Questions and answers about BlackBerry objections

October 8 2010, By PETER SVENSSON , AP Technology Writer

(AP) -- Some questions and answers about the threats to ban the use of BlackBerry's messaging and Web services:

Q: Which countries are involved?

A: India still has an end-of-October deadline for compliance with its eavesdropping laws. It has threatened to shut down BlackBerry services if Research In Motion Ltd., the Canadian company behind the phone, does not comply. Saudi Arabia and the United Arab Emirates made similar threats, but appear to have been mollified; the UAE announced Friday that it wouldn't ban the services on Monday as previously planned. Earlier, Lebanon and Indonesia have said they were considering similar moves, but have no firm plans.

In the U.S., the FBI would like the power to eavesdrop on all communications, repeating demands that have been shot down by Congress several times before.

Q: Why have they been going after BlackBerry?

A: The corporate version of the BlackBerry e-mail system is practically impossible to eavesdrop on, unless you have access to the corporate e-mail servers. The e-mails are encrypted while in transit, and even RIM doesn't have the keys to decrypt them. The system is designed to keep corporate and government secrets safe, but the countries are concerned that it could provide cover for illegal activity.

Q: What is encryption?

A: Encryption is the process of "locking" a message so that only the intended recipient can read it, using a digital "key." It's widely used on the Internet. Without it, online banking and shopping would not be possible, nor any other sensitive communications.

Q: What is RIM doing to meet demands that it open up the system?

A: The concessions it's made to Saudi Arabia and the UAE have not been spelled out, but in general, there isn't much RIM can do. Its system is built from the ground up for rock-solid security. That's the main reason corporations and governments allow employees to use it. To give a government wholesale access to e-mails on BlackBerry's corporate service, RIM would have to dismantle its whole system in the country and rebuild it in an insecure fashion. BlackBerrys would have to be modified to not encrypt messages. RIM's customers would move to other systems that still offer secure e-mail.

RIM co-CEO Jim Balsillie said last month that the company has no way of providing government officials with the text of encrypted corporate e-mails sent on its phones, but that it won't object if individual companies that use the devices hand over their encryption keys to authorities. Balsillie said countries that want access to BlackBerry e-mails could theoretically set up a national registry where companies doing business within their borders would have to provide government officials with the ability to peek at encrypted messages.

Some countries have said they want RIM to place a server within their borders, meaning e-mails between local BlackBerrys would not have to leave the country while in transit. That could assuage any fears that other countries can spy on locals' e-mail, even though doing so would be difficult if not impossible. But having a server in their own country wouldn't make it any easier for their law enforcement to read the e-mails.

Q: Aren't BlackBerry e-mails accessible to governments anyway?

A: Possibly, but not in a fast, easy way. The e-mails exist in decrypted form on corporate servers, but those may be overseas, and it takes time to get access to them through a legal process with warrants. RIM stresses that governments can satisfy national security and law enforcement needs without compromising commercial security requirements.

Q: What options to do locals and travelers have if BlackBerry services are shut down?

A: If they need secure communications, there are plenty of options, pointing to the futility of banning BlackBerry services. Business travelers can use their laptops to get secure corporate e-mails, or they can carry other smart phones, such as iPhones and those running Windows Mobile. Others can use encrypted Gmail connections, or standalone e-mail encryption programs.

However, Indian Internet service providers say the government is set to go after other encrypted services like Skype and Gmail next. That would amount to a large-scale attempt to undermine secure communications on the Internet. The U.S. FBI would also like "back doors" into all encrypted communications services.