TRUE ALPHA

Turning Innovation into Profits — One Breakthrough at a Time

The Surveillance State: How to Make Big Brother Work For You

Dear *True Alpha* Readers,

Big Brother is always watching.

Unless you're part of the tin foil hat-wearing brigade and have gone off the grid in a basement somewhere (in which case, how are you reading this?!), this is our reality.

But the truth is, as long as you're not hiding something sinister, the authorities probably aren't concerned about you. They've got bigger fish to fry. And therein lies a big opportunity for investors.

This growing industry has the potential to earn major profits for those who know where to look.

However, in an age when technology is constantly changing, finding the right companies to invest in can be tricky.

There are many up-and-comers… but which ones are truly making a difference? And which ones have staying power?

Those with cutting-edge technology that don't cross the civil rights line between security and snooping are the ones to watch.

Whether they focus on intelligence-gathering and data-collection, or tracking technology that aids in the apprehension of criminals, my Alpha Team is on the case to hunt down the best security stocks.

As the old saying goes, "If you can't beat 'em, join 'em."

Keep in mind that the companies mentioned below are not full True Alpha recommendations and won't be added to our official portfolio. But we'll track them closely and issue any necessary updates.

Ahead of the tape,

Louis Basenese
Investment Director, *True Alpha*

Your iPhone Is Stalking You

By David Dittman

Though we're not as practiced as our counterparts across the Atlantic, the United States has engaged in the art of espionage since long before we had a country to call our own.

For example, Gen. George Washington, commanding the Continental Army during the American Revolutionary War, made extensive and effective use of a spy ring that operated from Long Island and was instrumental in exposing Benedict Arnold's treachery.

Not long after our federal government was constituted, however, our information-gathering efforts metastasized into outright monitoring of the domestic population — full-blown surveillance.

John Adams, the second president of the United States, signed the Alien and Sedition Acts into law in 1798 as we slid toward war with our erstwhile ally France.

The Acts, including a measure to restrict speech critical of the government, were designed to suppress opposition, particularly the Democratic-Republican Party.

Then, during the Civil War, the government, including the U.S. Army, kept watch over groups in the Old Northwest, including the Copperheads, and suppressed activities that would or could threaten the Union war effort.

Organizing the Bureau of Military Information (BMI) and expanding on work begun by the famous Allan Pinkerton was a critical step toward ensuring battlefield success for the Army of the Potomac after 1863.

As our understanding of our destiny expanded to global proportions as a result of World War I and World War II, our intelligence capabilities grew, too.

The Birth of Big Brother

With the National Security Act of 1947, the Office of Strategic Services completed its evolution into the CIA.

Five years later, in 1952, came the National Security Agency (NSA).

Washington's spies informed on Loyalists and detailed British troop deployments using invisible ink and bespoke secret codes.

Adams' agents monitored newspapers for "seditious libel" material such as Rep. Matthew Lyon's essay in the Vermont Journal that, in October 1798, earned him an indictment for publishing letters with the "intent and design" to defame the government and President Adams.

The BMI used hot-air balloons, interviews with captured prisoners and well-placed agents in Confederate territory to gather order-of-battle and troop strength data.

The game-changer — the major breakthrough that took us from nascent hegemon to global empire — was the ability to collect information on a wide scale.

The exploits of "Wild" Bill Donovan's OSS during World War II went several steps further to include more sophisticated acts such as using double agents to protect Allied operations and going "behind the lines" to disrupt enemy operations via sabotage and various guerilla activities.

It was during the second half of the 20th century that counterintelligence, paramilitary operations, assassination and coup organizing became the primary stocks in trade of the American intelligence community.

We've since gone from monitoring pamphlets and commentaries published in newspapers to monitoring real-time communication, both foreign and domestic.

J. Edgar Hoover famously collected information on the rich and powerful, though mostly for his personal aggrandizement. COINTELPRO, the FBI's effort to fight domestic political dissent, took it wide.

The CIA's Operation Mockingbird used the mainstream media to disseminate information and influence the public, violating its charter.

"Total Information Awareness"

Nobody really knew what was going on with the NSA, though, until James Bamford's The Puzzle Palace came out in 1982.

Even back then, the conclusion, as Bamford titled a December 4, 1983 article for The Washington Post Magazine, was that "Big Brother Is Listening."

John Poindexter, who served as deputy national security adviser (1983—85) and national security adviser (1985—86) under President Ronald Reagan, kicked it up a notch with the introduction of the concept of "Total Information Awareness" (TIA) — a "Manhattan Project for Counterterrorism" — in the aftermath of the events of September 11, 2001.

Poindexter was head of the Pentagon's Information Awareness Office (IAO) when he proposed this "vast surveillance database to track terror suspects," according to the Cato Institute.

As Cato reported in January 2003, TIA would:

… according to Poindexter, "break down the stovepipes" that separate commercial and government databases, allowing OIA access to citizens' credit card purchases, travel itineraries, telephone calling records, email, medical histories, and financial information. It would give government the power to generate a comprehensive data profile on any U.S. citizen.

The U.S. Congress defunded TIA and the OIA in late 2003.

But the activities it engaged in were picked up by other government agencies.

We know this thanks to Edward Snowden.

Cyber Warfare Cranks Higher

And we know, thanks to Motherboard, Boing Boing, and The Intercept, that the ability of governments and corporations to monitor your activity and "gather" information about you is only getting more sophisticated.

On August 25, 2016, Motherboard reported the story of "a little-known Israeli surveillance vendor called NSO Group," which is "basically a cyber arms dealer."

One of its co-founders described NSO as "a complete ghost" in a 2013 Defense News article.

As Mike Murray, vice president of research for mobile security company Lookout, told Motherboard: "We realized that we were looking at something that no one had ever seen in the wild before. Literally a click on a link to jailbreak an iPhone in one step. One of the most sophisticated pieces of cyber-espionage software we've ever seen."

NSO's Pegasus malware "basically steals all the information on your phone, it intercepts every call, it intercepts every text message, it steals all the emails, the contacts, the FaceTime calls. It also basically backdoors every communications mechanism you have on the phone.

"It steals all the information in the Gmail app, all the Facebook messages, all the Facebook information, your Facebook contacts, everything from Skype, WhatsApp, Viber, WeChat, Telegram — you name it," said Murray.

The business of selling hacking services and other super-secretive methods of gathering information to governments is growing.

NSO, for example, has pitched to the Mexican government, and the CIA is also interested.

Two weeks after Motherboard published its NSO story, "Someone captured and leaked a live presentation by an RCS sales tech, demonstrating his company's cyber-weapon for spying on dissidents, criminals, and whomever else the customer wanted to infect."

Boing Boing has the video here.

And Sam Biddle reported on September 12, 2016, that The Intercept had come in possession of instruction manuals for Harris Corp.'s Stingray surveillance device.

Stingray is the system by which the police monitor cellular communication. Richard Tynan, a technologist with Privacy International, told The Intercept that "the 'Stingray II' device can impersonate four cellular communications towers at once, monitoring up to four cellular provider networks simultaneously, and with an add-on can operate on so-called 2G, 3G, and 4G networks simultaneously."

According to Tynan, "There really isn't any place for innocent people to hide from a device such as this."

It's easy to assume that official interest is based on NSO's claim that "it can help monitor smartphones of people targeted by government agencies."

Well, we're all targets. That's a 21st-century reality. But it was an 18th-, 19th- and 20th-century reality, too.

If he does nothing else well, The Man knows how to find you.

Smart investing,

David Dittman

How to Profit from Big Brother's Eye in the Sky

By Jonathan Rodriguez

To many people "surveillance" is a dirty word.

Especially when it follows the word "government."

The number of ways the government snoops on its citizens is seemingly growing every day.

It started with wire-tapping and traffic cameras and has expanded to include video monitoring, phone screening, and peeking into files stored on personal computers.

The list goes on.

Generally speaking, law enforcement agencies require a warrant before pilfering through computers or tapping into a person's cellphone.

But one of Uncle Sam's favorite surveillance methods has received a high-tech facelift and is providing a method for much more-than-legal searches…

The Heat is On

Thermal imaging is the visualization of heat that's invisible to the naked eye.

While visible light occupies a small sliver of the electromagnetic spectrum, infrared energy — or heat — spans a much larger range on the spectrum.

Thermal imaging unlocks this hidden band and translates temperature into light that we can see.

In some cases, these technologies can even see heat behind solid objects.

Many industries have employed this technology for a variety of uses.

For example, firefighters use thermal cameras to see through smoke, aiding efforts to locate people in burning buildings or survivors of building collapses.

And the technology is used on buildings to identify insulation failures and overheating electrical units.

But perhaps the biggest users of thermal-imaging systems are law enforcement agencies…

You Can Run… But You Can't Hide

In 2013, Dzhokhar Tsarnaev, one of the Boston Marathon bombers, hid from police inside a boat while on the run.

Working on a tip, a police helicopter fitted with a thermal-imaging camera circled the area — and while police on the ground couldn't see the terrorist, he couldn't hide from the infrared camera, which made his body heat clearly visible through the wood.

But the police aren't the only ones who use the technology.

Because methamphetamine labs produce an extreme amount of heat during the manufacturing process (much more heat than the average building), the Drug Enforcement Agency can fly planes with thermal cameras over a broad area in an effort to locate them.

The practice is questionably legal, but the intelligence gathered on sweeps often leads to search warrants.

The bottom line: The uses for thermal imaging are infinite — and the list of users is growing every day.

In fact, the global thermal-imaging market is expected to grow at a compound annual growth rate (CAGR) of 9.1%, hitting $6.5 billion by 2020, according to Grand View Research.

And this company stands to profit in a big way from thermal imaging's expanded use…

Illuminating the Way to Profits

Founded in 1978, **FLIR Systems Inc.** (FLIR) is one of the world's largest commercial thermal imaging companies.

Historically, the U.S. military, defense, and law enforcement agencies have been the main buyers of the company's high-end infrared imaging systems

But as thermal-imaging systems have become smaller and cheaper, a shift in demand has taken place…

Over the last 10 years, business from commercial clients in the United States has grown at a CAGR of 16% — more than double FLIR's government customer base.

In fact, commercial demand has grown so dramatically that the company now has a portable thermal camera called Flir One that attaches to a smartphone.

As government spending has plateaued slightly, FLIR shares have suffered. And a strong U.S. dollar has crimped the firm's overseas profits.

But now, the stock is priced just right for liftoff…

FLIR has a price-to-book ratio of 2.6 — a 19% discount to the industry average (3.2).

The company also boasts a debt-to-equity ratio of just 0.3 — half the industry average.

On FLIR's robust fundamentals, shares broke out of a two-year downtrend in March 2016, and have rallied since under momentum.

And with a market capitalization of just $4.3 billion, this nimble company has plenty of room to grow.

Now's the time to cash in on the opportunity.

On the hunt,

Jonathan Rodriguez

Are You Smart? If So, You're Being Watched

By Greg Miller

"We don't have to predict what people want. We know what they want."

That's the bold — and, frankly, scary — claim made by the small-cap stock best positioned to profit from the consumer side of surveillance.

The "consumer side" of surveillance, you ask? Oh, yes.

While much attention is given to the government's "surveillance state" and potential abuses of the massive amounts of data being gathered on us, the government is really the least of our worries.

If you're using smart technology in any capacity, there's already an enormous amount of information available about you — your employment, income, education, where you shop, what you buy, your political leanings… everything.

But now technology is emerging that will allow more companies to use that existing data. They can then combine it

with new data in order to build a profile so accurate that it might be able to predict your future actions.

It's intrusive, of course — designed to benefit whatever company is analyzing your data, be it for marketing, politics, or capitalist intentions.

But it's only a shadow of what's to come.

Ultimately, companies will have the ability generate, buy, or rent incomprehensible amounts of data about you.

For example, a car company might use your basic web-browsing and credit data to show ads for their cars. Soon it will be able to send you a personalized offer for exactly the car it thinks you want at the exact moment you're most likely to respond — while you're sitting at the mechanic's shop, for instance.

The challenge for the companies looking to use this data about you for their profit isn't a matter of collecting it — that's already happening at an alarming rate.

No, the challenge is organizing that data and finding patterns that make it useful.

That's where **Cogint Inc.** (COGT) comes in — a company that was rebranded and immediately began trading on the Nasdaq on September 26, 2016.

Reinventing Big Data

Cogint was founded by the father of Big Data, Hank Asher. Unfortunately, when he died in 2013, it sent the company into a tailspin.

However, things are now back on track and Cogint is positioned to help companies use data about you in three ways:

- The company's Fluent subsidiary, acquired at the end of 2015, helps companies decide who to target with online ads, how to do it, and when to do it. The goal is to increase the effectiveness of marketing budgets by giving online advertising companies the ability to advertise only to likely customers. Many companies provide this service, but Fluent has an edge. It's first in mobile — over 80% of its traffic comes from mobile devices, which is where users are taking their attention and business.

- Cogint's IDI business helps creditors find delinqent debtors. If someone has a judgment against them, IDI will find them. It will find out where they live, work, and bank. And whoever is collecting that debt will use that information to get their money. This division also provides identity verification and fraud detection services using much of the same information.

- IDI also provides "data analytics" which combines a company's own information with the huge amount of data that IDI owns or has access to and then generates new insights into a person's behavior — the better to place ads and promote commerce.

Cogint expects that the merging of Fluent's capabilities with IDI's legacy proficiencies to generate even more products in the future.

Cogint is backed by billionaire investor Dr. Philip Frost, who owns 28.65% of the company. Management owns another 23.5%.

Suffice to say, Dr. Frost and management have a lot at stake in Cogint's success. The company's float is also unusually small. That means it won't take much attention from Wall Street to drive Cogint shares higher.

The reimagined and rebranded Cogint is just getting started. Now's a good time to side with Dr. Frost and the company's management team to profit from the combination of Big Data with the surveillance state.

To living and investing in the future,

Greg Miller

Profiting From the Surveillance State… And at the Right Price

By Martin Hutchinson

Of the many companies that provide surveillance capabilities, finding those that both make money and are reasonably valued can be a tricky endeavor.

However, this company fits the bill.

While a great deal of money has poured into "Big Data" companies — both to enhance surveillance and to protect individuals — the problem remains: much of the profit relies on very large government contracts.

Therefore, cyber-security companies like **FireEye** (FEYE) spend huge amounts of money on marketing. In fact, FireEye's general and administrative expenses are almost equal to its revenue — hardly a way to make a profit!

But in an industry teeming with options, Israeli company **NICE Ltd.** (NICE) stands out for its deeply sinister name.

Fighting Crime on Three Fronts

Founded in 1986, the company's slogan is "Enabling Organizations to Operationalize Big Data" — which to lovers of the English language is equally disquieting.

NICE is the world's leading provider of software solutions that enable organizations in a variety of ways:

- **Improve Customer Experience:** Customer experience improvement software includes engagement analytics, handle time and workforce optimization, cross-channel interaction recording, and contact center compliance and fraud prevention.
- **Protect People and Assets:** In the public safety area, NICE is finding a niche in helping first responders and law enforcement. For example, it has an emergency communications contract with New York City.
- **Fight Financial Crime:** In this area, NICE boasts software that combats money laundering, detects and prevents fraud, monitors enterprise risks, and ensures compliance. In financial services, it concentrates on Tier 2 financial institutions, enabling them to protect themselves against financial crime and fraud.

"Nice" Numbers in An Industry That's Only Going to Grow

Unlike many companies in this industry, NICE is actually profitable.

Much of this is due to its broad base of more than 20,000 customers — including more than 80% of Fortune 100 companies. In addition, it concentrates on practical solutions to immediate problems, rather than large projects that could take years to develop.

NICE also has a strong base of recurring revenue. In the 12 months to June 2016, NICE revenue totaled $949 million, with net income from continuing operations of $147 million. Revenue is growing at 9% annually.

Plus, its balance sheet showed no debt and cash of $400 million as of June 2016. Its return on equity was a healthy 10.8%.

The company trades at a reasonable 2.8 times book value and pays a modest 1% dividend, too.

NICE is well-positioned to profit from the ongoing (and intensifying) fight against financial crime, as well as increasing demand for its surveillance products in general.

Whether or not you approve of the "surveillance state," it's increasingly inevitable in today's world and — if nothing else — NICE is, well, a nice investment in a pretty cruel market.

Good investing,

Martin Hutchinson