PRIVACY SOS

TRAPWIRE AND DATA MINING: WHAT WE KNOW

08/13/2012

Thought

Released on 2012-08-09 18:00 GMT

Email-ID	5355966
Date	2010-02-08 20:56:40
From	Anya.Alfano@stratfor.com
To	burton@stratfor.com

Regarding SF landmarks of interest--they need something like Trapwire more for threats from activists than from terror threats. Both are useful, but the activists are ever present around here.

These days every news cycle brings us more thoroughly disturbing reasons to be concerned about pervasive digital monitoring in the United States. This week things got extra interesting with the revelation of an enormous, shadowy surveillance company with deep ties to the CIA: Trapwire (http://trapwire.com) exploded on the surveillance scene like a bat out of hell. And people are justifiably freaked out about it.

But people are also publishing a lot of information that seems to have appeared out of the ether, grounded in no documentation whatsoever. There is no need to speculate or conjure surveillance bogeymen where they do not exist. The documented facts speak loudly enough.

Furthermore, we don't even have to look to pre-crime, globally networked spook software like Trapwire to be concerned about where we stand vis a vis privacy rights and government powers. Take the following stories **from just the past month** as a small sample of our problems, serving to illustrate the seriousness of our current predicament:

- On NSA dreams (http://www.technologyreview.com/news/428644/nsa-boss-wants-more-control-over-the-net/): "NSA Boss Wants More Control Over the Net: The Internet should be adapted to allow for oversight by the National Security Agency, the organization's boss says" (Technology Review, MIT, July 27, 2012)

- On NSA vacuum style (http://www.networkworld.com/community/node/81026) digital surveillance: "HOPE 9: Whistleblower Binney says the NSA has dossiers on nearly every US citizen" (NetworkWorld, July 15, 2012)

- On the feds using our cellphones as bugs (http://thenewamerican.com/usnews/constitution/item/12244-ninth-circuit-oks-feds-use-of-cellphone-as-roving-bugs): "Ninth Circuit OKs Feds Use of Cellphones as Roving Bugs" (The New American, July 28, 2012)

- On impunity and secrecy (http://www.theatlantic.com/politics/archive/2012/07/the-feds-violated-the-constitution-but-the-administration-wont-say-how/260239/) in spying: "The Feds Violated the Constitution but the Administration Won't Say How" (The Atlantic, July 24, 2012)

- On the National Counter Terrorism Center (NCTC) collecting (http://www.aclu.org/blog/national-security-technology-and-liberty/biggest-new-spying-program-youve-probably-never-heard) unimaginably large amounts of data about every single person and storing it for a very long time: "The Biggest New Spying Program You've Probably Never Heard Of" (ACLU, July 30, 2012)

- On impunity (http://livepage.apple.com/) for warrantless spying on a mass scale: "Appeals Court OKs Warrantless Wiretapping" (Wired, August 7, 2012)

- On face recognition (http://www.infosecisland.com/blogview/22082-FBIs-Facial-Recognition-is-Coming-to-a-State-Near-You.html): "FBI's Facial Recognition is Coming to a State Near You" (EFF, August 8, 2012)

- On the Microsoft and NYPD attempt (http://nymag.com/daily/intel/2012/08/nypd-domain-awareness-system-microsoft-is-watching-you.html) to recreate "Total Information Awareness": "The NYPD's Domain Awareness System Is Watching You" (New York Magazine, August 9, 2012)

And for those worried that the government will use its vast, unaccountable surveillance powers to intimidate and harass political activists or religious minorities, there's some news for you, too:

- On the targeting (http://www.thestranger.com/seattle/political-convictions/Content?oid=14397498) of political anarchists: "Political Convictions? Federal Prosecutors in Seattle Are Dragging Activists into Grand Juries, Citing Their Social Circles and Anarchist Reading Materials" (The Stranger, August 7, 2012)

- On JTTF raids (http://www.greenisthenewred.com/blog/home-raids-grand-jury-subpoenas-portland-olympia-seattle/6233/) of activist homes: "FBI and JTTF Raid Multiple Homes, Grand Jury Subpoenas in Portland, Olympia, Seattle" (Green is the New Red, July 25, 2012)

- On the NYPD's relentless and remorseless targeting (http://online.wsj.com/article/AP9a8e4574209c481892f60926a9619050.html) of Muslims: "Gov jabs at NYPD again over spying on Muslims" (Wall Street Journal, August 8, 2012)

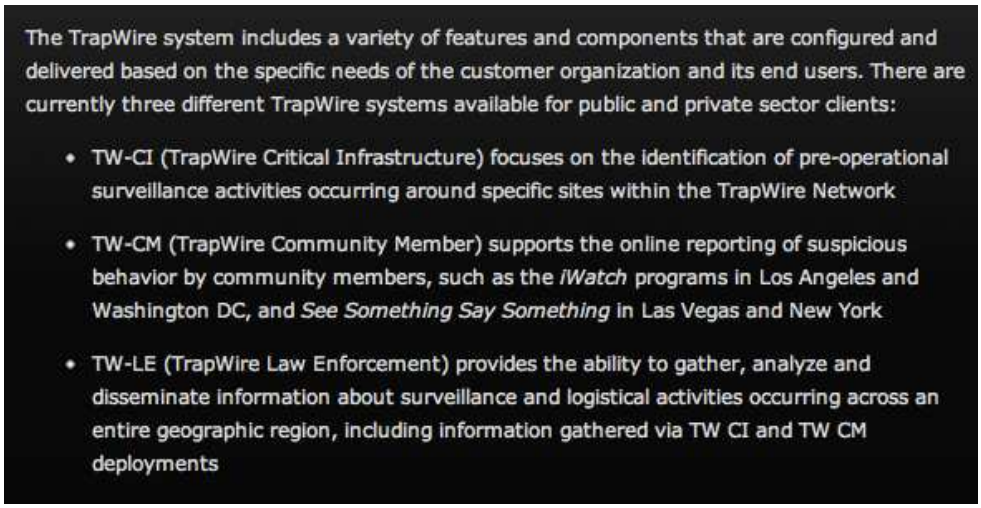
In other words, we are in a rough spot, Trapwire or no Trapwire. Having established that, let's move on to what we can prove Trapwire is, and what we cannot.

Unproven claims about Trapwire

Given what we know about other, active surveillance programs, there's no need to speculate that we are living in dangerous times. But unfortunately that's precisely what's happening on the internet this week.

This article (http://www.shtfplan.com/headline-news/confirmed-new-nationwide-trapwire-surveillance-system-is-actively-recording-monitoring-everything_08102012), for example, called "Confirmed: New Nationwide "Trapwire" Surveillance System is Actively Recording, Monitoring Everything," makes a series of extremely disturbing allegations that it supports with absolutely no documentation, beginning with its headline.

Among other unproven and somewhat hysterical allegations, the article claims that "The Trapwire system is actively monitoring every major city in the country." Really? The documents I've been able to locate show that the company's "TrapWire Community Member" program — which importantly is not the same as its critical infrastructure monitoring program or its law enforcement program — is operative in a number of major cities, including Washington DC, Las Vegas, New York and Los Angeles.



(https://2f8dep2znrkt2udzwp1pbyxd-wpengine.netdna-ssl.com/sites/all/images/trap_cities.png)

But I can't find any evidence to support the claim that it is operating where I live, for example, in Boston — or in Providence, RI, or ~~Portland, OR or Seattle, WA,~~ etc.. **(See correction/update here.)** It very well might be operating in every US city, but there is no evidence to back up such a claim.

The article further states that Trapwire's software integrates its license plate and CCTV

data with “what you bought on your credit card today and who you interacted with via text message or your favorite social network” without providing a shred of evidence for the latter. Trapwire’s website and its ~~patent~~ trademark filings confirm that its software attempts to integrate license plate and CCTV data, but makes zero mention of credit card information or SMS metadata. That's not to say the company's database doesn't have this information, but it is a fact that there's no documentation or other proof to give credence to these claims.

Salon.com (http://www.salon.com/topic/trapwire/) is the most high profile outlet to publish a claim I've seen batted about the internet for a few days — that Trapwire's system is more advanced than face recognition. Again, there's been zero evidence presented to back up this claim.

Speculating about Trapwire's prowess and reach is dangerous and unnecessary. After all, the facts the company laid out for us through its limited but nonetheless revealing digital trail are enough to raise the alarm.

Let’s turn to what we know about Trapwire.

Known knowns

Trapwire's early history

The first documentation of Trapwire’s existence comes from filing papers (http://tdr.uspto.gov/jsp/DocumentViewPage.jsp?76610388/APP20040910140226/Application/6/07-Sep-2004/sn/false#p=1) to the US patent office dated September 7, 2004. The papers ask for a trademark on Goods: "computer software for use in detecting terrorist surveillance of a facility and other pre-attack preparations on a facility or on persons associated with a facility". The trademark application was filed by a company called Abraxas Corporation, represented by a Danielle O. Saunders of McLean, Virginia — the heart of CIA country.

On April 5, 2005 the US patent office responded (http://tdr.uspto.gov/jsp/DocumentViewPage.jsp?76610388/OOA20050405112658/Offc%20Action%20Outgoing/7/05-Apr-2005/sn/false#p=1) by denying the trademark

application because of "likelihood of confusion" with two other companies' trademarks: "The applicant's mark, TRAPWIRE, is similar to the registered marks, TRIPWIRE and TRAPWARE. The marks are compared for similarities in sound, appearance, meaning or connotation."

On October 4, 2005 the patent office received a response (http://tdr.uspto.gov /jsp/DocumentViewPage.jsp?76610388/IPC20051005110759 /Paper%20Correspondence%20Incoming/8/04-Oct-2005/sn/false#p=5) from Abraxas Corporation, arguing that the products the three companies produce are different enough to warrant granting Abraxas the Trapwire trademark. Furthermore, it argues, its product will only be sold to an elite batch of discriminating clients who would engage in extensive research and consultation with the firm before buying it. This isn't "food snacks" you grab at the market without thinking twice, it says. It's a big, costly computer surveillance network made for the "discriminating purchaser." Indeed.

Somewhat hilariously, Abraxas points out that the two other companies — Tripwire and Trapware — make computer software products that allow individual computer users and large networks to detect unwanted attacks on their systems. Trapwire doesn't do that, the lawyers wrote. You can say that again.

The US patent office overturned (http://tdr.uspto.gov /jsp/DocumentViewPage.jsp?76610388/NTS20051114142113/Notation%20to%20File/1/14-Nov-2005/sn/false#p=1) its initial rejection on November 14, 2005, about a month after Abraxas' appeal. Four days before Christmas, on December 21, 2005, the patent office mailed (http://tdr.uspto.gov/jsp/DocumentViewPage.jsp?76610388/NOP20051221150714 /Notice%20of%20Publication/1/21-Dec-2005/sn/false#p=1) an official notice of publication for the Trapwire mark to attorney Danielle O. Saunders. The company had its trademark, and likely a very Merry Christmas.

The next document in the Trapwire file at the patent office is a notice (http://tdr.uspto.gov/jsp/DocumentViewPage.jsp?76610388/RAA20060105140838 /TEAS%20Revoke%20Appointed%20Attorney/1/05-Jan-2006/sn/false#p=1) to revoke power of attorney from Danielle O. Saunders, filed January 5, 2006. The company's power of attorney would change again multiple times over the next five years.

Finally, on September 26, 2005 the patent office received some more substantive information from the company, describing what it set out to do with its trademark. That document is titled "TrapWire™: Pre-Attack Terrorist Detection System for Protecting Critical Infrastructure". You can read it yourself here (https://2f8dep2znrkt2udzwp1pbyxd-wpengine.netdna-ssl.com/sites/all/files/trapwire.pdf) .

The basics: what does Trapwire do?

The whitepaper sketches out the contours of a pre-crime surveillance system that the former CIA agents (http://webcache.googleusercontent.com/search?q=cache:0pAfaMR-AFEJ:www.trapwire.com/management.html+&cd=1&hl=en&ct=clnk&gl=us)who run Trapwire Inc. hoped would work to "intercept a terrorist strike before it begins."

> ***TrapWire dramatically increases the ability to detect pre-attack preparations and to take appropriate action to detect, deter and intercept terrorist attacks. A visual monitor of the entire system — a map with dynamic status indicators for each entity connected to the TrapWire network — facilitates the ability of decision-makers to absorb vast quantities of information quickly and efficiently. The dynamic status indicators show the threat level at each facility and highlight those that have moved to a higher threat level over the preceding 24 hours. Security officials can thus focus on the highest priorities first, taking a proactive and collaborative approach to defense against attacks. The information collected by TrapWire can also be shared with law enforcement agencies to assist in their counterterrorism efforts.***

The company says "the basic premise behind" the technology "is as follows: Through the systematic reporting of suspicious events and the correlation of those events with other event reports for that facility and for related facilities across the network, terrorist surveillance operations can be identified..."

The services Trapwire offers to major corporations and governments can be broken down into three categories (http://www.trapwire.com/trapwire.html): critical infrastructure "hardening", suspicious activity report management, and data mining.

Using open-source information it is very difficult to determine what kinds data-inputs the system accesses. The only confirmed sources of data to the system are CCTV cameras, license plate readers and open source databases. (The latter contain a wealth of information about each and every one of us, so the combination of these three data sets alone is troubling.)

The Wikileaked Stratfor emails that revealed the existence of this shadowy surveillance network to the world contain at least 189 references to Trapwire. They reveal much more about what the program is used for than does the Trapwire public website.

Among the most disturbing emails in the Wikileaks GIF files is this (http://wl.wikileaks-press.org/gifiles/docs/5355966_thought-.html) one, written by a Stratfor analyst to the head of the firm. It gives us a troubling taste of how these private security companies view their role as intermediary between the government and the people:

> ***Regarding SF landmarks of interest–t*hey need something like Trapwire more for threats from activists than from terror threats. *Both are useful, but the activists are ever present around here.***

Look out for more on Trapwire in this space over the coming weeks. There's lots more to dig up on this sprawling security infrastructure and much more to say about its implications for our privacy and democracy, so stay tuned.

Correction/update: DHS funding documents (http://t.co/ygGSg6MK) confirm the agency paid $832,954 to deploy Trapwire in Washington, DC and Seattle, WA. The Northwest Regional Technology Center wrote () in July 2009 that Trapwire "will be piloted in the coming months at several damns [sic] in the Northwest, an international airport, and a neighborhood of office buildings. The technology collects key information without gathering personally protected information. The pilots will assess the utility of the technology for various infrastructure types, identify use and insertion challenges, and determine areas where additional capability would be beneficial." The results of the program would be shared with 11 states and Guam, it says. (h/t @not_me)

EQUIPMENT INVENTORY REPORTS FOR THE SOUTHWEST REGION (TEXAS, NEW MEXICO, ARI	INNOVATIVE EXECUTIONS, LLC	$196,089.42
CONTRACTUAL SUPPORT SERVICES FOR NATIONAL FOSC IN WILLISTON, VT	US INVESTIGATION SERVICES INC	$11,972,919.20
TECHNOLOGY DEMONSTRATION OF TRAPWIRE IN WASHINGTON, DC AND SEATTLE, WA.	ABRAXAS APPLICATIONS, INC.	$832,954.00
DUSO KMD 3 MONTH EXTENSION FOR HSIN-INTEL	THE ESP GROUP, LLC	$393,480.75
CONTRACT NO.: N/A	INTERNATIONAL BUSINESS MACHINES CORPORATION	$322,020.00

(https://2f8dep2znrkt2udzwp1pbyxd-wpengine.netdna-ssl.com/sites/all/images/dhs_seattle_trap.png)

Note: Without the attention and energies of @Asher_Wolf and @not_me, we might not

know about these emails. Follow them for more information on this story as it develops.

PRACTICE PRIVACY (HTTPS://PRIVACYSOS.ORG/TAKE-ACTION/PRACTICE-PRIVACY/)

Security in a Box
Tactical Technology Collective **(https://tacticaltech.org/projects/security-box)**

Encryption Works: How to Protect Your Privacy in the Age of NSA Surveillance
Freedom of the Press Foundation
(https://pressfreedomfoundation.org/encryption-works)

DIY Cybersecurity for Domestic Violence
A resource of privacy + compassion by HACK*BLOSSOM.
(https://hackblossom.org/domestic-violence/)

READ ALL » (HTTPS://PRIVACYSOS.ORG/TAKE-ACTION/PRACTICE-PRIVACY/)

TAKE ACTION

Pass robust state legislation in Massachusetts (https://aclum.org/take-action/contact-elected-officials/)

Pass robust federal legislation (https://action.aclu.org/secure/communities-warzones?ms=web_150408_racialjustice_militarization)

Pass local resolutions in towns and cities (https://privacysos.org/take-action/get-involved/)

SUPPORT ACLUm (https://aclum.org/take-action/give/)

Join ACLUm

find out about upcoming events and follow our latest reports.

Email Address* Zip Code* **SUBMIT**

ACLUm.org (https://aclum.org/) MiACLU.org (https://www.miaclu.org/en)