Smartphones and Privacy - The Frightening New Stalking Software Coming to a Government Near You

February 20, 2013 - What does your smart phone say about you? Can it tell people where you have been? Can it tell them what you've done? The answer to both questions is "yes." But the real question that you may find more interesting is, "Can it tell someone where you will be in the future and pinpoint a time that you will show up there?" The answer to that question also appears to be "yes", and with frightening accuracy.

Tweet

```
(function() {
var s = document.createElement('SCRIPT'), s1 = document.getElementsByTagName('SCRIPT')[0];
s.type = 'text/javascript';
s.src = 'http://widgets.digg.com/buttons.js';
s1.parentNode.insertBefore(s, s1);
})();
```

```
(function() {
  var po = document.createElement('script'); po.type = 'text/javascript'; po.async = true;
  po.src = 'https://apis.google.com/js/plusone.js';
  var s = document.getElementsByTagName('script')[0]; s.parentNode.insertBefore(po, s);
})();
```

The defense contractor Raytheon has developed a computer program that uses social media to track your every move. The technology is called Rapid Information Overlay Technology, or RIOT for short, and is probably better referred to as "stalkerware" instead of software.

RIOT uses postings to social media websites and GPS technology that is embedded in smart phones to dissect the life of the phone's owner. But instead of simply analyzing past events, it also predicts future behavior.

While we could attempt to explain exactly how the program works, there is no real need since Raytheon produced its own video. You'll find that at the end of this article. The company has stated that they have not sold the technology to anyone, but that is unlikely to remain the case for too long. They are a publically traded company with strong government ties. It is a fairly safe bet that they didn't develop RIOT for their health. Somebody in some govermentment agency wanted the technology.

The very existence of this software brings to mind a number of troubling questions. Ever since the Patriot Act became law, the government has had extremely easy access to electronic data such as phone records. RIOT has some very obvious law enforcement applications but it also has some just as obvious Fourth Amendment considerations. So, who will this stalkerware be used by, and who will they focus on? Will there be any court oversight involved? And does anyone who carries a smart phone have any privacy rights at all?

Just as important as the issues above, how do you keep this technology out of the hands of criminals and more repressive governments? As you will see in the video, Raytheon provides a lot of information about how the software works. It doesn't look like it would be too difficult for any other technology company or foreign government to come up with something similar. In fact, there are probably some hackers out there who are good enough to come up with a similar program.

If such a program became commercially available, every private detective in the country would want it. If you suspected your spouse of cheating on you, and you had a program like this, then you could even mount your own investigation. If you are a criminal and want to case someone's home, the software could give you a very good picture of when your victim's house is likely to be empty. And if you are a stalker who is intent on killing someone, RIOT would definitely simplify your task.

Right now, privacy laws simply aren't capable of dealing with this type of technology. There is nothing illegal about creating a program like this, and there really doesn't appear to be anything illegal about using the technology if you have access to it. This is a genie that can't be stuffed back into the bottle. That means that the only way to deal with it is to change our own behavior when we use smart phones.
Here is the video.

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