



# Federal Websites Reveal Uncomfortable Corporate Connections with TrapWire

Given the potential flood of legal challenges to its constitutionality, the corporation believed to be behind TrapWire is heading for higher ground, denying any association with the surveillance technology.

In a statement published on its website on August 13, Cubic Corporation attempted to sever the ties binding it to TrapWire. "Cubic Corporation (NYSE: CUB) acquired Abraxas Corporation on December 20, 2010. Abraxas Corporation then and now has no affiliation with Abraxas Applications now known as Trapwire, Inc. Erroneous reports have linked the company with Trapwire, Inc.," the company insisted.



Despite such denials, many are rightly worried about any corporate connection — no matter how tenuous — between Cubic and TrapWire given the former's access to the personal data of Americans through its other corporate interests. The synergy of such access with a massive surveillance apparatus could threaten the privacy of millions, as well as the freedom from unwarranted searches and seizures protected by the Fourth Amendment.

As for the scope and significance of TrapWire, the size of it cannot be exaggerated.

TrapWire is a massive and technologically advanced surveillance system that has the capacity to keep nearly the entire population of this country under the watchful eye of government 24 hours a day. Using this network of cameras and other surveillance tools, the federal government is rapidly constructing an impenetrable, inescapable theater of surveillance, most of which is going unnoticed by Americans and unreported by the mainstream media.

Unlike other elements of the central government's cybersurveillance program, word about TrapWire was not leaked by Obama administration insiders. The details of this nearly unbelievable surveillance scheme were made public by WikiLeaks, the anti-secrecy group founded by Julian Assange. The TrapWire story percolated from the millions of e-mails from the Austin, Texas-based private intelligence-gathering firm Stratfor, published this year by WikiLeaks. Covering correspondence from mid-2004 to 2011, these documents expose Stratfor's "web of informers, pay-off structure, payment-laundering techniques and psychological methods."

This coterie of Stratfor co-conspirators is apparently angry about the leaks, considering that the WikiLeaks servers have been under near-constant <u>Distributed Denial of Service (DDoS) attacks</u> since the TrapWire revelations began attracting notice of alternative journalists. Some outlets report that the cyberattacks are being carried out by agents of the American intelligence community determined to prevent the full depth of this scandal from being explored by reporters.

Exactly what is TrapWire? According to one description of the program, <u>from Russia Today</u>:



### Written by Joe Wolverton, II, J.D. on September 19, 2012



Former senior intelligence officials have created a detailed surveillance system more accurate than modern facial recognition technology — and have installed it across the US under the radar of most Americans, according to emails hacked by Anonymous.

Every few seconds, data picked up at surveillance points in major cities and landmarks across the United States are recorded digitally on the spot, then encrypted and instantaneously delivered to a fortified central database center at an undisclosed location to be aggregated with other intelligence.

Although many of the details remain undisclosed, it is known that the infrastructure of TrapWire was designed and deployed by Abraxas, an intelligence contractor based in northern Virginia headed and run by dozens of former American surveillance officers. As one article described it: "The employee roster at Abraxas reads like a who's who of agents once with the Pentagon, CIA and other government entities according to their public LinkedIn profiles, and the corporation's ties are assumed to go deeper than even documented."

The network is believed to be immense. An article published by transparency advocacy group Public Intelligence claims that Stratfor e-mails suggest that TrapWire is in use by the U.S. Secret Service, the British security service MI5, the Royal Canadian Mounted Police, as well as counterterrorism divisions in both the Los Angeles and New York Police Departments and the LA fusion center. The e-mails also suggest that TrapWire is in use at military bases around the country. A July 2011 email from a "Burton" to others at Stratfor describes how the U.S. Army, Marine Corps, and Pentagon have all begun using TrapWire and are "on the system now." Burton described the Navy as the "next on the list."

One e-mail in a set stolen from global intelligence firm Stratfor by hactivists Anonymous and leaked via WikiLeaks states:

We have an agreement in principle with Abraxas [TrapWire] to provide "streaming sitreps" to their clients via their desktop/homepage by the end of July. Their clients include Scotland Yard, #10 Downing, the White House, and many MNC's [multinational corporations].

As stated above, however, Cubic Corporation refutes these allegations, insisting that it is unrelated and unaccountable for TrapWire and its potential infringements of constitutional liberties.

Evidence <u>published online by privacysos.org</u>, however, appears to make Cubic's claims of innocence a bit more difficult to sustain.

For example, the report by privacysos.org cites a Federal Emergency Management Agency (FEMA) website that names TrapWire as a federally approved purchase and lists Abraxas Applications (a subsidiary of Cubic Corporation) as the point of contact for information about the system. The FEMA website states: "The Products Section includes commercially available product information that has been uploaded directly and voluntarily by the manufacturer."

As the privacysos.org investigation points out, "The company [Abraxas] was still listed on the FEMA website as the contact for TrapWire purchases on Feburary 3, 2011, well after December 20, 2010 when Cubic says Abraxas Corporation totally severed from TrapWire Inc."

Another federal department's online information database also links Cubic with Trapwire. An entry in the U.S. Patent and Trademark Office's website indicates that Abraxas held the trademark for TrapWire until June 23, 2011. This dates also falls after the date Cubic Corporation acquired Abraxas.

The privacysos.org article sums up the impact of the evidence:



### Written by Joe Wolverton, II, J.D. on September 19, 2012



Both the Department of Homeland Security website and the US Trademark Office directly contradict Cubic's denial of any association with Abraxas Applications or TrapWire. If the government's facts are correct, the Abraxas Corporation was managing sales for the TrapWire system at least as recently as February 2011 — meaning Cubic had its hands on both highly sensitive private information on millions of ordinary people and a networked surveillance system sold to governments.

While a preponderance of the evidence points toward the conclusion that Cubic Corporation is purposely publishing inaccurate descriptions of its relationship to TrapWire, there is a need for further investigation before a verdict is reached.

In the meantime, Americans wary of the sprawling surveillance state being supported financially and philosophically by the federal government are right to demand answers. The discrepancy between Cubic's denials and the information provided on two federal websites is sufficient provocation to insist that there be an official inquiry into the inner workings of TrapWire. We the people, as the ultimate sovereigns in this country, are entitled to be apprised of TrapWire's true origins, its integration with the ubiquitous CCTV cameras mounted on poles and buildings, and the use federal agencies are making of the images they are capturing and storing.

With the proliferation of drones and the prediction that by 2020 there will be 30,000 of these powerful all-seeing eyes patrolling the domestic airways, there is a legitimate fear that the addition of thousands of cameras networked together and fed to government agents is worth resisting and investigating before the connection between individual liberty and the Constitution is severed, as well.





## **Subscribe to the New American**

Get exclusive digital access to the most informative, non-partisan truthful news source for patriotic Americans!

Discover a refreshing blend of time-honored values, principles and insightful perspectives within the pages of "The New American" magazine. Delve into a world where tradition is the foundation, and exploration knows no bounds.

From politics and finance to foreign affairs, environment, culture, and technology, we bring you an unparalleled array of topics that matter most.



# **Subscribe**

#### What's Included?

24 Issues Per Year
Optional Print Edition
Digital Edition Access
Exclusive Subscriber Content
Audio provided for all articles
Unlimited access to past issues
Coming Soon! Ad FREE
60-Day money back guarantee!
Cancel anytime.