Threats of int'l BlackBerry bans echo US debate

August 16 2010, By PETER SVENSSON , AP Technology Writer

Customers enter a mobile phone shop as a billboard of a BlackBerry phone is placed at the entrance in Calcutta, India, Friday, Aug. 13, 2010. India may ask Google and Skype for greater access to encrypted information, once it resolves security concerns with BlackBerry, which is now under threat of a ban, according to a government document and two people familiar with the talks. (AP Photo/Bikas Das)

(AP) -- Threats by the governments of India, the United Arab Emirates and Saudi Arabia to shut down BlackBerry's corporate e-mail services reflect unease about a technology that the U.S. government also took a while to accept.

The foreign governments are essentially a decade behind in coming to terms with encryption, a technology that's fundamental to the Internet as a medium of commerce.

Encrypted communications are scrambled in a complex process to ensure that only the intended recipient can read them, using the proper digital key. This often takes place behind the scenes, without the user needing to do anything. When you submit your credit card number on a shopping site, the communication is encrypted. When you log in to your bank's site, that connection is encrypted as well.

Most companies use encrypted connections for their corporate e-mails, at least if employees need to access e-mail outside the office through virtual private networks and other secure systems. One of the reasons Research In Motion Ltd. has been so successful with its BlackBerry phones is that it brought that level of security to e-mail-capable phones.

Encryption, however, poses a problem for law enforcement officials. They can intercept encrypted messages, but can't read them, unless the encryption is poor and agents have vast computer resources to use in unscrambling them. Traditional investigative tools such as wiretaps don't work. Canada's RIM and other technology companies stress that they agree to legal requests from law enforcement, but in RIM's case, it can't decrypt the messages on its corporate e-mail service.

BlackBerrys seem to have been singled out by foreign governments because the devices provide an easy and convenient way to communicate securely. But there are many other ways to communicate in an encrypted fashion, and any government that's serious about squelching encrypted communications would need to go after them as well.

According to a representative of Indian Internet service providers, the Indian government plans to go after Google Inc., presumably for its Gmail service, and Skype SA for its voice and video conferencing software.

The U.S. State Department has waded into the issue, saying it hopes to

broker a compromise that addresses the legitimate security concerns of some governments while ensuring that the free flow of information is not compromised.

That's somewhat ironic, considering the U.S. restricts exports of encryption technology. The restrictions are light, but were quite comprehensive before 1999. The U.S. was concerned that it couldn't easily spy on foreign countries that used encryption for military and government communications.

In fact, until 1996, encryption at the level commonly in use today was classified as a munition. Companies that exported Web browsers and other software products had to make alternative versions with much weaker encryption for use abroad.

The First Amendment made it impossible to restrict encryption technology inside the U.S. But the Clinton administration still tried to get the industry to adopt the "Clipper Chip," a device that would encrypt communications but leave a "backdoor" for the government to decrypt messages. The idea led to a public outcry and had technical shortcomings, and it was ultimately abandoned.

With the rise of the Internet as a consumer medium in the 90s, encryption became a household technology. It became clear that restricting the use of tough encryption only to U.S. Internet users wasn't feasible.

Still, when the Clinton administration relaxed export controls, it was over the objections of its attorney general and FBI director.

The relaxation of export restrictions in 1999 wasn't the end of the debate, either. Two days after the 9/11 attacks, Sen. Judd Gregg, R-N.H., called for a global prohibition on encryption products that didn't

have backdoors for government surveillance; he was reviving the "Clipper Chip" idea.

In 2003, the Justice Department circulated draft legislation that would lengthen prison sentences for people who used encryption in the commission of a crime. Encryption defenders said it would do little to help catch terrorists, and it went nowhere.

Since then, the U.S. government has more or less accepted that encryption is here to stay. Wholesale access by law enforcement to encrypted communications may not be possible, but BlackBerry e-mails are decrypted at the corporate servers, and can be obtained from there with a warrant. Gmail connections are encrypted, but the messages are in the clear on Google's servers, and Google cooperates with law enforcement. Intercepting Skype is trickier because the audio and video conversations aren't stored, but security experts say there are ways to deal with this.

Then there's always human error. The alleged Russian spy ring that was arrested in the New York area in June used encryption, but one of them also left a password lying on his desk, where it was found by FBI agents who broke in. That enabled them to decrypt hundreds of messages.

RIM, the company behind the BlackBerry, doesn't have years to wait for foreign governments to adopt the more relaxed U.S. stance toward encryption. It has until the end of the month to comply with orders from Indian government, and it may have no way to do so short of shutting down service in the country.

The RIM system doesn't seem to be designed to give a backdoor to anyone, not even to those in the company, said Maribel Lopez, a technology analyst and consultant.

"It's not like RIM is sitting there with everybody's keys looking at everybody's stuff," she said. That doesn't give them much leeway in dealing with governments that want keys.

"This is actually a bit of disaster for them right now because there doesn't seem to be any good compromising midpoint," Lopez said.