should cater to the privacy and safety needs of the highest risk privacy-first users. By matching its design constraints to user

needs, the community will help Chinese users achieve the goals that they themselves consider most important. At the same time, tools that do not address privacy or security risks must make these limits clear to their users.

5. Make HTTPS a corporate social responsibility issue. The recent GitHub experience holds a powerful lesson: When commercially significant online platforms require encrypted connections—so that blocking them becomes an all or nothing choice—they can advance Internet freedom. Beyond the many other advantages of heightened security, this is a further reason to make encrypted-only sites a norm among companies. Important efforts already being made in this area (including the "HTTPS Now"effort jointly organized by the Electronic Frontier Foundation and Access Now) deserve support.[61] This goes beyond simply making HTTPS an *option*. We believe these benefits come from sites making secure web connections be the *only* way they can be reached from Internet-restricting environments. (At the same time, important challenges remain with HTTPS, and it is essential that the community keep working on those issues.[62])

4 CONCLUSION

The essence of the Internet freedom debate in China is segmentation, not blocking. When crucial business activity is inseparable from Internet freedom, the prospects for Internet freedom improve.

This fact may, however, be a double-edged sword. If the amount of circumvention that happens via a business-serving platform goes up, so too may that platform's risk of being blocked by the authorities. Some users of business-facing platforms in China have expressed frustration at this risk, and urged that these platforms not be used to run censorship-circumventing proxies.[63]

One response to these concerns would be to back away from using business-serving platforms as censorship circumvention resources. But, we would argue, a healthier response might move in the opposite direction, toward even *greater* integration between Internet freedom and business. Rather than working with particular online platforms, which may be individually vulnerable to censorship, the best long term answer might be to move anti-censorship deeper into the network infrastructure, incorporating it within the systems that large network operators use to exchange their traffic. Ideally, we might aim for a situation in which secure web access generally (rather than access to any particular platform) is inseparable from Internet freedom.

To the extent that specific business functions can be made inseparable from Internet freedom, this may also strengthen the policy argument that the GFW is a trade barrier inconsistent with China's WTO commitments.[64]

We hope this report will help spark discussion, debate, and further improvement for all stakeholders in the circumvention community—funders, developers, and most of all, censored users themselves.

A SURVEY METHODOLOGY AND DESIGN

Deciding to Conduct a Survey. Our objective was to study users' on-the-ground experiences of circumvention technology in China. We sought to build the evidence base, using the most robust techniques that were feasible in this challenging environment.

We began with an initial canvass of the Great Firewall Blog, a leading meta-blog that collects other online discussions of censorship circumvention tools from around the Chinese language web. We reviewed more than 350 posts published since May 20, 2012. This gave us a valuable inventory of recently used tools and services, while at the same time highlighting the need for a systematic, user-focused investigation of conditions on the ground. The blog posts (and comments on them) reflect individual user experiences with particular tools. To learn more about the experiences of the population as a whole, or to get a sense of what was typical, we would need to gather new data.

We decided to design and build a new survey instrument that would reach out directly to Chinese users of circumvention tools and ask them, in Chinese and through the Internet, to briefly share their experiences. We chose a structured approach, with multiple choice questions to allow for comparison and analysis. And we wanted the survey itself to have a very smooth user experience, taking at most five minutes to complete.[65]

Safety and Security. We were highly concerned about our respondents' security and privacy, given the obvious sensitivity of the topic at hand. We were mindful of the possibility that users, responding to our study, might attract negative attention or suffer negative consequences from the Chinese government. We took several steps designed to assess and mitigate this risk:

- **Gathering expert input** from others who work on Internet Freedom in China, including NGO leaders and businesspeople.

The message from these conversations was clear and consistent: risk can never be totally eliminated, but a user's decision to circumvent the Great Firewall is generally not, in itself, enough to attract negative attention from the authorities. Circumvention is sometimes cited as an additional infraction, when Internet users have gotten themselves into trouble for something else, such as having written objectionable content. But circumvention tool use, the subject of our study, was not in itself a dangerous topic for individual users to discuss.

- **Limiting data collection** to the things we actually wanted to know. We did not gather the names, email addresses, or social media pseudonyms of our respondents. We assured our respondents, at the beginning of the survey that: "Your responses are private—we will not ask you for identifying information."
- **Encrypting the survey web site.** Our survey was available only over encrypted web connections, meaning our respondents' answers would be not be visible to network intermediaries.
- **Limiting data release.** This work is driven and deeply informed by a strong commitment to openness. However, we have decided not to release our raw results, in order to forestall the possibility that respondents might be reidentified through cross-referencing with other information. We are glad to allow other researchers to analyze our raw data, subject to appropriate safeguards, and would welcome inquiries on this front.

We were also concerned that our survey itself, which we hosted on a U.S.-based Rackspace server, might be blocked by the Great Firewall. We had a contingency plan in place to establish a new server at a different location, if we were to be blocked. Fortunately, we have had no indication that the survey was ever blocked in any part of China.

Survey Design: Arriving at a Snowball Sample. Finding our sample of respondents, and motivating them to take the survey, were our central challenges in this effort. We did not have any method for choosing circumvention tool users at random. Nor does anyone know enough about Chinese users of circumvention tools to know which demographic markers would be characteristic of a representative sample.

We canvassed the social science literature, and consulted with experts in surveying hard to reach populations—heavy drug users, sexual

minorities, and other groups for whom a statistically representative sample is not available.

A common method for such groups is **snowball sampling**. A snowball sample starts with "seed" respondents, members of the target population who are already known to the researchers. Respondents who have completed the survey are then encouraged to invite other people they know, who are also in the target population. (Those respondents, in turn, are encouraged to invite their own contacts.) This technique lets researchers find new members of the target group as successive waves of respondents take the survey. Snowball sampling produces a non-statistical convenience sample. Results gathered this way cannot be assumed to be representative of the target population, but researchers can compare successive responses recruited by a particular seed to see if answers converge over time (suggesting a stable sample of that particular seed's network, as to a particular question). Each seed who recruits others becomes a cluster of responses, and where responses are consistent across clusters, this provides some reason to believe that similar responses might be found across a sample of the population as a whole.

A more recent advance on snowball sampling, feasible only under certain limited conditions, is **respondent-driven sampling** (RDS).[66] RDS starts with a convenience sample, but carefully controls the recruitment and referral process. Each respondent is recruited via a unique coupon (and is provided with a set number of her own coupons she can give out to additional members of the target population). This allows researchers to reconstruct the "referral chains" of who referred whom, and it limits the importance of any one person in the overall results. Long referral chains reduce the bias introduced by the initial choice of seeds. If the results from successive "waves" of respondents settle in to an equilibrium (which can be rigorously defined), then those results may be able to be generalized to the whole population. Both snowball sampling and RDS were developed in the offline context, though both have occasionally been used for online studies. RDS is particularly difficult to implement in the online context. It is natural online to share the same link with many friends, (whether via weibo, Twitter, email or otherwise). And a link received from one friend can easily be shared or forwarded to another. But RDS requires that no two respondents use the same ID number—which would have meant, in our case, that no two could use the same link (since the links embedded these unique IDs). Moreover, we would have had to limit

each respondent to recruiting only a fixed, small number of others.

Based on our early testing, we found that people were likely to complete the survey if they received it from a person they know and trust. Our seed respondents, motivated by a personalized appeal from one of the authors of this study, were generally happy to ask their contacts to participate. But those contacts did not, in turn, recruit many others. We decided to embrace a snowball sampling approach, which allowed each of our seeds to gather as many additional respondents for the study as he or she was able.

Our Approach to Incentives. Motivating users to take the survey was one of our primary concerns, particularly after seeking expert input on what might work best. One Shanghai-based management consultant told us flatly that there is no good survey data coming out of China—to the frequent disappointment of his data-driven American clients. The data, he said, is garbage: If you don't offer respondents an incentive, they won't participate—and if you do offer them an incentive, they will game the question. Another expert, a professional architect of Chinese consumer surveys, predicted it would be difficult for us to build trust with survey respondents, and encouraged us to consider offering material incentives.

After extensive thought, we determined that providing incentives over the web would be infeasible for this study. We did not want to know, or ask for, the identity or contact information of our respondents—both to protect their privacy, and because we feared that asking for identifying information would deter respondents from taking the survey. We were also concerned that providing an incentive (say, a coupon code for a one-month VPN subscription) could itself bias our sample, by drawing in participants who were particularly enticed by the incentive we were offering. In the worst case, spammers might provide fake answers—and pollute our data collection—in order to harvest the incentive.

Instead, we decided to take a soft incentive strategy. We sent each of our seeds a personalized note explaining what the survey was and why we needed their help to complete it. Once a user navigated to our site, we continued to focus on intrinsic personal motivations, highlighting the value and purpose of the feedback we receive. At the beginning of our survey, we made an altruistic appeal to potential respondents: "We realize that VPNs and proxies are often difficult to

use. We want to learn more about these challenges. By completing this survey, your input will help us make circumvention software better." At the end of the survey, we appealed again to respondents to forward the survey with their friends: "We are trying to gather input from a large and representative sample of circumvention tool users in China—and we can only do that with your help."

We also provided an informational incentive at the end of the survey, by displaying some interesting real-time statistics about the data collected so far. For example, we displayed the number of people who had already taken the survey, the reported usage rates of popular circumvention tools, and the most frequent concerns and problems faced when using these tools.

Our Data Collection Process. Once the survey was ready to launch, we compiled a list of 51 "seed" respondents, people who either live in China, or have close ties to people living in China. While this list represents a convenience sample of people who are among our team's personal contacts, we did attempt to choose a diverse set of our contacts, so downstream survey referrals would have a better chance of reaching into distinct subcommunities.

Beginning on December 3, we sent personalized e-mails to each of the seeds on this list, explaining in detail our survey goals, and asking them to take the survey (if appropriate) and share the survey's URL with their friends in China who also use circumvention tools. Each seed's survey URL contained a unique token, which allowed us to determine how widely the survey was spreading through each seed's social network.

We did not impose a quota on the number of referrals per survey. Instead, we simply asked our respondents to "please invite your friends to take this survey." We also did not specify exactly how our respondents should refer their friends—on the final page of the survey, we provided a direct survey URL, with a new unique token, that could be sent over e-mail, instant messaging or SMS. We also embedded four social media widgets under the direct survey URL—for Sina Weibo, Renren, Twitter and Facebook—with the same URL prefilled, to make it as easy as possible for our respondents to share our survey on their social networks.

We were careful to keep our survey as short as possible. Since we did

not provide hard incentives, we recognized that it would be difficult to convince strangers to complete a lengthy survey. We designed our survey to take less than five minutes. Indeed, the median survey completion time was 3 minutes and 37 seconds, and our completion rate was 78.1%—that is, only 369 respondents began the survey (i.e., got past the first page) but did not complete it. Overall, we received 6353 unique hits to our survey site, however we suspect that a large fraction of these hits were not actual humans: When a link is shared on Sina Weibo, for example, a Weibo bot will routinely visit the link to gather the site's title, description and images, so the shared linked will be usefully displayed on the social media site.

The survey was available in both Simplified Chinese and English, with the default language set to Simplified Chinese. We provided a language switcher at the top of the survey's landing page, but perhaps the switcher was not obvious enough. Of our completed surveys, only six respondents (0.45%) used the English version. This suggests that we may have missed out on sampling some portion of the ex-pat community living in China.

Our Sample. We collected 1319 completed survey responses, between Dec. 3, 2012 and Jan. 23, 2013. Of these, we filtered out any responses where:

- The respondent reported that he or she does not live in mainland China, and has not lived in mainland China for most of his or her life,
- The respondent's reported age is less than 10, or greater than 70, or
- The respondent reported that he or she has never used circumvention tools

In total, this meant filtering out 144 of the 1319 responses. The remaining 1175 responses were deemed valid, and our data analysis in the body of this report reflects those responses only.

Because relatively little is known about the overall population of circumvention tool users in China, it's difficult to assess the extent to which our sample is representative. Our sampling mechanism depended on how widely our survey was shared downstream through our respondents' social networks. Typically, it is instructive to look at

the length of referral chains to gauge the reach of the sample—with longer referral chains generally signifying broader, more representative, reach. However, in our case, we could not precisely determine the length of referral chains, because of the difficulty of tracking referrals in many social networking contexts. But, while we cannot say that our sample is representative of *all* Chinese circumvention tool users, we have collected a sizable cross-sectional dataset about an important subset of this population.

B SURVEY RESPONSE SUMMARY

For each question, we provide a table below that summarizes our survey response data. Each table separates the responses by the main seed group, and the sum of all respondents is shown in the righthand column. We gauge whether each trait in each group has converged to a steady level, where it is unlikely that additional data collection in each group would significantly impact our result. Formally, we follow the recommendation in the RDS literature[67] and define sample trait instability as:

$$\text{there exists } t < \tau \text{ such that } |\hat{p}_{(n-t)} - \hat{p}_{(n)}| > \epsilon$$

where τ = 50 and ϵ = 0.02. That is, if any of final 50 estimates differ by 2% from the final estimate, we flag the estimate as potentially unstable. In our survey sample, all of the traits for Groups 1 and 2 converged, and only a small fraction of the Others group traits did not. We mark those data cells in red in the tables below.

QUESTION 1 In what province do you live?

Answer	Group 1	Group 2	Others	All Respondents
Beijing Municipality	137 (24.7%)	57 (16.2%)	62 (23.0%)	256 (21.8%)
Guangdong Province	75 (13.5%)	55 (15.6%)	43 (16.0%)	173 (14.7%)
Shanghai Municipality	79 (14.3%)	48 (13.6%)	38 (14.1%)	165 (14.0%)
Zhejiang Province	62 (11.2%)	26 (7.4%)	17 (6.3%)	105 (8.9%)
Jiangsu Province	32 (5.8%)	25 (7.1%)	13 (4.8%)	70 (6.0%)
Sichuan Province	20 (3.6%)	23 (6.5%)	13 (4.8%)	56 (4.8%)
Hubei Province	13 (2.3%)	13 (3.7%)	11 (4.1%)	37 (3.1%)
Fujian Province	21 (3.8%)	10 (2.8%)	5 (1.9%)	36 (3.1%)
Shandong Province	13 (2.3%)	8 (2.3%)	5 (1.9%)	26 (2.2%)
Chongqing Municipality	7 (1.3%)	14 (4.0%)	4 (1.5%)	25 (2.1%)
Henan Province	14 (2.5%)	5 (1.4%)	5 (1.9%)	24 (2.0%)
Shaanxi Province	11 (2.0%)	7 (2.0%)	3 (1.1%)	21 (1.8%)
Tianjin Municipality	5 (0.9%)	11 (3.1%)	4 (1.5%)	20 (1.7%)
Other	4 (0.7%)	10 (2.8%)	6 (2.2%)	20 (1.7%)
Hunan Province	10 (1.8%)	5 (1.4%)	3 (1.1%)	18 (1.5%)
Anhui Province	7 (1.3%)	6 (1.7%)	4 (1.5%)	17 (1.4%)
Liaoning Province	5 (0.9%)	7 (2.0%)	4 (1.5%)	16 (1.4%)
Jiangxi Province	8 (1.4%)	2 (0.6%)	5 (1.9%)	15 (1.3%)

Hebei Province	7 (1.3%)	4 (1.1%)	4 (1.5%)	15 (1.3%)
Heilongjiang Province	6 (1.1%)	4 (1.1%)	4 (1.5%)	14 (1.2%)
Yunnan Province	4 (0.7%)	4 (1.1%)	1 (0.4%)	9 (0.8%)
Shanxi Province	5 (0.9%)	2 (0.6%)	2 (0.7%)	9 (0.8%)
Jilin Province	5 (0.9%)	1 (0.3%)	1 (0.4%)	7 (0.6%)
Guizhou Province	2 (0.4%)	4 (1.1%)	0 (0.0%)	6 (0.5%)
Hong Kong	0 (0.0%)	0 (0.0%)	5 (1.9%)	5 (0.4%)
Hainan Province	2 (0.4%)	1 (0.3%)	2 (0.7%)	5 (0.4%)
Gansu Province	0 (0.0%)	0 (0.0%)	4 (1.5%)	4 (0.3%)
Qinghai Province	0 (0.0%)	0 (0.0%)	1 (0.4%)	1 (0.1%)
Total	554 (100%)	352 (100%)	269 (100%)	1175 (100%)

QUESTION 2 What is your age?

Answer	Group 1	Group 2	Others	All Respondents
[25, 30)	219 (39.5%)	102 (29.0%)	80 (29.7%)	401 (34.1%)
[20, 25)	197 (35.6%)	94 (26.7%)	103 (38.3%)	394 (33.5%)
[30, 35)	92 (16.6%)	68 (19.3%)	40 (14.9%)	200 (17.0%)
[35, 40)	26 (4.7%)	38 (10.8%)	10 (3.7%)	74 (6.3%)
[40, 45)	4 (0.7%)	23 (6.5%)	13 (4.8%)	40 (3.4%)
[15, 20)	13 (2.3%)	10 (2.8%)	15 (5.6%)	38 (3.2%)
[45, 50)	1 (0.2%)	11 (3.1%)	1 (0.4%)	13 (1.1%)
[55, 60)	0 (0.0%)	3 (0.9%)	4 (1.5%)	7 (0.6%)
[10, 15)	2 (0.4%)	1 (0.3%)	1 (0.4%)	4 (0.3%)
[50, 55)	0 (0.0%)	1 (0.3%)	1 (0.4%)	2 (0.2%)
[60, 65)	0 (0.0%)	1 (0.3%)	0 (0.0%)	1 (0.1%)
[65, 70)	0 (0.0%)	0 (0.0%)	1 (0.4%)	1 (0.1%)
Total	554 (100%)	352 (100%)	269 (100%)	1175 (100%)

QUESTION 3 What is your gender?

Answer	Group 1	Group 2	Others	All Respondents
Male	517 (93.3%)	320 (90.9%)	189 (70.3%)	1026 (87.3%)
Female	26 (4.7%)	24 (6.8%)	73 (27.1%)	123 (10.5%)
No Answer	11 (2.0%)	8 (2.3%)	7 (2.6%)	26 (2.2%)
Total	554 (100%)	352 (100%)	269 (100%)	1175 (100%)

QUESTION 4 Have you used software to bypass the Great Firewall—such as a proxy or VPN?

Answer	Group 1		Group 2		Others		All Respondents	
On my computer								
Never	2	(0.4%)	0	(0.0%)	0	(0.0%)	2	(0.2%)
Longer than one month ago	130	(23.5%)	60	(17.0%)	74	(27.5%)	264	(22.5%)
Within the past month	422	(76.2%)	292	(83.0%)	195	(72.5%)	909	(77.4%)
On my phone								
Never	240	(43.3%)	89	(25.3%)	143	(53.2%)	472	(40.2%)
Longer than one month ago	100	(18.1%)	72	(20.5%)	43	(16.0%)	215	(18.3%)
Within the past month	214	(38.6%)	191	(54.3%)	83	(30.9%)	488	(41.5%)

QUESTION 5 How recently have you used each type of software to bypass the Great Firewall?

Answer	Group 1		Group 2		Others		All Respondents	
Web proxy								
Never	260	(46.9%)	157	(44.6%)	146	(54.3%)	563	(47.9%)
Longer than one month ago	229	(41.3%)	148	(42.0%)	86	(32.0%)	463	(39.4%)
Within the past month	65	(11.7%)	47	(13.4%)	37	(13.8%)	149	(12.7%)
Free VPN								
Never	247	(44.6%)	111	(31.5%)	135	(50.2%)	493	(42.0%)
Longer than one month ago	209	(37.7%)	116	(33.0%)	78	(29.0%)	403	(34.3%)
Within the past month	98	(17.7%)	125	(35.5%)	56	(20.8%)	279	(23.7%)
Paid VPN								
Never	330	(59.6%)	189	(53.7%)	158	(58.7%)	677	(57.6%)
Longer than one month ago	64	(11.6%)	47	(13.4%)	34	(12.6%)	145	(12.3%)
Within the past month	160	(28.9%)	116	(33.0%)	77	(28.6%)	353	(30.0%)
HTTP/SOCKS proxy								
Never	334	(60.3%)	182	(51.7%)	189	(70.3%)	705	(60.0%)
Longer than one month ago	109	(19.7%)	79	(22.4%)	44	(16.4%)	232	(19.7%)
Within the past month	111	(20.0%)	91	(25.9%)	36	(13.4%)	238	(20.3%)
Ultrasurf								
Never	407	(73.5%)	218	(61.9%)	189	(70.3%)	814	(69.3%)
Longer than one month ago	109	(19.7%)	102	(29.0%)	52	(19.3%)	263	(22.4%)
Within the past month	38	(6.9%)	32	(9.1%)	28	(10.4%)	98	(8.3%)
Tor								
Never	389	(70.2%)	209	(59.4%)	206	(76.6%)	804	(68.4%)
Longer than one month ago	149	(26.9%)	117	(33.2%)	51	(19.0%)	317	(27.0%)
Within the past month	16	(2.9%)	26	(7.4%)	12	(4.5%)	54	(4.6%)
GoAgent								
Never	255	(46.0%)	107	(30.4%)	173	(64.3%)	535	(45.5%)

Longer than one month ago	105	(19.0%)	68	(19.3%)	28	(10.4%)	201	(17.1%)
Within the past month	194	(35.0%)	177	(50.3%)	68	(25.3%)	439	(37.4%)
SSH								
Never	338	(61.0%)	170	(48.3%)	204	(75.8%)	712	(60.6%)
Longer than one month ago	92	(16.6%)	80	(22.7%)	25	(9.3%)	197	(16.8%)
Within the past month	124	(22.4%)	102	(29.0%)	40	(14.9%)	266	(22.6%)
PUFF								
Never	471	(85.0%)	266	(75.6%)	239	(88.8%)	976	(83.1%)
Longer than one month ago	65	(11.7%)	61	(17.3%)	24	(8.9%)	150	(12.8%)
Within the past month	18	(3.2%)	25	(7.1%)	6	(2.2%)	49	(4.2%)
PSiphon								
Never	485	(87.5%)	233	(66.2%)	220	(81.8%)	938	(79.8%)
Longer than one month ago	55	(9.9%)	87	(24.7%)	30	(11.2%)	172	(14.6%)
Within the past month	14	(2.5%)	32	(9.1%)	19	(7.1%)	65	(5.5%)
Freegate								
Never	232	(41.9%)	134	(38.1%)	108	(40.1%)	474	(40.3%)
Longer than one month ago	256	(46.2%)	164	(46.6%)	101	(37.5%)	521	(44.3%)
Within the past month	66	(11.9%)	54	(15.3%)	60	(22.3%)	180	(15.3%)

QUESTION 6 What are your main reasons for bypassing the Great Firewall?

Answer	Group 1		Group 2		Others		All Respondents	
To use Google, or other search engines	508	(91.7%)	326	(92.6%)	211	(78.4%)	1045	(88.9%)
To use Twitter, Facebook, or other social network sites	424	(76.5%)	301	(85.5%)	192	(71.4%)	917	(78.0%)
To read foreign news, like the New York Times	272	(49.1%)	245	(69.6%)	178	(66.2%)	695	(59.1%)
For my job	192	(34.7%)	88	(25.0%)	67	(24.9%)	347	(29.5%)
To access movies and music, like YouTube or P2P sites	129	(23.3%)	115	(32.7%)	88	(32.7%)	332	(28.3%)
To access adult websites	120	(21.7%)	79	(22.4%)	44	(16.4%)	243	(20.7%)
To communicate privately with people outside China	47	(8.5%)	61	(17.3%)	43	(16.0%)	151	(12.9%)
To communicate privately with people in China	22	(4.0%)	35	(9.9%)	28	(10.4%)	85	(7.2%)

QUESTION 7 Think about the tool you use most often. Why did you choose this tool?

Answer	Group 1	Group 2	Others	All Respondents
It's more reliable than other tools	266 (48.0%)	199 (56.5%)	116 (43.1%)	581 (49.4%)
It's faster than other tools	175 (31.6%)	143 (40.6%)	90 (33.5%)	408 (34.7%)
It's easier to install or configure than other tools	169 (30.5%)	146 (41.5%)	82 (30.5%)	397 (33.8%)
My previous tool got blocked	144 (26.0%)	106 (30.1%)	77 (28.6%)	327 (27.8%)
It's less expensive than other tools	124 (22.4%)	101 (28.7%)	55 (20.4%)	280 (23.8%)
It's the only option I know how to use	129 (23.3%)	50 (14.2%)	83 (30.9%)	262 (22.3%)
I trust the people who make this tool more	74 (13.4%)	87 (24.7%)	37 (13.8%)	198 (16.9%)
My friends use the same tool	77 (13.9%)	30 (8.5%)	62 (23.0%)	169 (14.4%)

QUESTION 8 In your experience, what is the most important problem with circumvention tools in general?

Answer	Group 1	Group 2	Others	All Respondents
The tools make the Internet slow	261 (47.1%)	144 (40.9%)	128 (47.6%)	533 (45.4%)
The tools don't work reliably	266 (48.0%)	149 (42.3%)	107 (39.8%)	522 (44.4%)
The tools are too hard to install or configure	195 (35.2%)	137 (38.9%)	90 (33.5%)	422 (35.9%)
I am concerned about being detected by the authorities	106 (19.1%)	76 (21.6%)	64 (23.8%)	246 (20.9%)
None—these tools always work well for me	85 (15.3%)	73 (20.7%)	42 (15.6%)	200 (17.0%)
The tools are too expensive	85 (15.3%)	66 (18.8%)	45 (16.7%)	196 (16.7%)
I don't know or trust the people who make the tools	56 (10.1%)	47 (13.4%)	23 (8.6%)	126 (10.7%)

QUESTION 9 Where do you turn for help when you have problems with circumvention tools?

Answer	Group 1		Group 2		Others		All Respondents	
Web search, blogs or news	486	(87.7%)	312	(88.6%)	207	(77.0%)	1005	(85.5%)
Other online acquaintances	179	(32.3%)	145	(41.2%)	75	(27.9%)	399	(34.0%)
Co-workers	123	(22.2%)	27	(7.7%)	45	(16.7%)	195	(16.6%)
Friends or family	46	(8.3%)	34	(9.7%)	65	(24.2%)	145	(12.3%)

QUESTION 10 How did you learn about the first tool you ever used?

Answer	Group 1		Group 2		Others		All Respondents	
Web search, blogs or news	396	(71.5%)	279	(79.3%)	152	(56.5%)	827	(70.4%)
Other online acquaintances	119	(21.5%)	86	(24.4%)	43	(16.0%)	248	(21.1%)
Friends or family	59	(10.6%)	34	(9.7%)	79	(29.4%)	172	(14.6%)
Co-workers	71	(12.8%)	23	(6.5%)	51	(19.0%)	145	(12.3%)

QUESTION 11 Of the following three policies, which option would you most agree with?

Answer	Group 1		Group 2		Others		All Respondents	
Keep filtering on domestic sites, but remove the Great Firewall	438	(79.1%)	254	(72.2%)	185	(68.8%)	877	(74.6%)
Keep the Great Firewall, but remove filtering on domestic sites	57	(10.3%)	47	(13.4%)	47	(17.5%)	151	(12.9%)
No answer	44	(7.9%)	42	(11.9%)	28	(10.4%)	114	(9.7%)
Keep current Internet regulations the same	15	(2.7%)	9	(2.6%)	9	(3.3%)	33	(2.8%)
Total	554	(100%)	352	(100%)	269	(100%)	1175	(100%)

QUESTION 12 What is your highest level of education?

Answer	Group 1		Group 2		Others		All Respondents	
University graduate	354	(63.9%)	200	(56.8%)	143	(53.2%)	697	(59.3%)
Postgraduate/ PhD	97	(17.5%)	57	(16.2%)	78	(29.0%)	232	(19.7%)
Vocational school	70	(12.6%)	52	(14.8%)	22	(8.2%)	144	(12.3%)
Senior high school graduate	23	(4.2%)	33	(9.4%)	18	(6.7%)	74	(6.3%)
No schooling	9	(1.6%)	3	(0.9%)	1	(0.4%)	13	(1.1%)
Junior high school graduate	1	(0.2%)	6	(1.7%)	4	(1.5%)	11	(0.9%)
Elementary school	0	(0.0%)	1	(0.3%)	3	(1.1%)	4	(0.3%)
Total	554	(100%)	352	(100%)	269	(100%)	1175	(100%)

QUESTION 13 What is your current job?

Answer	Group 1		Group 2		Others		All Respondents	
Information technology, computer, and software related industries	335	(60.5%)	112	(31.8%)	64	(23.8%)	511	(43.5%)
Student	101	(18.2%)	63	(17.9%)	84	(31.2%)	248	(21.1%)
Freelance / Self-employed	28	(5.1%)	47	(13.4%)	27	(10.0%)	102	(8.7%)
Manufacturing and production industries	13	(2.3%)	41	(11.6%)	13	(4.8%)	67	(5.7%)
Other	14	(2.5%)	18	(5.1%)	9	(3.3%)	41	(3.5%)
Teacher	4	(0.7%)	12	(3.4%)	23	(8.6%)	39	(3.3%)
Business and finance industries	14	(2.5%)	12	(3.4%)	13	(4.8%)	39	(3.3%)
Media	10	(1.8%)	12	(3.4%)	15	(5.6%)	37	(3.1%)
Civil servant/government	11	(2.0%)	15	(4.3%)	10	(3.7%)	36	(3.1%)
Unemployed	14	(2.5%)	15	(4.3%)	4	(1.5%)	33	(2.8%)
Health care or medical industries	9	(1.6%)	5	(1.4%)	5	(1.9%)	19	(1.6%)
Social Activist	1	(0.2%)	0	(0.0%)	2	(0.7%)	3	(0.3%)
Total	554	(100%)	352	(100%)	269	(100%)	1175	(100%)

QUESTION 14 Have you ever traveled overseas?

Answer	Group 1		Group 2		Others		All Respondents	
No	439	(79.2%)	258	(73.3%)	147	(54.6%)	844	(71.8%)
Yes	115	(20.8%)	94	(26.7%)	122	(45.4%)	331	(28.2%)
Total	554	(100%)	352	(100%)	269	(100%)	1175	(100%)

QUESTION 15 Where have you lived for most of your life?

Answer	Group 1		Group 2		Others		All Respondents	
In mainland China	530	(95.7%)	340	(96.6%)	218	(81.0%)	1088	(92.6%)
In Hong Kong, Taiwan, or foreign countries	24	(4.3%)	12	(3.4%)	51	(19.0%)	87	(7.4%)
Total	554	(100%)	352	(100%)	269	(100%)	1175	(100%)

C NOTES

1 INTRODUCTION

1 See David Bamman *et al.*, "Censorship and deletion practices in Chinese social media," *First Monday* (Mar. 5, 2012), finding that "the rate of message deletion is not uniform throughout the country, with messages originating in the outlying provinces of Tibet and Qinghai exhibiting much higher deletion rates than those from eastern areas like Beijing."

2 See, *e.g.*, Greg Walton, "China's Golden Shield: Corporate complicity in the development of surveillance technology," *China Rights Forum*, No. 1 (2002).

3 See Bamman, note 1.

4 See, *e.g.*, Jason Ng, blog post on Sina Weibo censorship techniques, (Sep. 12, 2011) [in Chinese]; Sanja Kelly, Sarah Cook, and Mia Truong, *eds.*, Freedom on the Net 2012 (Freedom House, 2012) at 134 ("Sina Weibo users consistently report diverse measures employed by the company to prevent the circulation of politically sensitive content on a range of topics—deleting individual posts, deceiving users by making posts appear to them to have been published but actually rendering them invisible to followers, shuttering accounts, and removing results from the application's search function.").

5 Rebecca MacKinnon, "China's Censorship 2.0: How Companies Censor Bloggers," *First Monday* (Feb. 2, 2009).

6 See, *e.g.*, "Baidu Revises Censorship Notice, Recommends Users Try Alternate Search Terms," *Fei Chang Dao blog* (Sep. 1, 2012).

7 See, *e.g.*, Michael Wines, "Crackdown on Chinese Bloggers Who Fight the Censors With Puns," *The New York Times* (May 28, 2012).

8 This was the December 28, 2012 Decision of the Standing Committee of the National People's Congress on Strengthening Online Information Protection; see Laney Zhang, "China: NPC Decision on Network Information Protection," *Global Legal Monitor* (Jan. 4, 2013). An earlier mandate began in December 2011, when Beijing municipality issued new rules requiring weibo services based in the city to verify the real names of all users. The new rules applied to many major services, including Sina Weibo which is a product of Beijing-based Sina Corp. The new rules took effect on March 16, 2012, but were not fully enforced. Sina's affiliates on the US stock market, and its 2011 annual report (published in April 2012, the month after the deadline) warned investors that "[w]e are required to, but have not, verified the identities of all of our users who post on [Sina] Weibo, and our noncompliance

exposes us to potentially severe punishment by the Chinese government." Such requirements first began in 2007, when the country's General Administration of Press and Publication started requiring online game users to identify themselves so that the government could limit how long children were allowed to play such games.

9 See Charles Arthur, "China tightens 'Great Firewall' Internet control with new technology," *The Guardian* (Dec. 14 2012).

10 See Comment by "Twofish" on "China Now Blocking Encryption", *Schneier on Security* (Dec. 28, 2012).

11 See, *e.g.*, Daniel Anderson, "Splinternet Behind the Great Firewall of China," *ACM Queue* (Nov. 29, 2012).

12 Rebecca MacKinnon, *Consent of the Networked* (Basic Books, 2012), at 48, describes the additional controls applied to student Internet connections on university networks: "Many of China's top universities . . . offer free broadband to students in their dormitories. But there is a catch: The service is free only for domestic websites and a select list of 'whitelisted' overseas websites. To access any other websites or services from outside of China, students are charged according to [how much data they use]. Most students, being on tight budgets, see very little of the global Internet.")

2 SURVEY FINDINGS

13 See Emil Protalinski, "Chinese government blocks Google.com, Gmail, Google+, Maps, Docs, Analytics, Drive, more [Update: Unblocked]," *The Next Web* (Nov. 9-10, 2012).

14 See discussion of recent developments in Chinese policy toward VPNs, at 23.

15 The Tor team is currently working to address this issue through a new tool called Obfsproxy—a system that will transform Tor traffic so that it resembles other (permitted) traffic.

16 The GFW Blog is hosted by the China Internet Project at UC Berkeley.

17 See "Help for Skype: What is TOM Online?".

18 See Jacqui Cheng, "Skype security flub leads to discovery of Chinese monitoring," *Ars Technica* (Oct. 2, 2008).

19 Original text: "翻墙工具会经常被封锁，需要经常换."

20 Original text: "中断次数多."

21 Original text: “翻墙工具(VPN)容易被封，没有稳定的翻墙方法.”

22 The OpenNet Initiative, for example, tracks state Internet censorship of “Web sites that provide e-mail, Internet hosting, search, translation, Voice over Internet Protocol (VoIP) telephone service, and circumvention methods,” and ranks China’s censorship of such sites as “substantial.” See China, OpenNet Initiative (Aug. 9, 2012).

23 *Id*.

24 See Jason Ng, “Survey of Chinese Netizens Over the Firewall” [in Chinese] (Apr. 30, 2010). His original words: “我个人是50%之中的一员，审查必须有明确的大众标准，不能以领导人的喜怒哀乐为参考。”

25 Original text: “填了一份，对其中一个问题不爽！保留gfw或国内网络审查？应该都取消.”

26 See Ng, note 24. In April 2010, Mr. Ng invited all his Twitter followers to take the survey (“欢迎参加中国网民翻墙调查，数据全都匿名记录.”)

27 Cormac Callanan *et al*., “Leaping Over the Firewall: A Review of Censorship Circumvention Tools, *Freedom House* (2011).

28 For example, we do not know how many responses were received from Chinese users. Questions about the overall user experience with circumvention—such as how users decide which tools to use—were asked as part of the survey, but these results are not included in the report.

29 *Id*. at 49.

30 *Id*.

31 See Ng, note 24.

32 Oiwan Lam, “China: Over the GFW,” *Global Voices* (April 30, 2010).

33 See phobos, “China blocking Tor: Round Two,” *Tor Project Blog* (Mar. 11, 2010).

34 See home page of the OpenNet Initiative (“Internet censorship and surveillance are growing global phenomena. ONI’s mission is to identify and document Internet filtering and surveillance, and to promote and inform wider public dialogues about such practices.”)

35 The earliest in this group of reports, compiled in 2007 and released in 2009, provides one of the most comprehensive overviews ever assembled of the global landscape of circumvention tools, reviewing each of the major blocking-resistant tools as they then existed. See Hal Roberts, Ethan Zuckerman, and John Palfrey, ”*2007*

Circumvention Landscape Report: Methods, Uses, and Tools," *Berkman Center for Internet & Society* (Mar. 5, 2009). The testing regime included field tests of each major tool in a range of locations throughout the world, including two cities in China. *Id*. at 4. As of that 2007 study, the leading tools were functional, if frustrating: they "allow[ed] users to circumvent Internet censorship, even in countries like China and Vietnam, which use sophisticated technology to filter," but also slowed down Internet access, created security risks, and were in some cases "extremely difficult for a novice Internet user to use." The team updated this evaluation in 2011, with what was by then an expanded and changed set of circumvention tools, conducting a series of remote tests that included a virtual private server in China. Hal Roberts *et al*., "*2011 Circumvention Tool Evaluation*," *Berkman Center for Internet & Society* (Aug. 2011). They found that the tools were still frustrating to use, and that overall access had gotten worse. Several of the tools were totally blocked in China—not only one of the simple web proxies and one of the VPNs, but also three of the nine dedicated, blocking-resistant tools that it tested. See 2011 Evaluation, at 9.

36 Hal Roberts, Ethan Zuckerman, Jillian York, Robert Faris, and John Palfrey, "2010 Circumvention Tool Usage Report," *Berkman Center for Internet & Society* (Oct. 2010).

37 *Id*. at 5.

38 See Roberts, note 36 at 12.

39 *Id*. at 2.

40 Hal Roberts, Ethan Zuckerman, Robert Faris, Jillian York, and John Palfrey, "The Evolving Landscape of Internet Control: A Summary of Our Recent Research and Recommendations," *Berkman Center for Internet & Society* (Aug. 18, 2011).

41 *Id*. at 2.

42 This was a measurement technique that could not be used for VPNs or for specialized circumvention tools. Roberts, note 36 at 5 ("For the blocking-resistant tools and the VPN services, we rely primarily on self-reporting from our survey, since the individual circumvention projects themselves are the only ones with the necessary data about their users. For the simple web proxies, we are able to use Google AdPlanner's data on generic web site visits to measure usage of each tool because each use of a web proxy is also a web page request in itself. We use search frequency as reported by Google Insights as a separate point of reference and confirmation for these other methods.")

43 Hal Roberts, Ethan Zuckerman, Jillian York, Robert Faris, and John Palfrey, "International Bloggers and Internet Control," *Berkman Center for Internet & Society* (Aug. 2012).

44 *Id*.

45 See Roberts, note 35.

46 See Anderson, note 11.

47 For technical details on GoAgent see the discussion on page 5.

48 See Paul Mozur and Carlos Tejada, "China's 'Wall' Hits Business: Firms Say Censorship Slows Web Connections, Curbs Access to Services," *The Wall Street Journal* (Feb. 14, 2013).

49 *AmCham 2013 Business Climate Survey*, American Chamber of Commerce in the People's Republic of China.

50 *Id*.

51 See discussion on page 2.

52 See Mozur, note 48. See also Reporters Without Broders, "The Enemies of Internet—Special Edition: Surveillance" (March 2013).

53 See Kevin Voigt, "International firms caught in China's security web," *CNN* (August 24, 2012).

54 See note 15.

55 There was a public debate about which, out of the millions of pieces of content hosted on the site, might have motivated the censors to block it—but there is no way to be sure of the reasons for their decision). One theory attributed the block to a software tool that helped users identify routers connected to the Great Firewall. See Martin Johnson, "GitHub blocked in China – How it happened, how to get around it, and where it will take us," GreatFire.org (Jan. 30, 2013). Another view held that the decision was "directly related to an automated train ticketing plugin . . . Due to [the] upcoming Chinese New Year, newly released train tickets are sold within minutes. That plugin introduces huge traffic to an already crumbling ticket vending site, and it has obviously made [the] railroad bureau angry." See comment of ccp0202, *Hacker News* (Jan. 21, 2013).

56 See Josh Ong, "GitHub partially unblocked in China following public outcry from local developers," *The Next Web* (Jan. 23, 2013).

57 See Johnson, note 55.

58 These are the people responsible for the popularity of simple web proxies that can be accessed by searching for "proxy" or related terms on a search engine.

59 See Roberts *et al*., note 36.

60 R. Deibert *et al*., eds., *Access Contested: Security, Identity, and Resistance in Asian Cyberspace*, MIT Press (2011).

61 See HTTPSNow Home Page and "'HTTPS Now' Campaign Urges Users to Take an Active Role in Protecting Internet Security," *Electronic Frontier Foundation* (Apr. 20, 2011).

62 The certificates used to identify trusted web sites can be forged, allowing Chinese censors or others to impersonate the encrypted site and intercept its traffic. In fact, a few days after GitHub was blocked, the Great Firewall briefly interjected a forged certificate for GitHub, though in that case, it was not a high quality forgery. See Martin Johnson, "China, GitHub, and the Man-in-the-Middle," *GreatFire.org* (Jan. 30, 2013). See also Ed Felten, "Web Certification Fail: Bad Assumptions Lead to Bad Technology," *Freedom to Tinker* (Feb. 23, 2010).

4 CONCLUSION

63 See, *e.g.*, Ivan Zhai, "Blocking of coding site has Chinese programmers up in arms," *South China Morning Post* (Jan. 23, 2013) ("Feng Dahui, a programmer and an influential blogger, in a noon Sina Weibo post asked whether or not the IT community should support the bloggers who posted sensitive content on the site. 'There are about 1,000 of them and they are accustomed to posting sensitive content no matter where they go, and have previously caused the blockages on Twitter and Google+. What do you think about this?' Feng asked."); Comment of Tom Yuin, "What are the odds Amazon EC2 gets blocked in China, and how to prevent that?," *Quora*, (Jun. 13, 2011) ("I think the best thing we can do to reduce this risk is to request people to not use EC2 as a VPN[.]").

64 See Office of the United States Trade Representative, "United States Seeks Detailed Information on China's Internet Restrictions" (Oct. 19, 2011).

A SURVEY METHODOLOGY AND DESIGN

65 We also explored a number of alternative possible methods, including the use of an open source "wiki-survey" system called All Our Ideas. As part of that exploration, we translated the All Our Ideas interface into Chinese, contributed our work to the project, and received public thanks for our efforts.

66 See Douglas D. Heckathorn, "Respondent-Driven Sampling: A New Approach to the Study of Hidden Populations."

B SURVEY RESPONSE SUMMARY

67 Krista J. Gile, Lisa G. Johnston, Matthew J. Salganik, "Diagnostics for Respondent-driven Sampling" (Sep. 27, 2012) at 11.