



**“China’s Media and Information Controls—The Impact in China and the United States”**

**Testimony to the U.S.-China Economic and Security Review Commission  
Robert Guerra, Project Director for Internet Freedom, Freedom House  
September 10, 2009**

Chairman Bartholomew and members of the Commission, thank you for the opportunity to speak to you today about the status of China’s information control activities and the implications for U.S.-China relations. The internet has become an important tool globally for the exchange of information and ideas, yet internet surveillance and censorship greatly limit its impact and hinder the development of accountable and democratic politics.

China is home to the largest number of internet users globally, with more than with 338 million as of June 2009.<sup>1</sup> As in many other repressive countries, the internet provides a space for discussion in China that is more open than other more traditional forms of media. Indeed, the sheer number of bloggers and online discussion forums suggests that the internet is offering Chinese citizens an unprecedented opportunity to exchange information and express ideas. Nevertheless, the Chinese apparatus for censoring, monitoring, and controlling the internet is one of the most advanced in the world.

The Commission’s hearing is important and timely given recent developments in China pertaining to the internet, including the government’s attempt to mandate the installation of filtering software on all personal computers, as well as the recent arrest of several bloggers amid a larger crackdown on human rights defenders. The Chinese government also exerts pressure on U.S. and other Western companies to obtain sensitive technology and information, which is then used to track internet users and limit free expression. It has also sold technology to other countries with repressive media environments, including Saudi Arabia. Given that the internet is indeed global and that technology companies operate across borders, the U.S. and other Western governments have the responsibility to support measures to ensure that technology companies do not violate human rights when conducting business in repressive environments.

**Freedom House’s Internet Freedom Program**

---

<sup>1</sup> China Internet Network Information Center, “CNNIC Publishes 24<sup>th</sup> Statistical Report on Internet Development in China,” <http://www.cnnic.cn/html/Dir/2009/07/28/5644.htm> (accessed September 14, 2009).

Freedom House functions as a catalyst for freedom and democracy through its proven strategy that combines analysis, advocacy, and action. We bring more than 15 years of experience in supporting freedom's frontline defenders in countries around the world.

Freedom House's Internet Freedom Program seeks to counteract the rising trend of government censorship and surveillance in repressive environments, including China. It aims to analyze the state of internet freedom, to expand the use of anticensorship technologies, to build support networks for citizens fighting against online repression, and to focus greater international attention on the growing threats to internet users' rights. Freedom House is also active in tracking global internet governance policy to ensure that forums such as the Internet Corporation for Assigned Names and Numbers (ICANN) and the United Nations Internet Governance Forum (IGF) establish sound standards that support freedom of expression online. Freedom House actively engages these policymakers by providing them with recommendations on how to strengthen internet freedom and by ensuring that they counter attempts by repressive regimes to erode user's rights. Freedom House also amplifies the voices of users in internet-restricted environments at these international forums.

In order to better understand current threats to internet freedom, Freedom House developed a pilot study to monitor and compare internet freedom globally, entitled *Freedom on the Net: A Global Assessment of Internet and Digital Media*, which was released in April 2009. The study identifies concerning trends in censorship and repression, including the manual removal of online content by government or judicial directives, the manipulation of online discussions by government-sponsored agents, and the "outsourcing" of censorship and monitoring from the government to private actors, including internet service providers, blog-hosting companies, internet cafes, and mobile phone operators.<sup>2</sup> This report presents a new methodology to analyze and track internet freedom globally and applies this methodology in 15 country reports, which assess internet freedom in different regions of the world and span the range of experiences from free to highly repressive environments for internet freedom. Funding for this report was provided by the U.S. Department of State, the U.S. the Agency for International Development, and the Dutch Ministry of Foreign Affairs.

With regard to China, *Freedom on the Net* finds that its internet remains among the most restricted globally. By means of comparison, China scored on par with Tunisia in terms of its overall level of internet freedom, which both ranked slightly worse than Iran. Indeed, the study finds that China's apparatus for censoring, monitoring, and controlling internet and mobile phone use is the most advanced in the world. The detailed report on China identifies the disturbing trend of authorities expanding their mechanisms of control to include the outright manipulation of online content through the use of government-sponsored agents who direct online discussions thereby influencing public opinion. China also has the greatest number of individuals in prison for their online activities, with as many as 49 behind bars in mid-2008, and imposes the longest prison sentences for violations of internet regulations among the countries surveyed.

---

<sup>2</sup> *Freedom on the Net: A Global Assessment of Internet and Digital Media*, Freedom House, 2009, <http://www.freedomhouse.org/template.cfm?page=383&report=79> (accessed September 14, 2009).

## The Green Dam Case in China

Freedom House was greatly alarmed by the Chinese government's proposal, issued in May 2009, to further restrict and monitor internet use and expand its surveillance capability through the required installation of Green Dam Youth Escort filtering software on all personal computers sold in China as of July 1. Although the Chinese government claimed that the software was intended to block pornographic material, it was, in fact, a more pervasive mechanism of censorship and surveillance. The software blocks politically sensitive online content, enables applications such as Microsoft Word to shut down if certain sensitive words are used, and would allow authorities to access a user's computer to monitor internet activity and obtain other personal information. On June 30, the Chinese government announced that the Ministry of Industry and Information Technology was postponing the mandatory installation of the software, citing a lack of preparation time. On August 13, the Ministry announced that it was completely withdrawing the requirement that Green Dam be installed on all personal computers.<sup>3</sup> While Freedom House applauds this withdrawal, the incident raises several pertinent issues, including whether the government will attempt to impose similar requirements in the future, as well as the roles and responsibilities of foreign governments and companies in global internet policy.

The Green Dam case illustrates that the Chinese government is not immune to criticism from foreign governments and industry groups with regards to its internet policy. Nevertheless, although the proposal was withdrawn, it is important to understand the motives behind the proposal, as well as the factors that caused the government to reverse its decision to mandate the installation of the software on all personal computers.

*What factors drove the Chinese government to attempt to have the Green Dam Youth Escort filtering software pre-installed on all personal computers in China?*

The ostensible factor that drove the Chinese government to attempt to have the Green Dam Youth Escort filtering software pre-installed on all personal computers in China was to protect youth from accessing pornographic material. However, it is likely that the Chinese government possessed ulterior motives in mandating the installation, including profit seeking and the desire to better control online content.

The possibility of corruption was raised early on in the development of Green Dam software, with the accusation that a local official fraudulently approved loans to the software company developing Green Dam, despite the misgivings of other officials.<sup>4</sup> Additionally, the issue of a profit motive by the government was raised with the

---

<sup>3</sup> "China's Great Firewall," *The Washington Post*, August 17, 2009, <http://www.washingtonpost.com/wp-dyn/content/article/2009/08/16/AR2009081601697.html> (accessed September 14, 2009).

<sup>4</sup> "Green Dam Developer Tied to Henan's Most Corrupt Official," *eChinacities*, July 24, 2009, <http://www.echinacities.com/main/ChinaMedia/ChinaMediaInfo.aspx?n=3332> (accessed September 14, 2009).

suggestion that the government would eventually purchase the Green Dam software, therefore profiting from its sales.<sup>5</sup>

Beyond the Chinese government's possible profit-seeking motives, an assessment of the Green Dam software demonstrates that its scope extends well beyond censoring pornographic material to include censoring of other politically sensitive information. The installation of censorship tools directly onto personal computers would be a very efficient means for authorities to control and monitor internet use and other computer activities. The suggestion that the software was intended for more than to block porn is supported by the wide scope and significant depth of the software, going beyond censoring porn to also censoring many politically sensitive topics. According to the University of Michigan<sup>6</sup> and the Open Net Initiative,<sup>7</sup> Green Dam software's reach is pervasive: it blocks access to websites containing certain key words and images that have to do with sensitive political and religious issues; it shuts down applications such as Microsoft Word if certain key words are detected; it updates easily to constantly change the terms that are censored; and it installs spyware on computers to monitor use.

*What caused the Chinese government to postpone the mandatory pre-installment of the software?*

Criticism of the government's proposal to require Green Dam software on all computers was swift and diverse. Domestically, bloggers and rights defenders criticized the initiative for introducing further restrictions on free expression.<sup>8</sup> Critics also highlighted the software's technical flaws, which would leave computers that run the software vulnerable to security breaches.<sup>9</sup>

Internationally, foreign governments and trade associations sharply criticized the initiative. On June 19, a coalition of technology associations presented Chinese Premier Wen Jiabao with a request that the Green Dam requirement be reversed; the letter was signed by the heads of 22 leading organizations, including the U.S. Chamber of

---

<sup>5</sup> Wang Xing, "China softens stance on Green Dam filter," *China Daily*, August 24, 2009, [http://www.chinadaily.com.cn/bizchina/2009-08/24/content\\_8606112.htm](http://www.chinadaily.com.cn/bizchina/2009-08/24/content_8606112.htm) (accessed September 14, 2009).

<sup>6</sup> Scott Wolchok, Randy Yao, and J. Alex Halderman, "Analysis of the Green Dam Censorware System." June 11, 2009, <http://www.cse.umich.edu/~jhalderm/pub/gd/> (accessed September 14, 2009).

<sup>7</sup> "China's Green Dam: The Implications of Government Control Encroaching on the Home PC." Open Net Initiative, <http://opennet.net/chinas-green-dam-the-implications-government-control-encroaching-home-pc> (accessed September 14, 2009).

<sup>8</sup> Andrew Jacobs, "Experts Say Chinese Filter Would Make PCs Vulnerable," *The New York Times*, June 12, 2009, <http://www.nytimes.com/2009/06/13/world/asia/13china.html> (accessed September 14, 2009); Rebecca MacKinnon, "China's Censorship Blowback," *RConversation*, June 25, 2009, <http://rconversation.blogs.com/rconversation/2009/06/chinas-censorship-blowback.html> (accessed September 14, 2009).

<sup>9</sup> "China's Green Dam: The Implications of Government Control Encroaching on the Home PC." Open Net Initiative, <http://opennet.net/chinas-green-dam-the-implications-government-control-encroaching-home-pc> (accessed September 14, 2009).

Commerce and the European-American Business Council.<sup>10</sup> There were also formal trade complaints from the United States Government<sup>11</sup>, as well as from the European Union Commission.<sup>12</sup> Finally, the proposed mandatory installation of Green Dam became an intellectual property issue after researchers discovered that California-based Solid Oak Software owned the code, and that Green Dam developers used the code without permission.<sup>13</sup>

Overall, the widespread criticism of Green Dam created a public relations disaster for the Chinese government. Green Dam raised the issues of corruption in terms of procurement, intellectual property and trade violations, and poor judgment on the part of the authorities given the software's severe technical shortcomings.

*If this initiative were successful, how would it have impacted internet freedom in China?*

The deployment of Green Dam would have impacted internet freedom in several ways. Green Dam would have increased the obstacles to internet access, given that the software would have impeded the ability of internet users to access circumvention tools, such as Ultrasurf, which is a tool to promote anonymity online. Green Dam would have severely increased limits on content, given that it would have blocked sensitive key words and images, and would have also regulated the use of applications. Overall, the installation of Green Dam software on all personal computers would have dramatically increased the scope and level of censorship faced by the average computer user in China. The software would have brought internet monitoring and censorship from the level of the government or internet service provider directly to the individual user's computer—bringing censorship directly into the home.

*What is the likelihood that the Chinese government will attempt to institute a requirement for the pre-installment of similar filtering software on Chinese computers in the future?*

Although the Chinese government reversed its mandate to require the installation of Green Dam on all personal computers, the initiative has not entirely disappeared. The Chinese government still requires that Green Dam software be installed on public computers, such as in schools and at internet cafes.<sup>14</sup> Furthermore, several PC

---

<sup>10</sup> Loretta Chao, "Big Business Groups Complain to China's Premier," *The Wall Street Journal*, June 27, 2009, [http://online.wsj.com/article/SB124599434995459155.html?mod=googlenews\\_wsj](http://online.wsj.com/article/SB124599434995459155.html?mod=googlenews_wsj) (accessed September 14, 2009).

<sup>11</sup> Kim Hart, "U.S. Presses China on Censorship," *The Washington Post*, June 25, 2009, <http://www.washingtonpost.com/wp-dyn/content/article/2009/06/24/AR2009062403452.html> (accessed September 14, 2009).

<sup>12</sup> "Chinese Censorship of Internet 'Unacceptable'" EUBusiness, <http://www.eubusiness.com/news-eu/1246009621.79/> (accessed September 14, 2009).

<sup>13</sup> Mark Hachman, "China's Filtering Software Contains Pirated Code," PCMag.com, June 12, 2009, <http://www.pcmag.com/article2/0,2817,2348705,00.asp> (accessed September 14, 2009).

<sup>14</sup> Loretta Chao and Jason Dean, "Chinese Delay Plan for Censor Software," *The Wall Street Journal*, July 1, 2009, [http://online.wsj.com/article/SB124636491863372821.html#mod=loomia?loomia\\_si=t0:a16:g2:r3:c0.0908524:b26085204](http://online.wsj.com/article/SB124636491863372821.html#mod=loomia?loomia_si=t0:a16:g2:r3:c0.0908524:b26085204) (accessed September 14, 2009).

manufacturers, including Lenovo, Acer, and Sony, are still shipping PCs installed with Green Dam software.<sup>15</sup> Furthermore, although the Chinese government will likely be wary of future measures that bring censorship directly to individual users' computers—given the multifaceted outcry against the initiative—the government will likely seek more subtle means of increasing monitoring and censorship, requiring vigilance among defenders of free expression online.

*How has the Global Network Initiative, an information technology industry group spearheaded by Microsoft, Google, Yahoo!, and numerous human rights groups, developed during the past year?*

Discussions on the formation of the Global Network Initiative (GNI) began in 2006. The GNI's establishment was prompted by the 2004 imprisonment of Chinese journalist Shi Tao, whose conviction was facilitated by information provided by Yahoo! on his email activities; the government accused him of violating state secrecy laws following an email message he sent through his Yahoo! account.<sup>16</sup> Since its formation, however, the GNI has not advanced at an acceptable pace. The GNI has still not found someone to fill the role of executive director. The Center for Democracy and Technology, which was instrumental in the GNI's establishment, explained that it has had difficulty finding someone with enough expertise to advance the agenda.<sup>17</sup> Furthermore, Google, Yahoo!, and Microsoft, the biggest companies within the GNI, are primarily Web 1.0. GNI does not have the support of newer social media—Web 2.0—companies such as Facebook and Twitter. Nor does the GNI have the support of European or other foreign companies. Because of the rapidly changing nature of the internet, it is imperative that GNI keep pace by appraising, changing, and implementing policies that conform to an ever-changing environment. While the GNI and its signatories are making an important step forward in responsible corporate policy, it is not enough for them to simply support the guidelines. In order to realize the full scale of their core commitments, GNI and its signatories must ensure that their practices are sufficient to ensure effective protection of the rights of internet users in repressive environments like China.

The chart below provides an overview of the main developments with regards to the internet globally over the past six years. It shows an increase in the number of bloggers who have been arrested, which correlates to an increase in the number of internet users. Fundamentally, it suggests that efforts, such as the GNI, that do not have the force of law, are not adequate to protect bloggers in repressive environments.

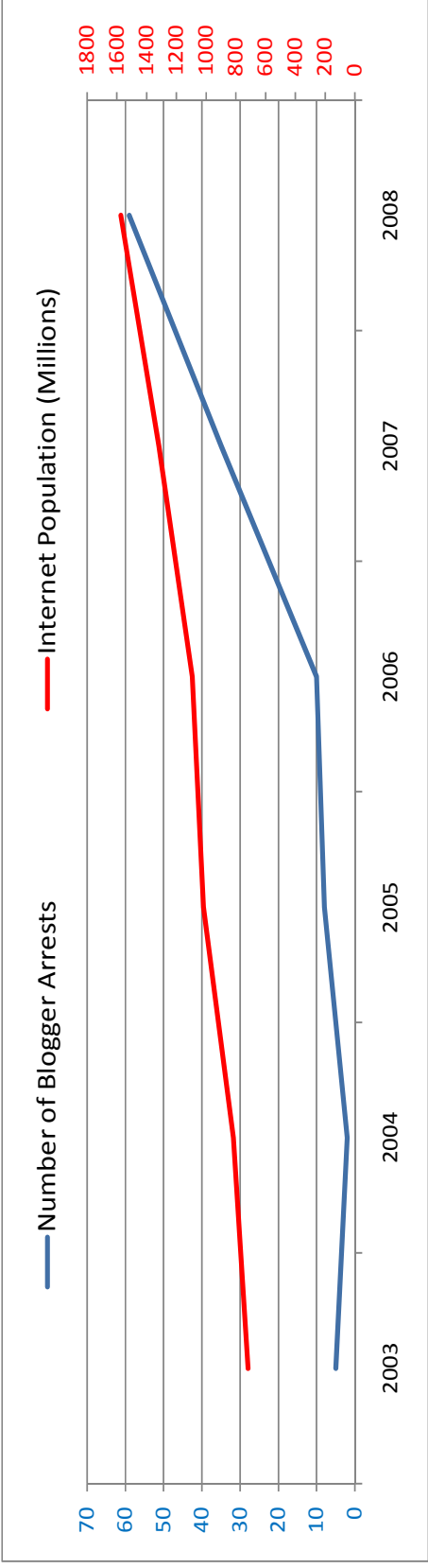
---

<sup>15</sup> Owen Fletcher, "China will still require Green Dam Web filter program," NetworkWorld, July 2, 2009, <http://www.networkworld.com/news/2009/070209-china-will-still-require-green.html> (accessed September 14, 2009); Jonathan Ansfield, "China Web Sites Seeking Users' Names," The New York Times, September 5, 2009 <http://www.nytimes.com/2009/09/06/world/asia/06chinanet.html?hp> (accessed September 14, 2009).

<sup>16</sup> "Priority Cases: Shi Tao, 10 Years in Prison for Sending an Email," Amnesty International, <http://www.amnestyusa.org/individuals-at-risk/priority-cases/shi-tao/page.do?id=1101243> (accessed September 14, 2009).

<sup>17</sup> Rosalie Marshall, "Global Network Initiative Fails to Take Off," V3.co.uk, August 5, 2009, <http://www.v3.co.uk/v3/news/2247333/lacking-staff-global-network> (accessed September 14, 2009).

# Major Internet Developments and Trends Over Time: Global Blogger Arrests and Internet Population



<p>1995 - MSN.com Launched</p> <p>1995 - Yahoo.com Launched</p> <p>1998 - Google.com Launched</p> <p>MySpace.com Launched</p> <p>Yahoo! Provides info leading to the arrest of Wang Xiaoning in 2002.</p> <p>Google buys Blogger.com</p> <p>Delicious.com Launched</p>	<p>Facebook.com Launched</p> <p>Digg.com Launched</p> <p>Yahoo! provides info that leads to conviction of Shi Tao.</p>	<p>YouTube.com Launched</p> <p>Twitter.com Launched</p> <p>Microsoft shuts down blogger Zhao Jing's blog on MSN.com</p> <p>Google, Yahoo!, Microsoft, and Vodafone begin series of dialogues aimed at understanding free expression as it relates to worldwide technology usage.</p> <p>Global Online Freedom Act submitted by Chris Smith (R-NJ)</p>	<p>FriendFeed.com Launched</p> <p>Google provides Indian Gov. with IP information leading to wrongful arrest of <i>Orkut</i> user.</p> <p>Google, Yahoo!, Microsoft, and Vodafone announce work on joint human rights charter.</p> <p>Promotion and Protection of Human Rights submitted by John Ruggie, Special Representative of the Secretary-General on the Issue of human rights and transnational corporations and other business enterprises.</p>	<p>Global Network Initiative Launched</p>
--	--	---	--	---

*What is needed for the GNI to serve as an effective means for limiting U.S. corporations complicity in China's internet censorship activities? How likely is it that this will occur?*

Several factors would need to change in order for the GNI to serve as a truly effective mechanism for limiting corporate complicity in censorship in repressive environments. First, success with regards to the GNI should be judged according to the ultimate impact of policies on internet users. This is critical so that the body does not become a forum for abstract discussion with little relevance to the average internet user in repressive environments. Second, the oversight, enforcement, and penalties encompassing the GNI should have the strength of law. Similarly, legislation should be developed to protect companies against pressure from repressive governments to filter content and turn over private data. Finally, the GNI should be truly global, and non-U.S. based technology companies should participate in the initiative.

**What the Global Network Initiative needs:**

- Greater focus on the end user: the GNI's success should be judged on the impact of policies on the end user.
- Stronger enforcement and oversight mechanisms: the GNI should be backed by the force of law.
- Truly global support: the GNI should be supported by non-U.S. based companies given the global and transborder nature of the internet.

*Should the U.S. Congress support the Global Network Initiative, or is it necessary to create legislation that would legally restrict U.S. companies from contributing to foreign government's information control activities?*

Freedom House supports the view that legislation, such as the proposed Global Online Freedom Act (GOFA), should be adopted by Congress. This would ensure that U.S. policy protects internet freedom and, at a minimum, would ensure that U.S. companies are no longer complicit in violations of internet users' rights. GOFA is critical to promoting freedom of expression and expanding the flow of information online. Specifically, GOFA would: require U.S. companies to host personal data outside of the physical reach of internet-restricting governments; give the U.S. Attorney General the authority to deny requests for personal data that might be used to repress dissidents; prevent U.S. companies from blocking access to U.S. government-supported websites; and require U.S. companies to disclose the methods of filtering they use and the content they block at the request of repressive regimes. In addition, GOFA would create an Office of Global Internet Freedom in the State Department and explore the feasibility of



introducing export controls on filtering and surveillance technologies to internet-restricting countries.

While voluntary codes of conduct, such as the GNI, are commendable, they are insufficient to shield U.S. companies from pressure to filter content or to turn over personal data on peaceful dissidents. GOFA will provide strong protection to U.S. companies against such pressure.

Rather than put U.S. companies at a competitive disadvantage, GOFA is likely to raise international standards for business to protect and advance internet freedom, much as the Foreign Corrupt Practices Act led to the OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions.

However, GOFA is not enough. Further policy initiatives are needed to defend and expand internet freedom:

- Congress should expand its efforts to advance internet freedom, for instance to draw attention to human rights abuses against internet users. These efforts should draw attention both to individual cases of human rights abuse and to broader violations of internet freedom, such as the sophisticated, multi-layered systems of internet censorship pioneered in China and increasingly exported to a growing number of countries.
- The U.S. government and other democratic governments have funded important internet freedom programs. Greater support is needed to advance indigenous efforts within internet-restricting countries to expand the space for free expression online. A multi-donor fund would bolster the shared commitments of democratic governments to provide such support. Such a fund is needed to:
  - expand education and exchanges with experts (academics, journalists, lawyers, etc.) in China on issues of online censorship and privacy
  - enhance advocacy by Chinese experts on internet freedom
  - provide direct support to victims of repression, such as arrested bloggers
  - build multi-stakeholder networks of internet freedom advocates across internet-restricting countries, so that they may learn from each other's creativity in challenging repression
  - facilitate translations of material related to freedom of expression online
  - increase research on internet censorship and violations of user rights
  - stimulate development of and expand access to innovative technologies to circumvent censorship and to protect personal data.
- The State Department should engage in more rigorous diplomacy in support of U.S. companies as they seek to avoid pressure to limit access to content or weaken protections on the personal data of internet users. This diplomacy should both challenge violations of internet freedom by repressive governments and build broader coalitions among democratic governments to advance internet freedom. The State Department should also seek to persuade democratic governments to adopt similar controls as the United States on exports of internet censorship and surveillance technologies to internet-restricting countries.

- The U.S. Trade Representative should explore the possibility of resisting internet censorship within the context of bilateral and multilateral negotiations or of challenges to trade barriers before the World Trade Organization.

**What democratic governments can do to support the expansion of internet freedom in repressive environments:**

- Publicize violations of rights of individual internet users and policies that increase levels of monitoring and censorship in repressive environments.
- Support indigenous efforts to promote internet freedom and raise awareness about issues of online censorship, such as through exchanges with students, academics, and journalists.
- Support companies that seek to avoid pressure by repressive governments that would limit access to content or violate the rights of individual internet users.
- Resist internet censorship within the context of bilateral and multilateral trade negotiations.

Through the adoption of the Global Online Freedom Act, rigorous diplomacy, support for free speech advocates in repressive environments, and Congressional engagement, the United States can lead international efforts to protect and advance freedom of expression online. At a time when the rights of internet users across the globe are increasingly at risk, U.S. leadership is critical to defend internet freedom, so that citizens living under authoritarian regimes may still find a space to speak openly, to connect with like-minded citizens, and to hold government to account.