Private Company's Camera Networking Program Raising Privacy Eyebrows

August 14, 2012 - A couple of weeks ago we published a story on facial recognition software and the privacy concerns that it is beginning to raise. What we didn't realize at the time was that the website Wikileaks was about to publish some email messages from a company named Stratfor that would detail a program to network surveillance cameras and have them all hubbed into a central system. That program - called TrapWire - is much more extensive than anything we previously believed to be in place. More importantly, the data being collected through it isn't just being used by law enforcement agencies. Much of it appears to be for sale to virtually anyoneâ€¦ for the right price of course. TrapWire - which is actually owned by a company of the same name, based in Reston, VA - raises a wide variety of privacy concerns; many of which have probably not even been seriously contemplated. And it could mean that the very idea of anonymity in modern society is an antiquated idea.

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 Stratfor email messages do not provide a comprehensive picture of TrapWire. But they do paint a picture of what the program is supposed to do. In short, it networks surveillance cameras from a wide variety of locations and then uses software to sort the data collected by those cameras. That may not sound like a big deal until you understand the scope of the project.

Unlike closed circuit surveillance systems that are localized - such as the type that you might find at a local convenience store - the Stratfor email messages indicate that the TrapWire is up and functioning in a variety of US cities as well as a number of overseas locations.

Once a camera is on TrapWire, the pictures taken through it can be run through software that does facial recognition and which recognizes a number of other biometric markers for individuals. These might include things like a person's walk or

how their limbs are proportioned in size to the rest of their bodies. In the case of automobiles, the software can track license plate movements across all TrapWire cameras and has the ability to recognize various other features associated with particular vehicles. Although the email messages don't indicate this, it is also probable that by tracking individual movements through cameras will eventually be paired with other electronic data to allow the tracking of financial activities; even if those activities involve cash transactions.

In terms of what this means for privacy, just consider a couple of scenarios. Let's say you drive from New York to Los Angeles. Theoretically, TrapWire could potentially track your entire trip. If they can get a picture of you with your car, they could then look further to see everyplace you visited - even on walking tours, or going to restaurants - throughout your entire trip. Now imagine that a portion of your trip involves some international travel. Even that may not be an issue for TrapWire. Once your face in their system, it has to be assumed that you can be tracked across the globe.

Such a network has profound privacy implications. Because the data is collected by a private firm, law enforcement can use it without any need for a warrant. Now, all of a sudden, if you become the target of a government investigation does this mean that the government can simply purchase a complete picture of your comings and goings without any regard to the Fourth Amendment? And, since TrapWire openly states that it will share information that it finds to be suspicious with law enforcement agencies, could the company's suspicions about you lead to a government investigation of your personal activities?

More importantly, what is to prevent a private entity from purchasing information about you from TrapWire? While the data isn't cheap - a license apparently costs $20,000 - it might be very useful to private investigators, attorneys, and even to criminals.

To be sure, TrapWire does have some legitimate uses. The network has apparently grown out of a desire on the part of governments around the world to be able to stop terrorism; a laudable goal. And TrapWire does have privacy policies that don't allow information that is marked to law enforcement use to be sold to people or organizations that are not a part of the law enforcement community. But, in the end, TrapWire is just a big database that is run by people. Large databases make very attractive targets for hackers. And people make mistakes that lead to data breaches. Even with the best of intentions, the risk for TrapWire to be used for the wrong purposes by government or for its data to fall into the wrong hands should give everyone pause.

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