



Cisco Systems, Inc.

170 West Tasman Drive

San Jose, CA 95134-1706

October 29, 2010

Mr. Jing Zhao & Morton Sklar, Esq.
160 Maidenhair Court
San Ramon, CA 94583

Subject: Response to your letter dated September 9, 2010

Dear Messrs. Jing and Sklar:

Thank you for your most recent correspondence, and for taking time to meet with several members of Cisco's senior management team on Friday, September 3, 2010. During our discussion, we provided an overview of Cisco's business in China, and of the general marketplace in China for Internet infrastructure. This letter is to provide further information regarding companies participating in the networking infrastructure market in China, as you had requested, and that information appears in the appendix to the letter. While the information is from the best research reports we could identify, this may not be a comprehensive list as there are many smaller technology providers - both China-based and otherwise - selling networking technology in China.

We believe that our policy of providing standards-based Internet equipment, refusing to customize equipment in a manner than might facilitate censorship, and actively opposing efforts of government to "balkanize" the Internet through national regulatory regimes, are the best way to ensure global freedom of expression using the Internet. To reiterate four points we made during the meeting:

- Cisco does not customize its products in any respect that would facilitate censorship, and sells the same basic products worldwide. Standard internet routing and switching equipment by its very nature allows for the filtering of sites accessible through the network. Given the almost constant attacks on the Internet from hackers and thieves, it would be impossible to sell any equipment without such capabilities for both public and private networks. Such capabilities are ubiquitous and available from every vendor of any sort of Internet routing and switching equipment.
- Cisco's sales are strictly in accordance with United States export control rules which limit sales of certain technologies in China and to various entities in China - rules which are informed by human rights concerns. We are in compliance with the Foreign Relations Act of 1991, and are familiar with the current rulemaking regarding the Commerce Control List under that Act. Cisco intends to remain in full compliance with that Act. We note that in your letter you asserted that Cisco made sales in violation of US export control rules. If you have information regarding any such sales, we would be grateful if you would provide it to us so that we can fully investigate.
- Cisco actively opposes efforts to impose local regulatory regimes. Efforts of the Chinese government, for instance to rate "network security" that favor local products ("MLPS") and requiring disclosure of source code and low level design information for "security routers" ("CCC") are the types of steps which can lead to a less open Internet. It is important to understand that our security products are not welcome in many markets, and the information in the Appendix to this letter clearly illustrates the point. And the MLPS and

CCC regulations, referred to above, would provide disincentives or make practically impossible such sales even to non-governmental entities.

- Cisco supports the principles of the Global Network Initiative for network operators. We have committed that where we operate a network, we will comply with GNI principles regarding due process. We do not sell certain products, such as voice communication interception devices (alluded to by you in your letter) at all.

To help ensure that we act in accordance with our principles, we have regular review of human rights concerns at both the senior management and board of director levels. Each business situation is unique and deserves thoughtful analysis accordingly to ensure maximum oversight, fulfillment of our values and the best possible protection of Cisco's reputation and your investment as a shareholder.

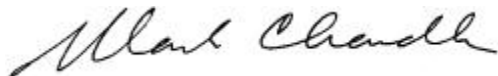
During our discussion you alluded to quotation from a Chinese then-government official which appeared in a 2001 Cisco internal powerpoint presentation. One element of the quotation referred to suppression of "hostile elements", including Falun Gong, as a goal of Chinese policy for network security. Contrary to the inference you attempted to suggest in the meeting, in no way did Cisco ever offer to provide products for that purpose (the presentation was a 90 page review of public sector networking in China, from forestry to traffic control to fire and public safety).

While we understand the potential appeal of pursuing a large, multi-national company such as Cisco to draw attention to the cause of freedom of expression, for the reasons above we believe that in this case that is misplaced and ultimately a counterproductive vehicle for raising those concerns. We believe the policies we support and the practices we implement represent the best chance we all have to ensure an open and free global Internet which maximizes the potential for freedom of expression.

We hope the attached summaries of reports from Frost & Sullivan and IDC regarding the Chinese market are helpful to you.

Once again, thank you again for engaging with us in a constructive discussion of the human rights implications of the dissemination of Internet technology. We have found your counsel to be valuable, and we appreciate your support.

Sincerely yours,

A handwritten signature in black ink, appearing to read "Mark Chandler". The signature is fluid and cursive, written in a professional style.

Mark Chandler

Senior Vice President, General Counsel and Secretary

APPENDIX

ANALYST REPORTS REGARDING CHINA INTERNET SECURITY MARKET

Source: Frost and Sullivan, IDC

Switching, Routing, Wireless LANs

These technologies link networks of computers together and/or enable Internet connectivity via wired or wireless connections. The overwhelming majority of Cisco's sales in this market are for enterprise use – that is, to facilitate communication within entities.

US/European Vendors (US-based unless otherwise noted)

- Alcatel/Lucent (France)
- Avaya/Nortel
- Brocade
- Cisco
- Dell
- Extreme Networks
- HP/3Com/H3C (HP recently acquired 3Com & its Chinese-based subsidiary, H3C)
- Motorola

Chinese Vendors

- Digital China
- Huawei
- Ruijie Networks
- TP Link
- ZTE
- Zyxel (Taiwan)

Network Security

Products prevent unauthorized network access, combat spam and malware, enable network management.

US/Western Vendors

- Checkpoint/Nokia (Israel; acquired Nokia network security division)
- Cisco
- Cyphertrust
- Fortinet
- HP/3Com/H3C
- IBM
- Juniper
- McAfee (in process of being acquired by Intel)
- Secure Computing

Chinese Vendors

- Huawei-Symantec (joint partnership with US-based Symantec)
- LeadSec (Lenovo)
- LinkTrust
- Neusoft
- NSFocus
- TopSec
- VenusTech

Note: According to the reports, the network security market within China is a highly fragmented one, with the leading vendor, Topsec, holding only a 15.2% share. While 7 of the top 10 vendors are Chinese companies, US firms do have a presence in the market, though less than 10% we believe. The network security market – including the Intrusion Detection/Intrusion Prevention Systems (IDS/IPS) sector - is almost completely controlled by Chinese vendors, with the top 6 Chinese-based companies alone possessing a combined market share of over 80%. (IDS/IPS devices monitor network traffic and are capable of identifying malicious activity, logging information and reporting events, and enabling a network operator to block or stop certain activity or network traffic.)