GlobalResearch
Center for Research on Globalization

The Government Is Spying On ALL Americans' Digital and Old-Fashioned Communications

Anyone Who Says the Government Only Spies On Potential Bad Guys Is Sadly Uninformed

By Washington's Blog
Global Research, July 12, 2013
Washington's Blog

Region: USA
Theme: Intelligence, Police State & Civil Rights

Even now – after all of the revelations by Edward Snowden and other whistleblowers – spying apologists say that the reports are "exaggerated" or "overblown", and that the government only spies on potential bad guys.

In reality, the government is spying on everyone's digital and old-fashioned communications.

For example, the government is photographing the outside information on every piece of snail mail.

The government is spying on you through your phone ... and may even remotely turn on your camera and microphone when your phone is off.

As one example, the NSA has inserted its code into Android's operating system ... bugging *three-quarters of the world's smartphones*. Google – or the NSA – can remotely turn on your phone's camera and recorder at any time.

Cell towers track where your phone is at any moment, and the major cell carriers, including Verizon and AT&T, responded to at least 1.3 million law enforcement requests for cell phone locations and other data in 2011. (And – given that your smartphone routinely sends your location information back to Apple or Google – it would be child's play for the government to track your location that way.) Your iPhone, orother brand of smartphone is spying on virtually everything you do (ProPublica notes: "That's No Phone. That's My Tracker").

The government might be spying on you through your computer's webcam or microphone. The government might also be spying on you through the "smart meter" on your own home.

The FBI wants a backdoor to *all* software. But leading European computer publication Heise said in 1999 that the NSA had *already* built a backdoor into *all Windows software*.

And Microsoft has long worked hand-in-hand with the NSA and FBI so that encryption doesn't block the government's ability to spy on users of Skype, Outlook, Hotmail and other Microsoft services.

(And leading security experts say that the NSA might have put a backdoor in all encryption standards years ago. ... meaning that the NSA can easily hack into encrypted communications.)

"Black boxes" are currently installed in between 90% and 96% of all new cars. And starting in 2014, all new cars will include black boxes that can track your location.

License plate readers mounted on police cars allow police to gather millions of records on drivers ... including photos of them in their cars.

If you have a microphone in your car, that might also open you up to snoopers. As CNET points out:

> Surreptitious activation of built-in microphones by the FBI has been done before. A 2003 lawsuit revealed that the FBI was able to surreptitiously turn on the built-in microphones in automotive systems like General Motors' OnStar to snoop on passengers' conversations.
>
> When FBI agents remotely activated the system and were listening in, passengers in the vehicle could not tell that their conversations were being monitored.

A security expert and former NSA software developer says that hackers can access *private* surveillance cameras. Given that the NSA apparently already monitors public cameras using facial recognition software, and that the FBI is building a system which will track "public and *private* surveillance cameras around the country", we can assume that government agencies might already be hacking into private surveillance cameras.

The CIA wants to spy on you through your dishwasher and other "smart" appliances. As Slate notes:

> Watch out: the CIA may soon be spying on you—through your beloved, intelligent household appliances, according to Wired.
>
> In early March, at a meeting for the CIA's venture capital firm In-Q-Tel, CIA Director David Petraeus reportedly noted that "smart appliances" connected to the Internet could someday be used by the CIA to track individuals. If your grocery-list-generating refrigerator knows when you're home, the CIA could, too, by using geo-location data from your wired appliances, according to SmartPlanet.
>
> "The current 'Internet of PCs' will move, of course, toward an 'Internet of Things'—of devices of all types—50 to 100 billion of which will be connected to the Internet by 2020," Petraeus said in his speech. He continued:
>
> > Items of interest will be located, identified, monitored, and remotely controlled through technologies such as radio-frequency identification, sensor networks, tiny embedded servers, and energy harvesters—all connected to the next-generation Internet using abundant, low cost, and high-power computing—the latter now going to cloud computing, in many areas greater and greater supercomputing, and, ultimately, heading to quantum computing.
>
> ***
>
> ITworld's Kevin Fogarty thinks that J. Edgar Hoover, were he still with us, would

"die of jealousy" upon hearing about the tools soon to be at Petraeus' disposal.

And they're probably bluffing and exaggerating, but the Department of Homeland Security claims they will soon be able to know your adrenaline level, what you ate for breakfast and what you're thinking ...from 164 feet away. (In addition, people will probably soon be swallowing tracking devices for medical purposes)

The government is allegedly scanning prisoners' brains without their consent at Guantanamo. In the near future, brain scanners may be able to literally read our thoughts (and see this).

The government is currently testing systems for use in public spaces which can screen for "pre-crime". As Nature reports:

> Like a lie detector, FAST measures a variety of physiological indicators, ranging from heart rate to the steadiness of a person's gaze, to judge a subject's state of mind. But there are major differences from the polygraph. FAST relies on non-contact sensors, so it can measure indicators as someone walks through a corridor at an airport, and it does not depend on active questioning of the subject.

CBS News points out:

> FAST is designed to track and monitor, among other inputs, body movements, voice pitch changes, prosody changes (alterations in the rhythm and intonation of speech), eye movements, body heat changes, and breathing patterns. Occupation and age are also considered. A government source told CNET that blink rate and pupil variation are measured too.
>
> A field test of FAST has been conducted in at least one undisclosed location in the northeast. "It is not an airport, but it is a large venue that is a suitable substitute for an operational setting," DHS spokesman John Verrico told Nature.com in May.
>
> Although DHS has publicly suggested that FAST could be used at airport checkpoints–the Transportation Security Administration is part of the department, after all–the government appears to have grander ambitions. One internal DHS document (PDF) also obtained by EPIC through the Freedom of Information Act says a mobile version of FAST "could be used at security checkpoints such as border crossings or at large public events such as sporting events or conventions."

The risk of false positives is very real. As Computer World notes:

> Tom Ormerod, a psychologist in the Investigative Expertise Unit at Lancaster University, UK, told Nature, "Even having an iris scan or fingerprint read at immigration is enough to raise the heart rate of most legitimate travelers." Other critics have been concerned about "false positives." For example, some travelers might have some of the physical responses that are supposedly signs of mal-intent if they were about to be groped by TSA agents in airport security.

Various "pre-crime" sensing devices have already been deployed in public spaces in the U.S.

The government has also worked on artificial intelligence for "pre-crime" detection on the Web. And given that programs which can figure out your emotions are being developed using your webcam, every change in facial expression could be tracked.

According to the NSA's former director of global digital data – William Binney – the NSA's new data storage center in Utah will have so much storage capacity that:

> "They would have plenty of space ... to store at least something on the order of 100 years worth of the worldwide communications, phones and emails and stuff like that," Binney asserts, "and then have plenty of space left over to do any kind of parallel processing to try to break codes."
>
> ***
>
> [But the NSA isn't stopping there.] Despite its capacity, the Utah center does not satisfy NSA's data demands. Last month, the agency broke ground on its next data farm at its headquarters at Ft. Meade, Md. But that facility will be only two-thirds the size of the mega-complex in Utah.

The NSA is building next-generation quantum computers to process all of the data.

NBC News reports:

> NBC News has learned that under the post-9/11 Patriot Act, the government has been collecting records on every phone call made in the U.S.

This includes metadata ... which can tell the government a *lot* about you. And it also includes content.

The documents leaked by Edward Snowden to Glenn Greenwald show:

> But what we're really talking about here is a localized system that prevents any form of electronic communication from taking place without its being stored and monitored by the National Security Agency.
>
> It doesn't mean that they're listening to every call, it means they're storing every call and have the capability to listen to them at any time, and it does mean that they're collecting millions upon millions upon millions of our phone and email records.

In addition, a government expert told the Washington Post that the government "quite literally can watch your ideas form as you type." A top NSA executive confirmed to Washington's Blog that the NSA is intercepting and storing virtually *all digital communications* on the Internet.

McClatchy notes:

> FBI Director Robert Mueller told a Senate committee on March 30, 2011, that "technological improvements" now enable the bureau "to pull together past emails and future ones as they come in so that it does not require an individualized search."

> The administration is building a facility in a valley south of Salt Lake City that will have the capacity to store massive amounts of records – a facility that former agency whistleblowers say has no logical purpose if it's not going to be a vault holding years of phone and Internet data.
>
> ***
>
> Thomas Drake, a former NSA senior executive who challenged the data collection for several years, said the agency's intent seems obvious.
>
> "One hundred million phone records?" he asked in an interview. "Why would they want that each and every day? Of course they're storing it."
>
> ***
>
> Lending credence to his worries, The Guardian's latest report quoted a document in which Alexander purportedly remarked during a 2008 visit to an NSA intercept station in Britain: "Why can't we collect all the signals all the time?"
>
> ***
>
> One former U.S. security consultant, who spoke on condition of anonymity to protect his connections to government agencies, told McClatchy he has seen agency-installed switches across the country that draw data from the cables.
>
> "Do I know they copied it? Yes," said the consultant. "Do I know if they kept it? No."

NSA whistleblower Russel Tice – a key source in the 2005 New York Times report that blew the lid off the Bush administration's use of warrantless wiretapping – says that the *content* and metadata of *all* digital communications are being tapped by the NSA.

The NSA not only accesses data directly from the largest internet companies, it also sucks up huge amounts of data straight from undersea cables providing telephone and Internet service to the United States.

After all, the government has secretly interpreted the Patriot Act so that "everything" is deemed relevant ... so the government can spy on *everyone*.

The NSA isn't the only agency which is conducting massive spying.

The Wall Street Journal notes:

> The rules now allow the little-known National Counterterrorism Center to ... copy entire government databases—flight records, casino-employee lists, the names of Americans hosting foreign-exchange students and many others. The agency has new authority to keep data about innocent U.S. citizens for up to five years, and to analyze it for suspicious patterns of behavior. Previously, both were prohibited. Data about Americans "reasonably believed to constitute terrorism information" may be permanently retained.
>
> The changes also allow databases of U.S. civilian information to be given to foreign governments for analysis of their own. In effect, U.S. and foreign governments would be using the information to look for clues that people might commit future crimes.

> "It's breathtaking" in its scope, said a former senior administration official familiar with the White House debate.

Reason notes:

> Gazillions. That's the number of times the federal government has spied on Americans since 9/11 through the use of drones, legal search warrants, illegal search warrants, federal agent-written search warrants and just plain government spying. This is according to Sen. Rand Paul, R-Ky., who, when he asked the government to tell him what it was doing to violate our privacy, was given a classified briefing. The senator — one of just a few in the U.S. Senate who believes that the Constitution means what it says — was required by federal law to agree not to reveal what spies and bureaucrats told him during the briefing.

Even if the US government weren't recording all of that data, England's GCHQ spy agency is … and issharing it with the NSA.

Germany, Australia, Canada and New Zealand are also recording and sharing massive amounts of information with the NSA.

Private contractors can also view all of your data … and the government isn't keeping track of which contractors see your data and which don't. And because background checks regarding some contractors are falsified, it is hard to know the types of people that might have your information.

And top NSA and FBI experts say that the government can *retroactively* search all of the collected information on someone since 9/11 if they suspect someone of wrongdoing … or want to frame him.

The American government is in fact collecting and storing virtually every phone call, purchases, email, text message, internet searches, social media communications, health information, employment history, travel and student records, and virtually all other information of every American.

The Wall Street Journal reported that the NSA spies on Americans' credit card transactions. Senators Wyden and Udall – both on the Senate Intelligence Committee, with access to all of the top-secret information about the government's spying programs – write:

> Section 215 of the Patriot Act can be used to collect any type of records whatsoever … including information on credit card purchases, medical records, library records, firearm sales records, financial information and a range of other sensitive subjects.

Many other government agencies track your credit card purchases as well. In fact, *all* U.S. intelligence agencies – including the CIA and NSA – are going to spy on Americans' finances.

The IRS will be spying on Americans' shopping records, travel, social interactions, health records and filesfrom other government investigators.

The Consumer Financial Protection Board will also spy on the finances of millions of

Americans.

As Washington Monthly noted in 2004, Congress chopped off the head of the Total Information Awareness program ... but the program returned as a many-headed hydra:

> A program can survive even when the media, the public, and most of Congress wants it killed. It turns out that, while the language in the bill shutting down TIA was clear, a new line had been inserted during conference—no one knew by whom—allowing "certain processing, analysis, and collaboration tools" to continue.
>
> ....Thanks to the Central Intelligence Agency and the National Security Agency, which had lobbied for the provision, TIA didn't die—it metastasized. As the AP reported in February [of 2004], the new language simply outsourced many TIA programs to other intelligence offices and buried them in the so-called "black budget." What's more, today, several agencies are pursuing data mining projects independent of TIA, including the Department of Homeland Security, the Justice Department, the CIA, the Transportation Security Administration, and NASA....Even with TIA ostensibly shut down, many of the private contractors who worked on the program can continue their research with few controls.

The government is flying drones over the American homeland to spy on us. Indeed, the head of the FBI told Congress that drones are used for domestic surveillance ... and that there are *no rules in place* governing spying on Americans with drones.

Senator Rand Paul correctly notes:

> The domestic use of drones to spy on Americans clearly violates the Fourth Amendment and limits our rights to personal privacy.

Emptywheel notes in a post entitled "The OTHER Assault on the Fourth Amendment in the NDAA? Drones at Your Airport?":

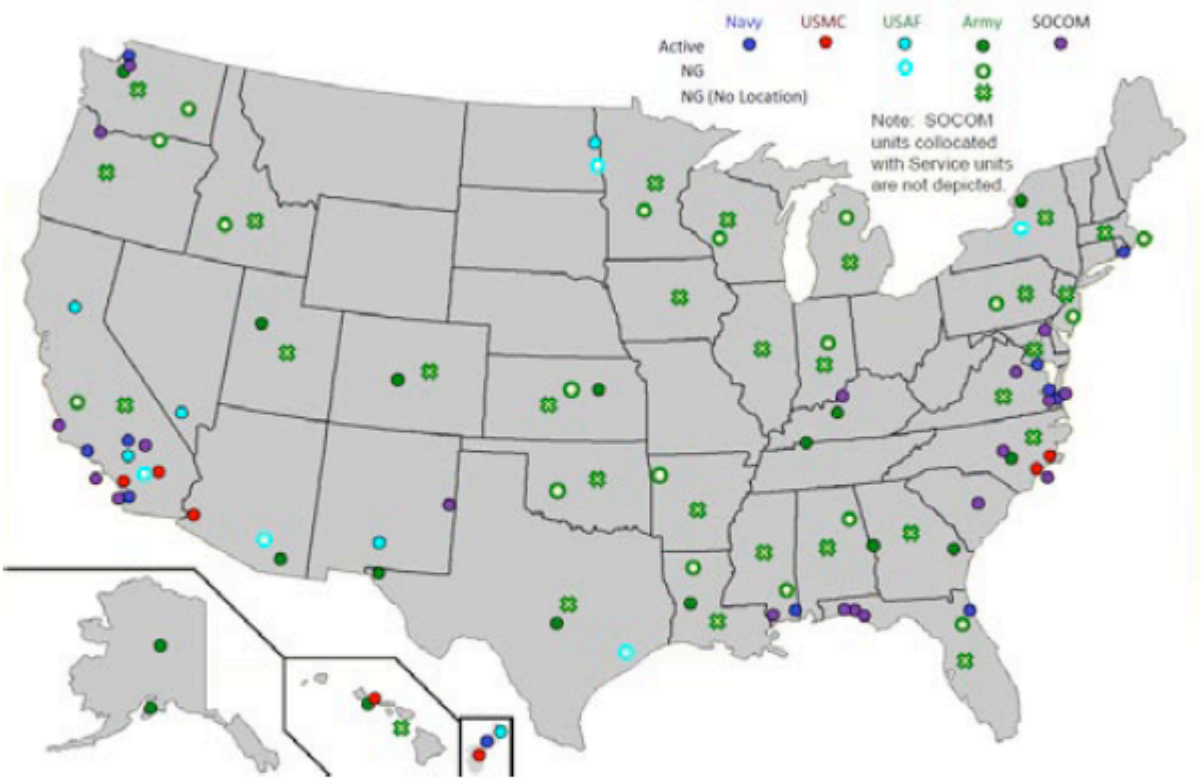

Figure 2: Planned DoD 2015 UAS Locations

> ***
>
> As the map above makes clear–taken from this 2010 report–DOD [the Department of Defense] plans to have drones all over the country by 2015.

Many police departments are also using drones to spy on us. As the Hill reported:

> At least 13 state and local police agencies around the country have used drones in the field or in training, according to the Association for Unmanned Vehicle Systems International, an industry trade group. The Federal Aviation Administration has predicted that by the end of the decade, 30,000 commercial and government drones could be flying over U.S. skies.
>
> ***
>
> "Drones should only be used if subject to a powerful framework that regulates their use in order to avoid abuse and invasions of privacy," Chris Calabrese, a legislative counsel for the American Civil Liberties Union, said during a congressional forum in Texas last month.
>
> He argued police should only fly drones over private property if they have a warrant, information collected with drones should be promptly destroyed when it's no longer needed and domestic drones should not carry any weapons.
>
> He argued that drones pose a more serious threat to privacy than helicopters because they are cheaper to use and can hover in the sky for longer periods of

> time.
>
> A congressional report earlier this year predicted that drones could soon be equipped with technologies to identify faces or track people based on their height, age, gender and skin color.

The military is paying for the development of drones with facial recognition software which "remember" people's faces ... and read "malintent".

Moreover, Wired reports:

> Transit authorities in cities across the country are quietly installing microphone-enabled surveillance systems on public buses that would give them the ability to record and store private conversations....
>
> The systems are being installed in San Francisco, Baltimore, and other cities with funding from the Department of Homeland Security in some cases ....
>
> The IP audio-video systems can be accessed remotely via a built-in web server (.pdf), and can be combined with GPS data to track the movement of buses and passengers throughout the city.
>
> ***
>
> The systems use cables or WiFi to pair audio conversations with camera images in order to produce synchronous recordings. Audio and video can be monitored in real-time, but are also stored onboard in blackbox-like devices, generally for 30 days, for later retrieval. Four to six cameras with mics are generally installed throughout a bus, including one near the driver and one on the exterior of the bus.
>
> ***
>
> Privacy and security expert Ashkan Soltani told the Daily that the audio could easily be coupled with facial recognition systems or audio recognition technology to identify passengers caught on the recordings.

RT notes:

> Street lights that can spy installed in some American cities
>
> America welcomes a new brand of smart street lightning systems: energy-efficient, long-lasting, complete with LED screens to show ads. They can also spy on citizens in a way George Orwell would not have imagined in his worst nightmare.
>
> With a price tag of $3,000+ apiece, according to an ABC report, the street lights are now being rolled out in Detroit, Chicago and Pittsburgh, and may soon mushroom all across the country.
>
> Part of the Intellistreets systems made by the company Illuminating Concepts, they havea number of "homeland security applications" attached.
>
> Each has a microprocessor "essentially similar to an iPhone," capable ofwireless communication. Each can capture images and count people for the police through a digital camera, record conversations of passers-by and even

give voice commands thanks to a built-in speaker.

Ron Harwood, president and founder of Illuminating Concepts, says he eyed the creation of such a system after the 9/11 terrorist attacks and the Hurricane Katrina disaster. He is"working with Homeland Security" to deliver his dream of making people "more informed and safer."

The TSA has moved way past airports, trains and sports stadiums, and is deploying mobile scanners to spy on people all over the place. This means that traveling within the United States is no longer a private affair.

You might also have seen the news this week that the Department of Homeland Security is going to*continue* to allow searches of laptops and phones based upon "hunches".

What's that about?

The ACLU published a map in 2006 showing that nearly two-thirds of the American public – 197.4 million people – live within a "constitution-free zone" within 100 miles of land and coastal borders:

The ACLU explained:

- Normally under the Fourth Amendment of the U.S. Constitution, the American people are not generally subject to random and arbitrary stops and searches.

- The border, however, has always been an exception. There, the longstanding view is that the normal rules do not apply. For example the authorities do not

need a warrant or probable cause to conduct a “routine search.”

- But what is “the border”? According to the government, it is a 100-mile wide strip that wraps around the “external boundary” of the United States.

- As a result of this claimed authority, individuals who are far away from the border, American citizens traveling from one place in America to another, are being stopped and harassed in ways that our Constitution does not permit.

- Border Patrol has been setting up checkpoints inland — on highways in states such as California, Texas and Arizona, and at ferry terminals in Washington State. Typically, the agents ask drivers and passengers about their citizenship. Unfortunately, our courts so far have permitted these kinds of checkpoints – legally speaking, they are “administrative” stops that are permitted only for the specific purpose of protecting the nation’s borders. They cannot become general drug-search or other law enforcement efforts.

- However, these stops by Border Patrol agents are not remaining confined to that border security purpose. On the roads of California and elsewhere in the nation – places far removed from the actual border – agents are stopping, interrogating, and searching Americans on an everyday basis with absolutely no suspicion of wrongdoing.

- The bottom line is that the extraordinary authorities that the government possesses at the border are spilling into regular American streets.

Computer World reports:

> Border agents don’t need probable cause and they don’t need a stinking warrant since they don’t need to prove any reasonable suspicion first. Nor, sadly, do two out of three people have First Amendment protection; it is as if DHS has voided those Constitutional amendments and protections they provide to nearly 200 million Americans.
>
> ***
>
> Don’t be silly by thinking this means only if you are physically trying to cross the international border. As we saw when discussing the DEA using license plate readers and data-mining to track Americans movements, the U.S. “border” stretches out 100 miles beyond the true border. Godfather Politics added:
>
> > But wait, it gets even better! If you live anywhere in Connecticut, Delaware, Florida, Hawaii, Maine, Massachusetts, Michigan, New Hampshire, New Jersey or Rhode Island, DHS says the search zones encompass the entire state.
>
> Immigrations and Customs Enforcement (ICE) and Customs and Border Protection (CBP) have a “longstanding constitutional and statutory authority permitting suspicionless and warrantless searches of merchandise at the border and its functional equivalent.” This applies to electronic devices,

according to the recent CLCR "Border Searches of Electronic Devices" executive summary [PDF]:

> Fourth Amendment
>
> The overall authority to conduct border searches without suspicion or warrant is clear and longstanding, and courts have not treated searches of electronic devices any differently than searches of other objects. We conclude that CBP's and ICE's current border search policies comply with the Fourth Amendment. We also conclude that imposing a requirement that officers have reasonable suspicion in order to conduct a border search of an electronic device would be operationally harmful without concomitant civil rights/civil liberties benefits. However, we do think that recording more information about why searches are performed would help managers and leadership supervise the use of border search authority, and this is what we recommended; CBP has agreed and has implemented this change beginning in FY2012.***

The ACLU said, Wait one darn minute! Hello, what happened to the Constitution? Where is the rest of CLCR report on the "policy of combing through and sometimes confiscating travelers' laptops, cell phones, and other electronic devices—even when there is no suspicion of wrongdoing?" DHS maintains it is not violating our constitutional rights, so the ACLU said:

> If it's true that our rights are safe and that DHS is doing all the things it needs to do to safeguard them, then why won't it show us the results of its assessment? And why would it be legitimate to keep a report about the impact of a policy on the public's rights hidden from the very public being affected?

***

As Christian Post wrote, "Your constitutional rights have been repealed in ten states. No, this isn't a joke. It is not exaggeration or hyperbole. If you are in ten states in the United States, your some of your rights guaranteed by the Bill of Rights have been made null and void."

The ACLU filed a Freedom of Information Act request for the entire DHS report about suspicionless and warrantless "border" searches of electronic devices. ACLU attorney Catherine Crump said "We hope to establish that the Department of Homeland Security can't simply assert that its practices are legitimate without showing us the evidence, and to make it clear that the government's own analyses of how our fundamental rights apply to new technologies should be openly accessible to the public for review and debate."

Meanwhile, the EFF has tips to protect yourself and your devices against border searches. If you think you know all about it, then you might try testing your knowledge with a defending privacy at the U.S. border quiz.

Wired pointed out in 2008 that the courts have routinely upheld such constitution-free zones:

> Federal agents at the border do not need any reason to search through

> travelers' laptops, cell phones or digital cameras for evidence of crimes, a federal appeals court ruled Monday, extending the government's power to look through belongings like suitcases at the border to electronics.
>
> ***
>
> The 9th U.S. Circuit Court of Appeals sided with the government, finding that the so-called border exception to the Fourth Amendment's prohibition on unreasonable searches applied not just to suitcases and papers, but also to electronics.
>
> ***
>
> Travelers should be aware that anything on their mobile devices can be searched by government agents, who may also seize the devices and keep them for weeks or months. When in doubt, think about whether online storage or encryption might be tools you should use to prevent the feds from rummaging through your journal, your company's confidential business plans or naked pictures of you and your-of-age partner in adult fun.

International airports are treated as "borders", exempt for Fourth Amendment protections. As such,*145* airports should be added to the map above.

Do you still believe that the government is only spying on bad guys in "targeted" searches?

Articles by: Washington's Blog