'Trapwire' an Orwellian social nightmare

by jax *Friday, Aug 24 2012, 1:19am*
international / prose / post

What is of major concern here is the perverse IDEOLOGY behind such projects!

> *Stolen emails from 'security' company Stratfor (published on WikiLeaks) reveal a very disturbing direction certain secretive groups/companies are taking with society in general. The recent revelation seems to reinforce the view that extremely frightened minority ruling elites view the masses as the enemy; the government supported development of comprehensive surveillance packages like 'Trapwire' does not help allay fears of totalitarian forces working behind the scenes with government and regulatory agencies against DEMOCRATIC principles and the best interests of the people.*

Abraxas, mythological Gnostic God that embodies light and dark

Wikileaks uncovers TrapWire surveillance: FAQ

by Zack Whittaker

Wikileaks' latest trove of leaked Stratfor emails details the breadth and potential impact of the TrapWire surveillance system. What is it, and are you affected?

Wikileaks has released as part of its *The Global Intelligence Files* series another vast cache of leaked emails from private intelligence firm Stratfor. Brought to the public eye is a system called TrapWire. This previously little known technology may have the ability to impact our everyday lives in the U.S. and abroad.

This serves as an FAQ to what we know so far.

It's worth noting -- as described below -- Wikileaks has been under a sustained denial-of-service attack, which has left the site unable to load for days, so some links below may not be available at the time of publication.

Here's what you need to know.

What is TrapWire?

In short, TrapWire is surveillance software used by both private industry and the U.S. government and its allies oversees, allowing both public and private sector users to help in counter-terrorism and

anti-crime efforts. The software uses algorithms and data from a variety of surveillance sources -- including CCTV and human-input from spotted 'suspicious' behavior -- to, in essence, 'predict' potentially criminal activity.

One leaked Stratfor-owned document, describes it as follows:

> There are a variety of new tools, such as TrapWire, a software system designed to work with camera systems to help detect patterns of pre-operational surveillance, that can be focused on critical areas to help cut through the fog of noise and activity and draw attention to potential threats.

While ordinary CCTV cameras are often 'passive' and monitored by humans, TrapWire-connected cameras, such as 'pan-tilt-zoom' cameras, are able to track people, along with license plate readers, called Automatic Number Plate Recognition (ANPR) from place to place.

A U.S. Patents and Trademark Office filing says the system is "centralized" and information flows in and out of its global office to 'regional' distribution centers. Despite being owned by a private company, the information collected by the system "can also be shared with law enforcement agencies."

As with any data mining software, the more data that is plugged into the system the greater its effectiveness.

Why such a recent controversy?

Wikileaks' latest release on August 10 of emails from private intelligence group Stratfor suggests the system is global, rather than limited to just the United States.

Simply put: it became increasingly clear how wide and far the extensive use of this software is. If one person is deemed to be acting suspiciously in one TrapWire covered area of the U.S., for example, the software may pick them up elsewhere by a different TrapWire network.

It also means that the surveillance once thought to be relatively passive is instead pre-emptive and sophisticated in its methods. It uses a "10-characteristic description of individuals," human activity, or "8-characteristic description" of vehicle information -- such as license plates and other identifiable marks -- which is then correlated with other information collected elsewhere.

The 'TrapWire Threat Meter' means threats can be passed on through the network while vulnerabilities are not, though nevertheless remains a far more extensive breach of citizen privacy than first considered or understood.

The system appears to be 'for hire' in that it can be bought and used by private industry. For example, in a 2005 interview with former CIA employee (since removed from his corporate profile) and Abraxas founder and chief executive Richard Helms, he says:

> ...the nuclear industry has 104 civilian owned and operated nuclear power plants, and yet they don’t collect or share pre-attack information. TrapWire can help do that without infringing anyone’s civil liberties.

In a 2007 whitepaper, Abraxas describes TrapWire's ability to determine "suspicious activity in less

than 60 seconds."

Who owns TrapWire, and how does it connect with governments?

The TrapWire software is now owned by TrapWire Inc., a Reston, VA company. But it wasn't always.

(Comment was sought from TrapWire Inc. regarding this story, but no reply had been received at the time of writing.)

Abraxas Corp. created TrapWire under its subsidiary firm Abraxas Applications Inc., according to Public Intelligence, a respected research site. Abraxas Corp. trademarked the TrapWire software in a filing with the U.S. PTO in 2006.

But Abraxas Corp. is now owned by Cubic Corporation, which bought the firm in November 2010 for $124 million in cash.

According to one report, Cubic acquired Abraxas Corp., TrapWire's former parent company, after TrapWire was spun out as a separate entity. One of the terms of the acquisition was to "cause the corporate name of Abraxas Applications, Inc. to be changed to a name that does not include 'Abraxas' or any variation thereof."

Abraxas, in a statement released on Monday, said: "Abraxas Corporation then and now has no affiliation with Abraxas Applications now known as TrapWire, Inc."

Abraxas is based in Northern Virginia, according to the trademark filing. Many of its employees -- there are around 60 listed on LinkedIn, but thought to be in the low hundreds -- come from the U.S. military or other public sector organizations, including the U.S. intelligence community.

The U.S. government has given both TrapWire and Abraxas more than $1.6 million in the past 12 months from the Dept. of Homeland Security, Dept. of Defense, and the General Services Administration.

In one leaked email, former Stratfor chief executive and current vice president Fred Burton claims:

> Do you know how much a Lockheed Martin [defense contractor] would pay to have their logo/feed into the USSS CP? MI5? RCMP? LAPD CT? NYPD CT?

This suggests that the NYPD and LAPD counter-terrorism divisions, the U.S. Secret Service, Canada's Royal Canadian Mounted Police and the U.K.'s domestic intelligence agency MI5 are all clientele of the TrapWire service.

Where is TrapWire installed?

The leaks suggest the TrapWire system is installed in major cities on both sides of the Atlantic, such as public places in Washington D.C., New York, Los Angeles, Seattle, and privately owned casinos in Las Vegas.

TrapWire is also implemented in London, U.K., and cities in Canada.

Downing Street, the home and office of the British Prime Minister, would neither confirm nor deny the use of TrapWire despite a leaked email claiming otherwise. However, Scotland Yard, home of London's Metropolitan Police, said it had "no knowledge of any contract or discussion."

London Stock Exchange (LSX) is said to be protected by "heavy surveillance coverages *[sic]* (TrapWire)" and other "predictive software" according to one leaked email.

The LSX did not respond for comment at the time of publication. The White House, also understood to be a TrapWire customer, also did not respond to comment more than a day later.

In another email, claims were made by one British publication that the New York City system was under surveillance by TrapWire. This may have been an exaggeration.

In one leaked email, although the New York subway is mentioned, it suggests a surveillance officer could acquire human intelligence from the subway -- not from technological means, as the system is not used, according to the NYPD -- which can be transformed into structured data in TrapWire to assist in other subway systems, for example, where the system is implemented.

> ...a suspect conducting surveillance of the NYC subway can also be spotted by TrapWire conducting similar activity at the DC subway, connecting the infamous dots. An additional benefit of TrapWire is that the system can also be used to help "walk back the cat" after an attack to identify terrorist suspects and modus operandi.

However, *The New York Times* poured cold water on the suggestions. Speaking to Paul J. Browne, the NYPD chief's spokesperson: "We don't use TrapWire."

Also in the report, the *Times* said:

> TrapWire was tried out on 15 surveillance cameras in Washington and Seattle by the Homeland Security Department, but officials said it ended the trial last year because it did not seem promising.

The report suggests the leaked emails 'boasted' about capabilities and claims some of the links connected by the media are "false."

Do reports collected by TrapWire go to the government?

Yes. Suspicious reports that may indicate a crime or act of terrorism could be committed are passed to 'the government.'

In one example, reports are passed to the FBI but it is not clear outside of the United States whether these are handed to domestic police and intelligence services, or directly back to the U.S. authorities as per Safe Harbor agreements (see below) for distribution through back-channel intelligence networks.

In another leaked email, TrapWire "suspicious activity reports" (SAR) are fed "directly" and "automatically" to the National SAR Initiative, dubbed NSI. They are also passed to the FBI's eGuardian system when a threat to commit crime is identified.

For example, it may be that if a person is identified in two high-target places in a certain time period, this may indicate a terrorist could be planning reconnaissance, but equally a tourist visiting the attractive city sights.

What sort of data can be collected from TrapWire?

The exact details of the data collected by TrapWire are not clear. Video and facial recognition, and human-sourced intelligence, along with automatic license plate reading and other 'points' are collected, but it's safe to assume that vehicle color and a person's ethnicity may be recorded.

In one leaked email, it says:

> [Surveillance] footage can be walked back and track the suspects from the get go with facial recognition software (or TrapWire) technology.

Some news publications suggest there is "no evidence" to suggest facial recognition technology is in use. The email suggests "or TrapWire technology" indicating the possibility -- though not confirmation -- that the software can recognize faces.

Back to *The New York Times'* article, it says a "a privacy statement on the TrapWire Web site says the software does not capture 'personal information'."

However, in a Safe Harbor privacy policy notice, TrapWire may collect:

> "Sensitive Personal Information" means personal information that confirms race, ethnic origin, political opinions, religious or philosophical beliefs, or trade union memberships, or that concerns health or sex life."

It also says:

> Once a suspicious activity in entered into the system it is analyzed and compared with data entered from other areas within a network for the purpose of identifying patterns of behavior that are indicative of pre-attack planning. Generally, no Personal Information or Sensitive Personal Information is recorded by the TrapWire system, and no such information is used by the system to perform its various functions.

"Generally" does not mean "always," however. This often-broad scope definition allows for a wide range of sensitive personal information to be collected, but does not guarantee that it will be. While a person's ethnicity may be collected, a person's sexuality or nationality -- for example -- might be difficult to determine, even by humans.

Does TrapWire scour social networks, such as Twitter or Facebook?

No evidence suggests TrapWire is able to access social media services. There does not appear to be any evidence to suggest TrapWire collects credit or debit card information, cell phone, or Internet-related data.

Who in the technology world enables or powers TrapWire?

Despite the recent news that Microsoft and New York City were partners in a new system that on the face of it appears similar to TrapWire, the two systems are not connected or related.

New York Mayor Michael Bloomberg announced this month the Domain Awareness System, a

system developed with Microsoft, which performs " data aggregation and analysis," according to sister-site *CNET*.

CNET's Elinor Mills wrote:

> "We're finding new ways to leverage already existing cameras, crime data, and other tools to support the work of our investigators, making it easier for them to determine whether a crime is part of an ongoing pattern," Bloomberg said. For example, the system can alert analysts to the presence of suspicious packages and cars while police search for suspects using smart cameras and license plate readers.

Microsoft was not mentioned any of the *The Global Intelligence Files* leaks as far as we can tell.

Another leaked email suggested Salesforce may have been interested in TrapWire, and Google had some "relationship" with the firm.

> Salesforce Hqs in San Fran is interested in TrapWire after I briefed them on their wonderful capabilities

Salesforce said it does not comment on "rumors".

Regarding Google's connection to TrapWire, claims were made that Google had some connection with the company following the search giant's pulling out of China in 2010 over the government's alleged hacking.

> I think the timing is right to revisit our relationship w/GOOGLE and sense growing frustration (and chaos) on their part in light of the Chinese penetrations and intellectual property theft. I've been playing constant phone tag w/their security director, who I believe is traveling.

Google did not comment on the claims.

PC maker chief executive Michael Dell is also mentioned in a number of emails, but the connection is not clear from the context.

If TrapWire is 'centralized,' does it breach EU data protection laws?

The Safe Harbor framework allows for U.S. companies to comply with strict European Union data protection laws. Companies must be certified by the U.S. Department of Commerce.

Because TrapWire Inc. is a U.S.-based company, to operate within the EU, it must comply with the EU's laws. While a Safe Harbor agreement does not prove that TrapWire is used within the 27 member states of Europe, but it does strongly suggest that it is.

From TrapWire's Safe Harbor privacy policy:

> This Policy outlines our general policy and practices regarding personal information

> entered into our United States based systems by European Economic Area (“EEA”) subscribing customers, and personal information entered into our EEA based systems which may be accessed from the United States.

Having said that, under the Patriot Act, it is technically possible for the U.S. government or judiciary to force a wholly owned EU subsidiary of a U.S. parent company to hand over data across the Atlantic, Safe Harbor notwithstanding, without the data subject from being informed, such as the person whose data is collected.

The U.S. Department of Commerce's Safe Harbor certification pages says TrapWire was verified "in-house" -- a valid form of compliance under the rules -- in 2008, and is scheduled for its next certification in 2013.

The certification page says that the United Kingdom comprises the only named "relevant countries from which personal information is received." This suggests a U.K. headquarters or a primary client in the U.K., such as Downing Street, as previously mentioned.

ZDNet's Michael Lee reports that on Wednesday, Sen. Scott Ludlam will ask the Australian Senate to force the Australian government to confirm or deny whether or not it uses TrapWire, and what it knows about the surveillance system.

If TrapWire networks are decentralized, can they communicate with each other?

In one leaked email from Abraxas employee, R. Daniel Botsch explains that:

> If a network has 25 sites, those 25 sites match against each other's reports. They can also send reports to any other site on the network and they can post reports to a network-wide bulletin board.

He notes: "Sites cannot share information across networks." However, there was suggestion back in 2010 that some networks, such as the Las Vegas and the LAPD networks, could eventually merge:

> However, we do cross-network matching here at the office. If we see cross-network matches, we will contact each affected site, explain that the individual(s) or vehicle they reported has been seen on another network, and then offer to put the affected sites into direct contact. We have not yet had a cross-network match. I think over time the different networks will begin to unite."

How did Wikileaks end up with this information?

In late 2011, it was revealed that 'hacktivist' collective Anonymous had stolen a vast cache of emails from Stratfor. These were handed to Wikileaks for analysis and ultimately distribution. Anonymous claimed to have accessed more than 200 gigabytes of data.

In February 2012, Wikileaks said it would begin publishing the 5 million emails. Stratfor founder and chief executive George Friedman described the release as 'deplorable,' but warned, "some of the emails may be forged or altered to include inaccuracies."

In similar vain to the Wikileaks' "Spy Files" and "Syria Files," the leaks were published

incrementally. Anonymous is thought to have also been behind the theft of the Syria Files.

Wikileaks down: Was it under attack?

It's possible, and highly likely. Sister-site *CBS News* reported that Wikileaks said it had suffered a denial-of-service attack that saw the whistleblower's website swamped with visitors that pushed the servers over capacity. The attacks "intensified" earlier this month and expanded to include sites affiliated with Wikileaks. /tabid/78/articleType/ArticleView/articleId/32/Cubic-Agrees-to-Buy-Abraxas-Corporation.aspx">bought the firm in November 2010 for $124 million in cash.

According to one report, Cubic acquired Abraxas Corp., TrapWire's former parent company, after TrapWire was spun out as a separate entity. One of the terms of the acquisition was to "cause the corporate name of Abraxas Applications, Inc. to be changed to a name that does not include 'Abraxas' or any variation thereof."

Abraxas, in a statement released on Monday, said: "Abraxas Corporation then and now has no affiliation with Abraxas Applications now known as TrapWire, Inc."

Abraxas is based in Northern Virginia, according to the trademark filing. Many of its employees -- there are around 60 listed on LinkedIn, but thought to be in the low hundreds -- come from the U.S. military or other public sector organizations, including the U.S. intelligence community.

The U.S. government has given both TrapWire and Abraxas more than