

**Senate Judiciary Committee**  
**Subcommittee on Human Rights and the Law**  
**“Global Internet Freedom: Corporate Responsibility and the Rule of Law”**  
**May 20, 2008**

**Questions for the Record – Shiyu Zhou, Global Internet Freedom Consortium**

**Questions from Senator Tom Coburn:**

**1. In your opinion, can communication services like email or blogging sites ever be used safely — in other words, without the risk of identifying cyber dissidents — in countries like China?**

**Answer:** Yes, they can be used safely even in China, if users effectively take advantage of end-to-end anti-censorship tools like the Global Internet Freedom Consortium (GIF) provides. Starting from account registration, to downloading emails or posting blogs, to visiting other sites, users have to use secure anti-censorship tools to hide their identity.

Of course, it would be even safer if users can use the email services and blogging sites GIF has been providing, which resides in the United States but with their native language interface, and is a full end-to-end solution when users use our anti-censorship tools to access these services.

**2. Google rightfully prides itself on transparency — that even though it must sometimes censor in compliance with local laws, it provides a notice to let its customers know what has been done. Would a similar disclosure be effective for users of communication services like email or blogging? Perhaps a notice disclosing the fact that the Internet service provider must operate in compliance with local law and that information exchanged may be subject to government review?**

**Answer:** It is not transparency, it is censorship. In fact, Chinese Internet police have been doing it by forcing ISPs to place images of big-eyed net police cartoons on their websites. Chinese Internet users have already lost their trust in the domestic ISPs. Even for foreign ISPs, since the Shi Tao-Yahoo incident, Chinese users no longer trust them. But that does not mean they do not need safe, secure email and blogging services, and that is why GIF has been providing such services to censored users.

**3. Would you please submit to the subcommittee all evidence you have showing Cisco's alleged cooperation with the Chinese Government?**

**Answer:** Yes. We have submitted some materials already. Attached is some additional info:

(1) [psindustryknowledge\\_Eng.pdf](#) gives an overview of the Public Security

Industry of China, and lays out the marketing strategy for Cisco-China to sell products and solutions to the Chinese police.

On page 57, it reveals that one of the major objectives of the GSP is to "combat 'Falun Gong' evil cult." On page 58, it shows that Cisco offers much more than just routers; it offers planning, construction, technical training, and operations maintenance for GSP.

(2) GSP-background-English.pdf gives an overview of the needs of GSP and Cisco's high-level solutions meeting the needs.

(3) The Cisco Chronical (translated from the Chinese version on Cisco's website) shows that Cisco not only helped the Chinese authorities construct the level-2 and level-3 of GSP, but also did level-1, which is the backbone of GSP.

(4) Cisco-and-1st-Level-GSP.rtf (translated from the Chinese version on Cisco's website) explains more details on how Cisco helped the Chinese authorities construct level-1 backbone of GSP.

(5) The translation of the two paragraphs in the Chinese version of Wikipedia on GSP (which are missing in the English counterpart of Wikipedia) explains that China's Great Firewall is part of the GSP.