Cell Phone Privacy Software Making Governments Worry

May 28, 2013 - It's an old story. Governments around the world spend billions of dollars annually on new snooping technologies. They want access to as much information about as many people as possible. Then along comes an entrepreneur who spends far less money to develop technology that defeats everything that those governments are trying to do. That entrepreneur then markets his/her technology to the public; making all of those governments more than a little nervous. That is precisely what is happening with regard to smart phones.

You probably think that your business is none of the governments business. Regardless of what country, state or municipality that you live in, it is a pretty safe bet that your government would disagree with you on that point. They might not say it publically, but actions do speak louder than words.

For instance, the FBI is currently developing the world's largest law enforcement database for use with facial recognition software. And the NSA has a secure facility that is capable of monitoring virtually every phone call made in the world. Those are just a couple of very large and expensive examples that we know about, so it is a pretty good bet that there are many other examples that are not receiving public scrutiny. It is no wonder that these organizations aren't too happy that consumers can now defeat some of this snooping capability for as little as $3 per month.

Within the past two months, two new companies have made their encryption software available for sale to the public. Last month, Silent Circle - an American company - launched a service that encrypts phone calls, text messages, video calls and email for $20 per month. For another $29 per month, you can even encrypt the phone calls of people who don't subscribe to Silent Circle.

And this month, Seecrypt - a South African Company - launched a service that will encrypt calls and text messages for $3 per month. To use Seecrypt, both the sending and receiving phone need to subscribe to their services, but the company does offer a three month free trial.

Given the features and benefits that both services offer, there is a real business market that could lead people to use these services even if privacy isn't their primary concern.

For example, as a part of the Seecrypt service, you can call any other phone on your list of trusted contacts anywhere in the world, with no per minute charges. You will still have to pay applicable data rates, but if you have an unlimited data plan with your cell phone carrier, that's not an issue.

Both of these services have the US and European governments very concerned. Neither service currently has any back-doors built into them that would allow the government to eavesdrop on conversations; even with a search warrant. That is already leading to demands by some politicians that the services be modified. Since Silent Circle is an American Company, it is probably most vulnerable to such demands but that is shear speculation on our part. Seecrypt has simply said that it will not comply with these types of demands.

Both companies claim to retain as little data as possible. And both companies are relying encryption keys that they don't have access to. That means that even if some government agency did manage to get their hands on raw data stored by one of them, it would be virtually impossible to decipher. Since both companies use single-use encryption systems, the keys are theoretically impossible to break.

This technology battle over privacy presents some real dilemmas for governments around the world. First and foremost is probably dealing with terrorism. There are also issues with regard to other criminal activity such as money laundering, the drug trade, etcâ€¦ There is absolutely no doubt services like these can be used in ways that hurt everyone.

But there is also a flip side that coin. Anyone who lives in a repressive regime and who has real reason to fear their government can now overcome their government's monitoring activities.

From a business perspective, there is good reason to encrypt both calls and data transmissions. Encryption services reduce the possibility of data breaches - which are costly for businesses and consumers - and can help protect trade secrets. These services don't just protect users from government snooping. They also prevent hacking and corporate espionage. And they do so at reasonable prices.

If both consumers and businesses begin to see real benefits from encryption services such as the two described here, and they do see wide adaptation, then it could very well become nearly impossible for governments to snoop on calls or other data transmissions. But it is a safe bet that billions of additional dollars will be spent trying.
byJim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.
Follow me on Twitter:

Follow ACCESS