September 20, 2006

Secretary Carlos M. Gutierrez
Office of the Secretary
U.S. Department of Commerce
1401 Constitution Avenue, N.W.
Washington, D.C. 20230

Dear Secretary Gutierrez:

The Electronic Privacy Information Center (EPIC) is a public interest research center in Washington, DC that focuses on privacy and emerging civil liberties issues. We are writing to you regarding the export of high-tech surveillance equipment to China's security forces by American companies. We believe that the current policy of the Department of Commerce establishes a double standard that prohibits the export of traditional security devices while permitting the sale of products that make possible far more widespread surveillance and political control. We urge you to reexamine this policy.

EPIC realizes the importance to the economy of increasing exports to China and other countries where there is an existing trade imbalance. However, the possibility that the Chinese authority may use this technology to track dissidents, journalists, or members of "unauthorized religions" is an issue that needs to be addressed.

As you are aware, the United States has placed restrictions on the exporting of products destined for use by Chinese security forces. These restrictions were put in place following the Tiananmen Square massacre of 1989.[1] Although low-tech equipment, such as tear gas and handcuffs, fall within these restrictions, other, more hi-tech equipment, such as database software and video probes, do not. Some of the larger American technology businesses have been exporting these products to customers in China, including the Chinese Ministry of Public Security.

Although advancements have been made in recent years, the Chinese government's human rights record remains poor, as the U.S. State Department's 2005 report on human rights practices in China confirms. The report states that, since 2004, "the [Chinese] government adopted measures to control more tightly print, broadcast and electronic media, and censored online content. Protests by those seeking to redress grievances increased significantly and were suppressed, at times violently, by security

[1] Foreign Relations Authorization Act of 1991, Pub. L. No. 101-246 § 901

forces."[2] The report also lists many human rights problems that exist in China, including the monitoring of citizens' mail, telephone and electronic communications, as well as the nonjudicially approved surveillance and detention of dissidents.[3]

According to the report, "during the year authorities monitored telephone conversations, facsimile transmissions, e-mail, text messaging, and Internet communications. Authorities also opened and censored domestic and international mail. The security services routinely monitored and entered residences and offices to gain access to computers, telephones, and fax machines. All major hotels had a sizable internal security presence, and hotel guestrooms were sometimes bugged and searched for sensitive or proprietary materials.[4]

The 2005 State Department human rights report further finds that:

> Some citizens were under heavy surveillance and routinely had their telephone calls monitored or telephone service disrupted. The authorities frequently warned dissidents and activists, underground religious figures, former political prisoners, and others whom the government considered to be troublemakers not to meet with foreigners.[5]

Clearly, the Chinese authorities perform an unacceptably high level of surveillance and monitoring, and are very likely to use advanced technology they import from the U.S., or elsewhere to facilitate this.

The State Department report also states that from 2004 to 2005, the government continued to encourage expanded use of the Internet, while monitoring use and control of content. It also took steps to increase monitoring of the Internet, restricted the information available online, and punished those who violated regulations.[6]

The 2005 edition of *Privacy and Human Rights*,*: An International Survey of Privacy Law and Developments,* published by EPIC and Privacy International, draws attention to the high levels of government surveillance in China. We found, for example, that in 2005 the Beijing Internet Safety Service Center of the Beijing Public Security Bureau recruited 4,000 web "watchdogs" to put cybercafes and Internet service providers in Beijing under surveillance.[7] Human rights groups estimated that in 2002 alone the

---

[2] U.S. DEPT. OF STATE, BUREAU OF DEMOCRACY, HUMAN RIGHTS, AND LABOR, CHINA COUNTRY REPORT ON HUMAN RIGHTS PRACTICES 2005 (2006),http://www.state.gov/g/drl/rls/hrrpt/2005/61605.htm.
[3] *Id.*
[4] *Id.*
[5] *Id.*
[6] *Id.*
[7] EPIC AND PRIVACY INTERNATIONAL, PRIVACY AND HUMAN RIGHTS: AN INTERNATIONAL SURVEY OF PRIVACY LAWS AND DEVELOPMENTS 369 (2006) (quoting Shi

Chinese government employed 30,000 people to monitor Internet traffic. In 2004, Amnesty International reported that more 50 Internet users were serving prison terms of posting opinions online in during that year.[8]

The fact that surveillance technology can be used in China for political repression is an ongoing concern. The Ministry of Civil Affairs controls all social organizations in China. Every one must be reported and registered with this Ministry. Labor unions remain illegal. Government authorities systematically monitor some individuals and groups more closely than others. Advocates of democratic reform, human rights activists, and minorities are all kept under close watch.[9] Software produced by U.S. owned companies could allow Chinese police to tap into data repositories held by the Ministry of Public Security, further facilitating this monitoring. [10]

A recent article in *BusinessWeek* notes, "American manufacturers say that they are under no obligation or ability to determine whether Chinese security forces use the technology for political repression." The article further indicates that Cisco distributed brochures at a police technology trade show in Shanghai in 2002 in which the company referred to its products with such phrases as "strengthening police control" and "increasing social stability."[11]

Allowing high-tech products to slip through the export restrictions goes against the ideology of the 1990 legislation, which was enacted, among other things, to suspend "export licenses for any crime control and detection instruments and equipment to China." The Department of Commerce should scrutinize any applications for export licenses for this technology extremely carefully.

The American democratic tradition, and its worldwide reputation of valuing democracy, and individual freedoms could be undermined by the involvement of the U.S. technology industry in authoritarian and suppressive actions taken by the Chinese communist government against its citizens. Companies need to be presented with a strong legislative framework in which to carry out their trade with Chinese customers.

Sincerely,

Marc Rotenberg, President
Electronic Privacy Information Center (EPIC)

Ting, *Search on for 4,000 Web Police for Beijing*, SOUTH CHINA MORNING POST, June 17, 2005).
[8] *Id.*
[9] *Id.* at 362.
[10] *Helping Big Brother Go High Tech*, BUSINESSWEEK, Sept. 18, 2006, *available at* http://www.businessweek.com/magazine/content/06_38/b4001067.htm.
[11] *Id.*

Enclosure

EPIC, PRIVACY AND HUMAN RIGHTS: AN INTERNATIONAL SURVEY OF PRIVACY LAWS AND DEVELOPMENTS (2006)

CC:

Chairman Henry J. Hyde and Vice Chairman Christopher H. Smith of the U.S. House of Representatives Committee on International Relations

Chairman James A. Leach and Vice Chairman Dan Burton of the U.S. House of Representatives Committee on International Relations Subcommittee on Asia and the Pacific.

Chairman Cliff Stearns and Ranking Member Jan Schakowsky of the U.S. House of Representatives Subcommittee on Commerce, Trade and Consumer Protection.