GlobalResearch
Center for Research on Globalization

NSA Spying Directly Harms Internet Companies, Silicon Valley, California … And the Entire U.S. Economy

By Washington's Blog
Global Research, July 31, 2013
Washington's Blog

Theme: Global Economy, Intelligence

Mass surveillance by the NSA may *directly harm* the bottom of line of Internet companies, Silicon Valley, California … and the entire national economy.

Money News points out:

> The company whose shares you own may be lying to you — while Uncle Sam looks the other way.
>
> Let's step through this. I think you will see the problem.
>
> Fact 1: U.S. financial markets are the envy of the world because we have fair disclosure requirements, accounting standards and impartial courts. This is the foundation of shareholder value. The company may lose money, but they at least told you the truth.
>
> Fact 2: We now know multiple public companies, including Microsoft (MSFT), Google (GOOG), Facebook (FB) and other, gave their user information to NSA. Forget the privacy implications for a minute. Assume for the sake of argument that everything complies with U.S. law. Even if true, the businesses may still be at risk.
>
> Fact 3: All these companies operate globally. They get revenue from China, Japan, Russia, Germany, France and everywhere else. Did those governments consent to have their citizens monitored by the NSA? I think we can safely say no.
>
> Politicians in Europe are especially outraged. Citizens are angry with the United States and losing faith in American brand names. Foreign companies are already using their non-American status as a competitive advantage. Some plan to redesign networks specifically to bypass U.S. companies.
>
> By yielding to the NSA, U.S. companies likely broke laws elsewhere. They could face penalties and lose significant revenue. Right or wrong, their decisions could well have damaged the business.
>
> Securities lawyers call this "materially adverse information" and companies are required to disclose it. But they are not. Only chief executives and a handful of technical people know when companies cooperate with the NSA. If the CEO can't even tell his own board members he has placed the company at risk, you can bet it won't be in the annual report.
>
> The government also gives some executives immunity documents, according

> to Bloomberg. Immunity is unnecessary unless someone thinks they are breaking the law. So apparently, the regulators who ostensibly protect the public are actively helping the violators.
>
> This is a new and different investment landscape. Public companies are hiding important facts that place their investors at risk. If you somehow find out, you will have no recourse because regulators gave the offender a "get out of jail free" card. The regulatory structure that theoretically protects you knowingly facilitates deception that may hurt you, and then silences any witnesses.
>
> This strikes to the very heart of the U.S. financial system. Our markets have lost any legitimate claim to "full and fair disclosure." Every prospectus, quarterly report and news release now includes an unwritten NSA asterisk. Whenever a CEO speaks, we must assume his fingers are crossed.
>
> ***
>
> Every individual investor or money manager now has a new risk factor to consider. Every disclosure by every company is in doubt. The rule of law that gave us the most-trusted markets in the world may be just an illusion.

In a subsequent article, Money News wrote:

> Executives at publicly traded companies are lying to shareholders and probably their own boards of directors. They are exposing your investments to real, material, hard-dollar losses and not telling you.
>
> The government that allegedly protects you, Mr. Small Investor, knows all this and actually encourages more of it.
>
> Who lies? Ah, there's the problem. We don't know. Some people high in the government know. The CEOs themselves and a few of their tech people know. You and I don't get to know. We just provide the money.
>
> Since we don't know which CEOs are government-approved liars, the prudent course is to assume all CEOs are government-approved liars. We can no longer give anyone the benefit of the doubt.
>
> If you are a money manager with a fiduciary responsibility to your investors, you are hereby on notice. A CEO may sign those Securities and Exchange Commission filings where you get corporate information with his fingers crossed. Your clients pay you to know the facts and make good decisions. You're losing that ability.
>
> For example, consider a certain U.S. telecommunications giant with worldwide operations. It connects American businesses with customers everywhere. Fast-growing emerging markets like Brazil are very important to its future growth.
>
> Thanks to data-sharing agreements with various phone providers in Brazil, this company has deep access to local phone calls. One day someone from NSA calls up the CEO and asks to tap into that stream. He says OK, tells his engineers to do it and moves on.
>
> A few years later, Edward Snowden informs Brazilian media that U.S. intelligence is capturing these data. They tell the Brazilian public. It is not happy. Nor are its politicians, who are already on edge for entirely unrelated reasons.

What would you say are this company's prospects for future business in Brazil? Your choices are "slim" and "none." They won't be the only ones hurt. If the U.S. government won't identify which American company cheated its Brazilian partners, Brazil will just blame all of them. The company can kiss those growth plans good-bye.

This isn't a fantasy. It is happening right now. The legality of cooperating with the NSA within the United States is irrelevant. Immunity letters in the United States do not protect the company from liability elsewhere.

***

Shouldn't shareholders get to know when their company's CEO takes these risks? Shouldn't the directors who hire the CEO have a say in the matter? Yes, they should. We now know that they don't.

The trust that forms the bedrock under U.S. financial markets is crumbling. [A theme wefrequently explore.] If we cannot believe CEOs when they swear to tell the truth, if companies can hide material risks, if boards cannot know what the executives they hire are actually doing, any pretense of "fair markets" is gone.

When nothing is private, people and businesses soon cease to trust each other. Without trust, modern financial markets cannot function properly.

If U.S. disclosure standards are no better than those in the third world, then every domestic stock is overvalued. Our "rule of law" premium is gone.

This means a change for stock valuations — and it won't be bullish.

CNN reports:

Officials throughout Europe, most notably French President Francois Hollande, said that NSA spying threatens trade talks.

***

For the Internet companies named in reports on NSA surveillance, their bottom line is at risk because European markets are crucial for them. It is too early assess the impact on them, but the stakes are clearly huge. For example, Facebook has about 261 million active monthly European users, compared with about 195 million in the U.S. and Canada, and 22% of Apple's net income came from Europe in the first quarter of 2013.

***

In June 2011, Microsoft admitted that the United States could bypass EU privacy regulations to get vast amounts of cloud data from their European customers. Six months later, BAE Systems, based in the United Kingdom, stopped using the company's cloud services because of this issue.

***

The NSA scandal has brought tensions over spying to a boil. German prosecutors may open a criminal investigation into NSA spying. On July 3, Germany's interior minister said that people should stop using companies like Google and Facebook if they fear the U.S. is intercepting their data. On July 4,

> the European Parliament condemned spying on Europeans and ordered an investigation into mass surveillance. The same day, Neelie Kroes, the EU's chief telecom and Internet official, warned of "multi-billion euro consequences for American companies" because of U.S. spying in the cloud.
>
> ***
>
> Transparency is an important first step. Its absence only exacerbates a trust deficit that companies already had in Europe. And trust is crucial. Google's chief legal officer recognized this on June 19 when he said, "Our business depends on the trust of our users," during a Web chat about the NSA scandal. Some companies have been aggressive in trying to disclose more, and others have not. But unless the U.S. government loosens strictures and allows greater disclosure, all U.S. companies are likely to suffer the backlash.
>
> ***
>
> The Obama administration needs to recognize and mitigate the serious economic risks of spying while trying to rebuild its credibility on Internet freedom. The July 9 hearing of the Privacy and Civil Liberties Oversight Board is a start, but much more is needed. More disclosure about the surveillance programs, more oversight, better laws, and a process to work with allied governments to increase privacy protections would be a start.
>
> The European customers of Internet companies are not all al Qaeda or criminals, but that is essentially how U.S. surveillance efforts treat them. If this isn't fixed, this may be the beginning of a very costly battle pitting U.S. surveillance against European business, trade, and human rights.

The Atlantic notes:

> Most communications flow over the Internet and a very large percentage of key Internet infrastructure is in the United States. Thus, foreigners' communications are much more likely to pass through U.S. facilities even when no U.S. person is a party to a particular message. Think about a foreigner using Gmail, or Facebook, or Twitter — billions of these communications originate elsewhere in the world but pass through, and are stored on, servers located in the U.S.
>
> ***
>
> Foreigners … comprise a growing majority of any global company's customers.
>
> ***
>
> From the perspective of many foreign individuals and governments, global Internet companies headquartered in the U.S. are a security and privacy risk. And that means foreign governments offended by U.S. snooping are already looking for ways to make sure their citizens' data never reaches the U.S. without privacy concessions. We can see the beginnings of this effort in the statement by the vice president of the European Commission, Viviane Reding, who called in her June 20 op-ed in the New York Times for new EU data protection rules to "ensure that E.U. citizens' data are transferred to non-European law enforcement authorities only in situations that are well defined, exceptional and subject to judicial review." While we cheer these limits on government access, the spying scandal also puts the U.S. government and American companies at a disadvantage in ongoing discussions with the EU about upcoming changes to its law enforcement and consumer-privacy-focused data directives, negotiations critical to the Internet industry's ongoing

> operations in Europe.
>
> Even more troubling, some European activists are calling for data-storage rules to thwart the U.S. government's surveillance advantage. The best way to keep the American government from snooping is to have foreigners' data stored locally so that local governments – and not U.S. spy agencies — get to say when and how that data may be used. And that means nations will force U.S.-based Internet giants like Google, Facebook, and Twitter, to store their user data in-country, or will redirect users to domestic businesses that are not so easily bent to the American government's wishes.
>
> So the first unintended consequence of mass NSA surveillance may be to diminish the power and profitability of the U.S. Internet economy. America invented the Internet, and our Internet companies are dominant around the world. The U.S. government, in its rush to spy on everybody, may end up killing our most productive golden goose.

(Internet companies comprise the most vibrant sector of our economy.)

San Diego Union-Tribune writes:

> California and its businesses have a problem. It's called the National Security Agency.
>
> ***
>
> The problem for California is not that the feds are collecting all of our communications. It is that the feds are (totally unapologetically) doing the same to foreigners, especially in communications with the U.S. California depends for its livelihood on people overseas — as customers, trade partners, as sources of talent. Our leading industries — shipping, tourism, technology, and entertainment — could not survive, much less prosper, without the trust and goodwill of foreigners. We are home to two of the world's busiest container ports, and we are a leading exporter of engineering, architectural, design, financial, insurance, legal, and educational services. All of our signature companies — Apple, Google, Facebook, Oracle, Intel, Hewlett-Packard, Chevron, Disney — rely on sales and growth overseas. And our families and workplaces are full of foreigners; more than one in four of us were born abroad, and more than 50 countries have diaspora populations in California of more than 10,000.
>
> ***
>
> News that our government is collecting our foreign friends' phone records, emails, video chats, online conversations, photos, and even stored data, tarnishes the California and American brands.
>
> ***
>
> Will tourists balk at visiting us because they fear U.S. monitoring? Will overseas business owners think twice about trading with us because they fear that their communications might be intercepted and used for commercial gain by American competitors? Most chilling of all: Will foreigners stop using the products and services of California technology and media companies — Facebook, Google, Skype, and Apple among them — that have been accomplices (they say unwillingly) to the federal surveillance?
>
> The answer to that last question: Yes. It's already happening. Asian

> governments and businesses are now moving their employees and systems off Google's Gmail and other U.S.-based systems, according to Asian news reports. German prosecutors are investigating some of the American surveillance. The issue is becoming a stumbling block in negotiations with the European Union over a new trade agreement. Technology experts are warning of a big loss of foreign business.
>
> John Dvorak, the PCMag.com columnist, wrote recently, "Our companies have billions and billions of dollars in overseas sales and none of the American companies can guarantee security from American spies. Does anyone but me think this is a problem for commerce?"
>
> ***
>
> It doesn't help when our own U.S. Sen. Dianne Feinstein is backing the surveillance without acknowledgment of the huge potential costs to her state.
>
> It's time for her and House Minority Leader Nancy Pelosi, who has been nearly as tone-deaf on this issue, to be forcefully reminded that protecting California industry, and the culture of openness and trust that is so vital to it, is at least as important as protecting massive government data-mining. Such reminders should take the force not merely of public statements but of law.
>
> California has a robust history of going its own way — on vehicle standards, energy efficiency, immigration, marijuana. Now is the time for another departure — this one on the privacy of communications.
>
> ***
>
> We need laws, perhaps even a state constitutional amendment, to make plain that California considers the personal data and communications of all people, be they American or foreign, to be private and worthy of protection.

And see this.

The bigger picture is that a country's economic health is correlated with a strong rule of law more than*any other factor*.

Yet America has rapidly fallen into a state of lawlessness, where fundamental rights – such as protection against mass spying by the government – have been jettisoned.

The government is spying on just about *everything* we do. Even the government's attempted denials of this fact confirm it.
