

- [Home](#)
- [Firedoglake](#)
- [News](#)
- [TBogg](#)
- [Seminal](#)
- [ATTACKERMAN](#)
- [La Figa](#)
- [FDL Action](#)
- [Work](#)
- [Elections](#)
- [FDL TV](#)
- [Book Salon](#)

[Login Here](#)

Username: Password: Remember Me

[« Liveblogging Prop 8 Trial: Day Three, Wednesday PM Two \(Thirteen\)](#)

[Liveblogging Prop 8 Trial: Day Four, Thursday AM One \(Fourteen\) »](#)

[China Google Attack and the Terrorist Surveillance Program](#)

By: [bmaz](#) Wednesday January 13, 2010 5:42 pm

submit

[Tweet](#) 89 [Share](#) 23 [23](#)



As you may know, there was quite a lot of buzz this week about Google potentially leaving China over the hacking of Google's system. From [MSNBC/Reuters](#):

Google, the world's top search engine, said on Tuesday it might shut down its Chinese site, Google.cn, after an attack on its infrastructure it believed was primarily aimed at accessing the Google mail accounts of Chinese human rights activists.

Unlike ordinary viruses that are released into cyberspace and quickly spread from computer to computer, the type of attack launched against Google and at least 20 other companies were likely handcrafted uniquely for each targeted organization.

It appears to be a problem that is quite deep according to an in depth [article in MacWorld](#):

Google, by implying that Beijing had sponsored the attack, has placed itself in the center of an international controversy, exposing what appears to be a state-sponsored corporate espionage campaign that compromised more than 30 technology, financial and media companies, most of them global Fortune 500 enterprises.

The U.S. government is taking the attack seriously. Late Tuesday, U.S. Secretary of State Hillary Clinton released a statement asking the Chinese government to explain itself, saying that Google's allegations "raise very serious concerns and questions."

But the [Macworld article](#) goes on to explain why the United States government may be taking this *much more seriously* than they let on:

"First, this attack was not just on Google. As part of our investigation we have discovered that at least twenty other large companies from a wide range of businesses – including the Internet, finance, technology, media and chemical sectors – have been similarly targeted," wrote Google Chief Legal Officer David Drummond in a [Tuesday blog posting](#).

"Second, we have evidence to suggest that a primary goal of the attackers was accessing the Gmail accounts of Chinese human rights activists."

Drummond said that the hackers never got into Gmail accounts via the Google hack, but they did manage to get some "account information (such as the date the account was created) and subject line."

That's because they apparently were able to access a system used to help Google comply with search warrants by providing data on Google users, said a source familiar with the situation, who spoke on condition of anonymity because he was not authorized to speak with the press.

"Right before Christmas, it was, 'Holy s***, this malware is accessing the internal intercept [systems],'" he said.

Uh, "account information", "subject line", "search warrants" and "intercept systems". That ring a bell? This appears to indicate that the state-sponsored Chinese hackers have hacked into the portion of the Google

infrastructure that deals with government warrants, intercepts, national security letters and other modalities pertinent to the Terrorist Surveillance Program. That, if true, could be very problematic, one would think.

Now, this is based upon information and belief, but it is my understanding that Google doesn't store any gmail data in China, which means that this search warrant/intercept machine was located in the US, likely in Mountain View California

That is, if Google's Mountain View HQ search warrant search interface/computer was hacked, we are probably talking about the same computer used by the Google Legal Department to perform queries in response to DOJ warrants, subpoenas, national security letters, and FISA orders.

Yeah, if that is the case it could be a problem.

[104 Comments](#) [Spotlight](#)

Tags: [FISA](#), [Google](#), [Terrorist Surveillance Program](#), [China Google Attack](#), [Wiretapping](#), [national security letters](#)

Related Posts

No related posts.



104 Responses to “China Google Attack and the Terrorist Surveillance Program”

PJEvans January 13th, 2010 at 6:17 pm

[1](#)

Yeah, if that is the case it could be a problem.

Understatement of the year so far, I think.

I'd just about bet that there are a *lot* of people in the government who have worked many late nights trying to find out the extent of this.

[Reply](#)

pdaly January 13th, 2010 at 6:32 pm

[2](#)

If China published the data it stole from Google and this data demonstrated the breadth of National Security Letter collection, perhaps China could do much to prod Americans to demand their privacy back.

By stealing the data, perhaps China has slowed down the job flight from America to China, so China may have helped average Americans again.

But China probably doesn't care about the average American I assume. Perhaps China will use National Security Letter information as a bargaining chip to obtain concessions from Washington DC, or else China publishes.

Of course, merely stealing US corporate innovation, as noted in the articles, would also be a boon to China.

[Reply](#)

[MadDog](#) January 13th, 2010 at 6:36 pm

[3](#)

Shorter China: “*We love us some TSP! Share, please!*”

 [Reply](#)

[Peter](#) January 13th, 2010 at 7:29 pm

[4](#)

What's a little warrantless electronic eavesdropping among friends? All it takes is for the person at the top to scribble "national security!!!" on the dotted line, and then you can send your electron pushers to dip in to the Toobz and take what you want, right?

That's what BushCo *said* the procedure was, at any rate.

/snark

That said, PJEvans is right. In fact, I'd say that "Understatement of the year so far" is an understatement.

 [Reply](#)

[BoxTurtle](#) January 13th, 2010 at 7:44 pm

[5](#)

Well, this is interesting. Here's a new point to consider.

The Chinese hacked into the TSP subsystem, but they DIDN'T get any gmail data they really wanted. That means that while the gmail system admin was restricted to internals, the TSP system CAN be accessed from the outside. Meaning that the TSP probably has 24x7 no warrant access to everything google does. The TSP folks simply sign on. And that's the area that got hacked.

It further means that google itself knows exactly what the government is looking at, because from the above it's clearly logged well enough that they could detect the intrusion.

And it means google could provide a list of all those accounts the government has queried.

Boxturtle (Wanna bet the other hacked systems are related to the SAME TSP? Didn't think so...)

 [Reply](#)

[pdaly](#) January 13th, 2010 at 7:49 pm

[6](#)

Wonder why google is going public about the hack, but Yahoo is mum about whether it too was hacked.

 [Reply](#)

[pdaly](#) January 13th, 2010 at 7:52 pm

[7](#)

In response to [BoxTurtle @ 5](#)

And it means google could provide a list of all those accounts **the government** has queried.

I guess google could substitute the name of any country for the phrase 'the government'

 [Reply](#)

[Rayne](#) January 13th, 2010 at 7:53 pm

[8](#)

Sorry, but Google has not published the location of its data centers. As of late 2008 there were at least 15-18 known data centers, with three of them located in Asia.

And one of those three in Beijing.

There could be many smaller ones as they had worked with Sun Microsystems circa 2004-2005 to design "mobile" data centers — basically, a 40-ft. van or container stuffed to the gills with servers and network equipment which could be dropped anywhere.

The question not being asked is whether any U.S. gov't contractor working on TSP-like project might not have had a security breach, perhaps in the form of a worker who sold info about Google's systems.

Or perhaps whether Google has had foreign nationals in its employ who sold them out.

 [Reply](#)

[pdaly](#) January 13th, 2010 at 7:55 pm

[9](#)

Does anyone else get the feeling that a transoceanic cable is going to blow very soon?

 [Reply](#)

[Rayne](#) January 13th, 2010 at 7:57 pm

[10](#)

In response to [pdaly @ 6](#)

IMO, Google's acting as it is because it took careful note of the damage Yahoo's position on China cost its shareholders and ultimately its brand. I seriously doubt that Brin/Page are as worried about shareholders as they are about the brand; once a brand is substantively damaged, barriers mount to any innovation.

I note that in the last 24 hours Gmail changed its policy from https optional to https by default — which means they are ratcheting up security. Another appropriate response to protect brand.

 [Reply](#)

[Rayne](#) January 13th, 2010 at 7:59 pm
[11](#)

BTW, the threat Google made about pulling out of China was multifaceted. What do you think might be in Gmail servers in Beijing? And what happens if the server farm is yanked out?

 [Reply](#)

[pdaly](#) January 13th, 2010 at 8:01 pm
[12](#)

In response to [Rayne @ 10](#)

But I remember Google coming under fire several years ago for its search engine in China self censoring sites the Chinese politicians did not want the locals finding. Or something to that effect?

 [Reply](#)

[Peterr](#) January 13th, 2010 at 8:03 pm
[13](#)

In response to [BoxTurtle @ 5](#)

google itself knows exactly what the government is looking at, because from the above it's clearly logged well enough that they could detect the intrusion.

From a technical POV, Google *has* to know, in order to function — and the government *has* to let them know.

Apart from whatever Google does for TSP and the government, Google has to constantly defend its networks from all kinds of problems: glitches traceable back to idiot programmers, prank hacks from the “let's see if we can get into X” crowd, malicious hacks that try to shut down their system, and invasive hacks that try to steal from it. When an anomaly appears, someone at Google has to figure out what category it falls into, and then take steps to address it.

Without some kind of heads up from the government, Google would see someone dipping into the system and try to fight the intrusion. If Google succeeds and walls off the intruder, the government is out of the wiretap business. Instead, they get a note from the government telling them “these are not the droids you are looking for” and so Google pretends they never saw anything out of the ordinary.

At least they officially pretend that.

Programmers and security folks, however, might possibly have had unofficial conversations in the halls of conventions and such, trading stories about the droids they never saw.

 [Reply](#)

[Rayne](#) January 13th, 2010 at 8:21 pm
[14](#)

In response to [pdaly @ 12](#)

Yahoo caught a much larger rash of crap about that than Google, and it hurt them badly as they were on the bubble at that time, struggling with an ineffective business model.

China can censor the whole damned thing at the receiving end; it's a joke that it was ever a bone of contention here. Just kept the right-wing Christianist pinheads something to keep them busy when they weren't attacking liberals and gays, I guess.

 [Reply](#)

[bmaz](#) January 13th, 2010 at 8:34 pm
[15](#)

In response to [Rayne @ 10](#)

I am not certain where the infrastructure intrusion was personally, but the Google Chief Legal Officer pretty much explicitly stated the tell tale parameters as well as stating “search warrant” database. That is not innocuous.

 [Reply](#)

[orionATL](#) January 13th, 2010 at 8:48 pm
[16](#)

Damn, bmaz

you're putting pieces of the puzzle that weren't supposed to fit.

If the flat faces do this stuff, it is dastardly spying.

If the round faces do it, it is being done in the interest of national security.

And just think,

Those poor Chinese people don't have a constitution that
Protects their rights

Like we do.

Lucky us to have a supreme court to protect our individual citizens' rights.



[Reply](#)

[Rayne](#) January 13th, 2010 at 8:55 pm

[17](#)

In response to [bmaz @ 15](#)

They aren't going to tell us much about the intrusion. It would be grossly negligent for any provider of IT services to say much more than they already have, simply because it would be the equivalent of pointing out opportunities to other entities looking for a way in.

The damage isn't innocuous, but the "search warrant" database breach is not as big a threat to Google's operations as any breach of corporate info might be. Individuals may not have a clue that info about them has been accessed, but corporations already have an idea and they'd sue the crap out of Google if they felt that Google had not done everything possible to stop intrusions.

The other tell-tale came not from Google but from Adobe, and I think that it's been ignored and understated. [Adobe was hit as well](#), and may also have been key to the intrusion process. Again, they aren't saying much — but their newer products have potential back doors in them, and the PDF file format has become so ubiquitous in business that virtually everybody in the business world has multiple PDF files on their computers at any time.

Let's speculate and imagine for a second that the search warrant system which allows all governments to request user information requires submission of a warrant in the form of a PDF file...

IMPORTANT — for any readers here, if you have not already updated your antivirus, anti-malware and firewall software, you need to do so. And you need to run the the antivirus and the anti-malware this week. You also need to check to see if all your patches are up to date if you do not have your patches set up for automatic update (Patch Tuesday was yesterday, by the way). It's possible that a lot of patching was pushed over the last couple of months by affected companies, but this could be a rolling process.

Yes, I said months; there's been a known security issue with Adobe Reader/Acrobat since December. You may want to check [Secunia advisories](#) for urgent notices about security problems.

And don't forget to check for any firmware upgrades to your home network router as these may also include security enhancements.



[Reply](#)

[fatster](#) January 13th, 2010 at 9:10 pm

[18](#)

O/T, but related. This guy seems to have deeper weirdness than we've been led to believe.

"Cass Sunstein, a Harvard law professor, co-wrote an academic article entitled "Conspiracy Theories: Causes and Cures," in which he argued that the government should stealthily infiltrate groups that pose alternative theories on historical events via "chat rooms, online social networks, or even real-space groups and attempt to undermine" those groups."

[Link](#).



[Reply](#)

[Rayne](#) January 13th, 2010 at 9:14 pm

[19](#)

In response to [fatster @ 18](#)

Jeebus, fatster, that's a doozy. Based on that piece alone I'd say Sunstein has absolutely NO business ever working for our government. He'd better not be a short-lister for the next SCOTUS seat if he can't grok First and Fourth Amendments.



[Reply](#)

[fatster](#) January 13th, 2010 at 9:32 pm

[20](#)

In response to [Rayne @ 19](#)

Yeah, plus he's advocating creating a government-led conspiracy to undermine the other conspiracy theorists. I mean, aside from consideration of all those pesky legal, Constitutional questions and such.



[Reply](#)

[Arbusto](#) January 13th, 2010 at 10:15 pm

[21](#)

Google's attitude is su casa es mi casa regarding user privacy. I'd be pleasantly surprised if they don't happily bend over for any/all warrants, ala AT&T. OTOH, Google's Programmers are the best, so this hack is a needed wake up call for it and the USofA.



[Reply](#)

[prostratedragon](#) January 13th, 2010 at 10:27 pm

[22](#)

In response to [fatster @ 18](#)

You can download pdf of an apparent earlier version [at this page](#). Tell your friends.

 [Reply](#)

qweryous January 13th, 2010 at 10:33 pm

[23](#)

In response to [fatster @ 18](#)

Well...I'm not so sure that is such a good idea.

Can you say Cointelpro?

Mr Sunstein might need to "educate" some of us on just how this is to work, why he thinks it is legal, any sole source contracts involved in this, and so on. I'm sure more questions will be supplied by others on this "idea" of his.

OH another question already:

Who has he been getting legal advice from?

Might be good news for Dr. Gruber though..

I posted a seminal diary thanks to your suggestion (on a different topic).

 [Reply](#)

qweryous January 13th, 2010 at 10:39 pm

[24](#)

In response to [Arbusto @ 21](#)

Google's programmers may be the best, or may be the best available on the open market.

They may be the best available in the United States.

The best programmers in the world may have been the victim of something other than other better programmers.

 [Reply](#)

[Jeff Kaye](#) January 14th, 2010 at 12:15 am

[25](#)

It's clear to me the government knows what it wants to know, or can. If, in their lust to collect information on their own citizens, they opened a technical door for foreign penetration, then the joke is on them (and more infernally, on us).

I'd say we are also witnessing the spooks' version of "the Great Game," which is counterintelligence. Were they let in? Did they really not access email text? Which people were the Chinese looking at? Were they really political opponents of the Chinese regime, or sheep-dipped double agents (or triple agents)?

Larry Olivier's voice in my ear: "Is it safe?"

And as an aside, a fascinating look in at the supposed good guy corporation, and its dealings with the government.

 [Reply](#)

qweryous January 14th, 2010 at 12:23 am

[26](#)

In response to [Jeff Kaye @ 25](#)

And their slogan at some point was "Do No Evil" iirc.

"sheep-dipped double agents (or triple agents)?"

That reminds me of the rumored Jethro Bodine 'secret "double naught" agent/spy'.

 [Reply](#)

NMvoiceofreason January 14th, 2010 at 5:21 am

[27](#)

I have a client who was attacked by Chinese hackers in the past month.

Defense in depth, starting with a good firewall with an intrusion detection system, layered with e-mail protection and individual antivirus/antispayware won the day.

And look at all the help the government provides (zero, zip, nada).

Obama's cyber czar is more interested in implementing the new versions of TSP/TIA than in defending the homeland against attack.

THAT should worry you.

 [Reply](#)

klynn January 14th, 2010 at 5:40 am

[28](#)

In response to [fatster @ 18](#)

A disturbing paper from a pro AIPAC person.

A disinformation campaign on conspiracy theory websites? Hmmm...How many are there out there regarding AIPAC and Israeli Spies?

The dates on the paper submission and update are interesting (January 17, 2008 and April 3, 2008.)

Why even care about conspiracy theory websites?

Just wondering, could China get all the docs on the AIPAC spy case with this hack?

 [Reply](#)

klynn January 14th, 2010 at 5:46 am

[29](#)

Boy, this is an [interesting take](#) on the hit from the BBC just a few hours ago.

The cyber-attack that made Google consider pulling out of China was run of the mill, say security experts.

Google revealed its move following attempts to hack Gmail accounts of human rights activists.

The search giant said analysis showed that the series of attacks originated from inside China.

“This wasn’t in my opinion ground-breaking as an attack. We see this fairly regularly. said Mikko Hypponen, of security firm F-Secure.

“Most companies just never go public,” he added.

See, “you didn’t see anything.”

 [Reply](#)

[Rayne](#) January 14th, 2010 at 5:47 am

[30](#)

There are going to be a lot of people running their mouths and keyboards about this situation. They are going to go after the biggest target, because that’s the nature of the beast — there are many interests who do not want Google to do well for competitive reasons, and they will take every opportunity to trash Google, many doing so in a way that shapes an ignorant public’s opinion. I’ve been paid as a consultant to support this very purpose; I know competitors are doing it, just like you know lobbyists are actively working against health care reform.

Even this thread displays some of that FUD at work (fear, uncertainty and doubt — a well-known tactic first used as a deliberate marketing strategy by a large American software manufacturer). Even the belief that any internet service provider could operate in contravention of local or national law is stunning, but there’s a lot of FUD out there which insists that IT firms absolutely should and must operate in a manner which defies legal systems.

Google has some of the very best IT professionals working for them for several reasons. Not just compensation/benefits/working conditions draw them, but the ability to do what have been incredibly *subversive* things from the perspective of the traditional corporate IT world. 20% of an employee’s time may be spent on personal computing projects. Think about it: these people don’t have to go and grovel to venture capitalists funded by other corporations for cash, they can do the work while being paid. AND they have free resources for working on their code, like hosting. This is an organization which also “eats its own dog food” and publicly; if they fail, they do so, *plein air*, right where we can see it while it’s still in beta. Google Mail was beta for years; the new Nexus One was deployed to staff first for testing before being launched to the public. We can see this all in remarkably transparent fashion, before we have to part with a buck for any of their products.

(How many of us are using Gmail and don’t even pay a dime for it and the ever-increasing gigs of storage they offer, but whine when their product burps? Pretty unrealistic expectations we’ve acquired.)

The other critically subversive approach Google has taken is that it is an active advocate of [open source technology](#). Which means anybody with the wherewithal can see inside the products they are promoting — like the [Android](#) operating system. Google’s progenitors understand that information wants to be free including intellectual property like code (and I mean free to move, not free like beer). Hacking open source is tough because ANYBODY can see it being done; it’s not a closed black box into which people can’t see for purely proprietary reasons.

So what’s the problem here? The Average Joe without any IT background at all has no ken about these issues. Nor do they realize that THEY are part of the problem. Read more carefully the stories being published about this situation: *the exploit involved other company’s/ies’ software*.

Think about it. The Average Joe is expecting Google to police not only it’s own network, servers and mail systems, but to know every single vulnerability of other company’s/ies’ software. Oh, and to do so on a global basis.

And all the while, the Average Joe continues to email massive piles of attachments containing exploits embedded in other company’s/ies’ products to and from their Gmail accounts without a care in the world. In most cases, without regular security processes in place at their own desktop, laptop, mobile device.

But it’s all Google’s fault. Bad Google, bad.

It would be nice if the Average Joe learned enough about this situation to realize they are the biggest risk in computing because of their lack of knowledge. It'd be nice if the Average Joe decided to practice safe computing on a regular, systematic basis. Cheese-on-a-stick, it's amazing that people will put their personal information on unsecured networks and devices, but worry about shaking hands with somebody for fear of contagion.

And yes, I'm a Google shareholder, as I've disclosed before. This crap is going to cost me (actually, my kids' college fund) some value over the short term. But I'm going to continue to hold what is the biggest single source of innovation I know of in spite of this situation. (Not intended to be used as advice for investment purposes — your mileage may vary.)

 [Reply](#)

[klynn](#) January 14th, 2010 at 5:57 am

[31](#)

This was an [interesting write-up](#) from Wired.

“Over the last few months, we’ve been researching the security/latency tradeoff and decided that turning https on for everyone was the right thing to do,” Gmail Engineering Director Sam Schillace wrote in the Gmail blog.

This option often wasn't necessary when people used fixed and trusted connections, such as their home or office DSL or cable lines. But as Wi-Fi connections, especially public ones, became more popular, hackers began using simple sniffing software to snoop on people's online activities with the goal of stealing passwords.

Still, the switch doesn't encrypt e-mail — it simply encrypts the communications in transit between Google's servers and a user's computer — the same as when you use your bank's website. E-mails sent to other people are transmitted in the clear as they have always been. True encrypted e-mail can only be read by the sender and receiver, regardless of how they move across the internet.

Read More <http://www.wired.com/threatlevel/2010/01/google-turns-on-gmail-encryption-to-protect-wi-fi-users/#ixzz0cawoFT6b>

 [Reply](#)

[Rayne](#) January 14th, 2010 at 5:59 am

[32](#)

Here at [this link](#) is an article about the mega-patch Adobe just released to address known security problems.

And no mention at all about where this vulnerability might have appeared or what damage it might have done since it was first discovered. NONE.

 [Reply](#)

[klynn](#) January 14th, 2010 at 6:01 am

[33](#)

In response to [Rayne @ 32](#)

Thanks for the link.

Rayne,

Any insights about the report from Wired regarding the efforts to protect Wi-Fi connections?

 [Reply](#)

[Rayne](#) January 14th, 2010 at 6:01 am

[34](#)

In response to [klynn @ 31](#)

Yeah, see my comment at (10). I'd already turned on https.

Shouldn't some users be asking themselves if their non-Gmail provider offers https mail security?

[edit -- in response to klynn at (33) -- would be good to read Wikipedia's rather basic overview on [HTTP Secure](#) encryption and/or About.com's [explainer on HTTPS](#). It can be a little cryptic, but I think most people will get the gist of what this means.

But the problem with relying on HTTPS is that the vulnerability continues at the end-points of a transmission -- at the server if unsecured, and at the user end which is all too often unsecured.]

 [Reply](#)

[klynn](#) January 14th, 2010 at 6:06 am

[35](#)


In response to [Rayne @ 34](#)

Thanks. That makes sense.

Can you flush out the contrasts going on in reports? The “big news” versus “oh this is S.O.P. and happens all the time.” ‘

In some ways you addressed this @30. Just didn't know if you would have any other insights.

 [Reply](#)

 [bobschacht](#) January 14th, 2010 at 6:12 am

[36](#)

Those interested in Day 2 of the FCIC Financial Crisis Inquiry Commission, I'll be continuing to take notes and comments at the [Seminal Diary](#) set up yesterday. Eric Holder (AG), Sheila Bair (FDIC) are up this morning.

Bob in AZ

 [Reply](#)

klynn January 14th, 2010 at 6:16 am

[37](#)

In response to [klynn @ 35](#)

I mean, here's an [example of the contrast](#) from this AM. Totally contradicts the BBC.

 [Reply](#)

[Rayne](#) January 14th, 2010 at 6:26 am

[38](#)

In response to [klynn @ 35](#)

No additional insights, except that whatever happened was big enough to give the biggest IT company in the world heartburn and cause them to go public in a fashion which must have required communication with the Department of State. An announcement like this is tantamount to an acknowledgment of a cyber-war, not something taken lightly.

It's been SOP for years that certain countries try to breach networks and servers to obtain both national security info and proprietary info; for some countries these kinds of information are completely entwined, not separate issues. But something big must have happened over the last months — perhaps not a single event, but a series of events — for news over the last 48 hours to have boiled over with regard to China.

I suspect we are caught in a tit-for-tat which began with the order by PRC to install [monitoring/blocking software](#) as of July this last year. This ramped up hacking activity against PRC, which in turn ramped up its own activity. And now that this single attack or series of recent attacks has embroiled more than a couple dozen U.S. firms including military equipment providers...well, the Google announcement is really the smallest part of this situation.

I am far more worried about the proprietary info obtained from certain corporations than I am any exploitation of a TSP-like program.

 [Reply](#)

TarheelDem January 14th, 2010 at 6:28 am

[39](#)

It also means that the (most likely spoofed) origin addresses and destination addresses used in the communication of the messages that contained the hacking code passed through the telephone switches that NSA has a line splitter on.

As news has come out, it is not limited to Google. And it focuses on human rights activists.

What I find interesting is that the companies mentioned are likely to have as employees in the US a number of Chinese nationals, some of whom who might be seen by the Chinese government as supporters of human rights movements in China. No data, just a hunch about those on H1-B visas and others who might have gained US citizenship. And who have friends and relatives in China.

But then again, it might be one of those situations with a motive of "because we can".

 [Reply](#)

ondelette January 14th, 2010 at 6:32 am

[40](#)

In response to [Rayne @ 30](#)

Not sure where that stunning defense came from, but Google has the best working for it that it can find — under 28 years old, that is.

 [Reply](#)

klynn January 14th, 2010 at 6:38 am

[41](#)

I am far more worried about the proprietary info obtained from certain corporations than I am any exploitation of a TSP-like program.

Exactly. That has been my worry.

 [Reply](#)

klynn January 14th, 2010 at 6:43 am

[42](#)

Here's [even more](#) to add to the pot being stirred.

China this morning issued a statement saying it resolutely opposed hacking and was itself a victim of cyber attacks, in its first response to Google's hacking claims. In a statement posted on the state council information office website, cabinet spokesman Wang Chen reminded companies of their need to abide by internet controls, citing their "social responsibilities". The remarks did not mention Google directly. The source told the Guardian the company's decision was largely influenced by the experiences of Sergey Brin's Russian refugee background.

 [Reply](#)

wigwam January 14th, 2010 at 6:47 am

[43](#)

Why didn't we do a pre-emptive strike?

 [Reply](#)

klynn January 14th, 2010 at 6:51 am

[44](#)

The last quote in this [Toronto Star](#) article is interesting.

"Google's resolve to avoid complicity with such flagrant violations of freedom of expression and association deserves praise," the independent Human Rights Watch said.

"Google's response sets a great example," said Ganesan, the organization's director of its corporations and human rights program. Sharon Hom, director of the U.S.-based Human Rights in China, said the revelation of Internet hacking had a message for all companies operating or yearning to operate inside China.

"This is a wake-up call to the international community about the real risks of doing business in China," said Hom, "especially in the information-communications technology industry – an industry that is essential to the protection of freedom of expression and privacy rights."

Not everyone applauded Google's resolve to stand up to Chinese authorities.

"I don't think that a big multi-national company can really abandon the largest market with infinite growth potential," wrote Chinese blogger Jiang Baijing. "Google is not a child who can do anything that he wants. Google is not any individual's Google; Google is the capitalists' Google. Capital will do everything possible to maximize profit, even things that it does not like.

"Should they withdraw from the China market as a result?" he asked. "That would be too naive."

 [Reply](#)

milly January 14th, 2010 at 7:21 am

[45](#)

In response to [fatster @ 18](#)

And did the comments on Harvard related to Larry Summers just disappear here the other day?

I could be wrong but others noticed something strange going on. When this happens I don't always think it is the webmasters taking charge.

Since I have written quite a bit about Larry Summers and his vested interest in wind farms through D E Shaw Group and ties to Enron..have seen similiar things happen before on other sites.

Cass Sustein out of Harvard thinks 9/11 truth groups should be infiltrated coming right after the comments disappeared on Harvard's shady investments makes you go hmmm.

 [Reply](#)

milly January 14th, 2010 at 7:22 am

[46](#)

Daily Kos lurkers...flame it. We need some exposure on this.

 [Reply](#)

[Rayne](#) January 14th, 2010 at 7:22 am

[47](#)

Tarheel Dem (39) — yes, most of those companies have Chinese nationals or ex-pats on board, but they're already, um, well-tracked without this recent attack. This appears to be much more focused on acquiring info which could leapfrog development.

ondelette (40) — I can't divulge anything more about my consulting history. If you knew my background, you would understand entirely the impetus behind (30). As for the implication that age plays some role in Google's hiring: How many people you know over a certain age with the kind of work style and flexibility required to do Google-type work?

I know very few over 40 who can do it, who are not already management some place, who get the nature of open source in their bones and can work at the pace of current development. And I'm in the business, it's my field, and I'm in my late 40's. It's become a world for digital natives, and many Gen X don't fit in that world. Boomers? very rare visitors, most will never be natives.

 [Reply](#)

[twolf1](#) January 14th, 2010 at 7:23 am
[48](#)

[new post up top...](#)

 [Reply](#)

[Rayne](#) January 14th, 2010 at 7:41 am
[49](#)

In response to [klynn @ 44](#)

I would think carefully about that last comment and about the source.

As a Chinese national explained it to me in 2000 (we worked together at one of the companies targeted by this recent spate of exploits – that’s all I can say about it), people like him are sent to this country to acquire the entrepreneurial skills and knowledge that they don’t have in China. He understood that some of what they are trying to acquire is cultural and not academic in nature, although they do try to glean some of it through American business schools. That said, there is still a very big difference between Americans’ concept of business and that of the Chinese — even a decade later. A Chinese national speaking about capitalist motivations from within China does so knowing they are being monitored, and without actually experiencing capitalism as Americans know it. It’s simply loaded.

And then there’s the nature of Google itself; it is NOT a traditional capitalist corporation. Its heavy reliance on open source and free intellectual property should tell you it is not easy for Americans to pigeonhole it, let alone the Chinese.

My spouse does business in China; it has been the topic of much pillow talk that even regions of China have considerably different approaches to business. Some of this is deeply embedded in culture, going back centuries, making business with the west very challenging. At the same time there are areas of the country which are far more contemporary and do business easily with the west. What we are seeing in some ways is an internal struggle within China, which is trying to rapidly catch up and gain more control over its own destiny while juggling these dramatic differences within its own country.

Not to mention the additional challenge of being America’s biggest banker. Talk about unruly children.

 [Reply](#)

[ondelette](#) January 14th, 2010 at 7:42 am
[50](#)

In response to [Rayne @ 47](#)

Bull. Get an interview at Google and you are being interviewed for a senior position by a slate who all have less than 6 months experience and know more about campus life at CMU or Stanford than about working stunning applications. There is no barrier to Google’s workstyle or to the innovativeness needed at any such company that knocks out older workers, only prejudice and the belief that a person older than you is a threat. And if you really believe that there really is no ability in GenX or Boomer workers to do such work in such lifestyles, you are part of the problem. I’m a second generation computer person, boomer or no. I got my first computer kit in 3rd grade, and went to my first computer show in 4th grade, even if my first video game was Space War, so what?

Not that Google’s unique on that account in the valley.

And as for espionage and surveillance and protecting private information, Google also requires (in addition to an NDA and multiple disclaimers and legalese looking things), permission to run both a criminal background check and a complete and full credit check as a pre-condition for interview (as in well before any decision to hire). Must be that don’t do evil thingy.

 [Reply](#)

[klynn](#) January 14th, 2010 at 7:51 am
[51](#)

In response to [Rayne @ 30](#)

I agree with a great deal that you post in this comment, and I do not have your background.

Education would help. We are in a constant battle with our kids in educating them on safe computing practices. It is a difficult task. Schools fail to teach about security issues. Basically kids are just told, “No, don’t do that.” This kind of response usually fails to show the gravity so kids just ignore what they hear.

I’ve got pretty sensible kids who have taken a number of computer classes and security has never been a topic. We are on this issue constantly at home. Especially since we are ID theft victims.

 [Reply](#)

[ondelette](#) January 14th, 2010 at 7:59 am
[52](#)

In response to [Rayne @ 49](#)

As a Chinese national explained it to me in 2000 (we worked together at one of the companies targeted by this recent spate of exploits – that’s all I can say about it), people like him are sent to this country to acquire the entrepreneurial skills and knowledge that they don’t have in China. He understood that some of what they are trying to acquire is cultural and not academic in nature, although they do try to glean some of it through American business schools.

I may be out of date, but when I was in school, different Chinese nationals came to this country to study for different reasons. They ran the gamut. But many are quite nationalistic, and are here to benefit the home

country, as are others from other nations. Some are not here for academic purposes. I had the strange opportunity to find myself the only friend of a Chinese woman in one of my classes. She spoke almost no English and was pretty much shunned by other Chinese in the class. Eventually, I was ordered by the professor (himself a Chinese-American immigrant) not to speak Chinese with her any further. That pretty much ended her human interactions in the department. I later found out she was a spy, sent to monitor the other Chinese in the department. By contrast, we had a student in my department who was a political asylee, he was also sent to America on exactly the same terms as the above spy (China paying for his 1st year in grad school, etc.) with the expectation that he would ask for asylum, which he did.

 [Reply](#)

klynn January 14th, 2010 at 8:00 am

[53](#)

In response to [Rayne @ 49](#)

I posted it out of interest in the fact it was the first article I have read with such a quote, thus worth at least looking at the source and motives.

China is a strong business and personal interest in the klynn household. Mr. klynn has a background in graduate work in East Asian studies focused on China as well. The whole family studies Chinese language and history too. So I can confirm your observations in your last two statements.

 [Reply](#)

[Rayne](#) January 14th, 2010 at 8:01 am

[54](#)

In response to [ondelette @ 50](#)

Sorry, we'll have to agree to disagree.

As for Google's hiring process: that's standard fare at any Fortune 500 company.

Took me days to finish all the form work for a job at a Fortune 100 company, including multi-page NDA and NCA forms. Any time one works in a firm which has research content one should expect this. It'd be evil to hire people who have criminal backgrounds to work on private content which might contain materials sensitive to business and national security.

Or are companies supposed to hire just any Joe or [Sergey](#) off the street without any care for their background?

 [Reply](#)

[Rayne](#) January 14th, 2010 at 8:08 am

[55](#)

ondelette (52) — Yes, "well-tracked" as I said in (47). I've had staffers covering stories who've told me that students here have been bused to events to attend protest rallies. When asked, the students hedge, but it's clear they are expected to attend in exchange for their continued permission to be here.

klynn (53) — let me know if you can recommend a good online site for learning Mandarin. We could really use one here. Gets frustrating that my "round-eye" spouse is learning so much Mandarin that we have to catch up.

Appreciate the article you linked in part because it was from Toronto, not US; that's yet another angle to add to the mix. It's all one really big transnational puzzle.

 [Reply](#)

Mary January 14th, 2010 at 8:13 am

[56](#)

In response to [Peterr @ 13](#)

*Google *has* to know, in order to function*

And to bill.

@16 – Yeah, poor schmucks – no Constitution. Good thing they've got Google looking out for them. Until China starts paying per US scale.

@18 – that's flat out creepy. I guess if he'd been at OLC, we wouldn't have had all that "alternative" history (there are no wmds in Iraq & Iraq was not behind 9/11) out there now.

@27 -it does.

@38 "*I am far more worried about the proprietary info obtained from certain corporations than I am any exploitation of a TSP-like program*" Doesn't that presuppose that all the many people who can rummage around via the access of a TSP program are going to be innocents who would never use TSP for anything other than finding terrorists?

I'm kind of confused, doesn't the argument go something like – If you're not doing anything wrong, it shouldn't bother you to have the government (of China) pawing through it?

 [Reply](#)

fatster January 14th, 2010 at 8:18 am

[57](#)

In response to [prostratedragon @ 22](#)

Will do. Many thanks.

 [Reply](#)

fatster January 14th, 2010 at 8:19 am

[58](#)

In response to [qweryous @ 23](#)

I'll cruise right over there to read your article, soon's I get through the rest of these comments. Happy you've done that!

 [Reply](#)

ondelette January 14th, 2010 at 8:23 am

[59](#)

In response to [Rayne @ 54](#)

Criminal background checks deal with whether they are hiring criminals. Full credit checks do what? They have no grounds for a credit check as a condition for interview.

We can agree to disagree, but if the EEOC ever comes out of the severe dormancy that the Bush people put it into in their last years (3 cases in 2008, down from ~1700/yr, the usual before Bush), Google (and some others) will be facing a lot of very public complaints about hiring.

I don't know what your background is, but getting told one is too old to create, by a guy who's still just a GPA, when one is being hounded to finish up on patent applications is just too sweet. It really doesn't work that way.

 [Reply](#)

fatster January 14th, 2010 at 8:32 am

[60](#)

In response to [Rayne @ 54](#)

Sergey! I do enjoy following the exploits, which is hard to do since so little is published. Do you know if [any more has happened with Sergey](#) since last November?

 [Reply](#)

[Rayne](#) January 14th, 2010 at 8:36 am

[61](#)

Mary (56) — And any internet service provider is supposed to what, exactly, when presented with a warrant demanding info? Have you seen anything which confirms that Google has opened the door wide open to allow any governmental agency to have unfettered access to users' info in violation of Google's own privacy policy?

ondelette (59) — somebody with serious credit problems is a risk if they are in a position with access to certain kinds of proprietary, national security or financial info. I don't have a problem with credit checks; there are far more breaches of corporate security for financial reasons than most people realize.

As for who I am: I'm 49, I'm now a consultant specializing in business intelligence and my services have been used by large IT and small service businesses. I'm on the other side of the interview desk during hiring and sometimes on the other-other side when I'm trying to win a new consulting gig.

 [Reply](#)

[Nate](#) January 14th, 2010 at 8:39 am

[62](#)

Here's a fascinating addendum to this post. I found this in terms of Bing vs. Google. Looks like Microsoft instantly sold out to the Chinese government to buy better access for their search engine.

[Bing censors it's content for China](#)

Nate

 [Reply](#)

[Rayne](#) January 14th, 2010 at 8:42 am

[63](#)

In response to [fatster @ 60](#)

Haven't seen anything...it's way, way too quiet.

I've seen people defending him, but damn, if he was in the business as long as he was, why was he so stupid? why didn't he firewall/partition his personal stuff from bank stuff? he left a trail of what he was doing in his files; maybe he's explained it away for the feds, and maybe the banksters don't want everything out in public, who knows?

 [Reply](#)

pmj6 January 14th, 2010 at 8:43 am

[64](#)

If I were in the Chinese government, I might also be interested (alarmed?) by the fact that your supposedly private gmail account might be an open book to the US gov't, given the well documented explosion in the use of "national security letters". In other words, the US gov't could very well use this capability for

espionage against Chinese citizens. I can see that the Chinese gov't might be interested in learning whether in fact that was taking place.

 [Reply](#)

[Rayne](#) January 14th, 2010 at 8:45 am

[65](#)

In response to [Nate @ 62](#)

Yeah, and where's the screaming horde ranting about MSFT's sellout?

It might do well to remember that the heat on Yahoo about selling out to the Chinese came at a time when Yahoo was seriously considering mergers/acquisitions.

Ahem.

 [Reply](#)

fatster January 14th, 2010 at 8:48 am

[66](#)

In response to [Rayne @ 63](#)

Many thanks. I'll try and be on the look-out for updates on him, too.

 [Reply](#)

fatster January 14th, 2010 at 8:50 am

[67](#)

On a related note ("security" vs freedom), we have much work to do:

Poll: Most Americans would trim liberties to be safer

[Link.](#)

 [Reply](#)

ondelette January 14th, 2010 at 8:52 am

[68](#)

In response to [Rayne @ 61](#)

I'm an R&D person. mid-fifties. I produce IP. I go to interviews and get told by overpromoted 30 year olds that it will be great when people like me invent a chip that will go in somebody's brain so they will still be able to think when they turn 50 (I do cognitive stuff). I smile sweetly and thank them for the opportunity to speak to them (while inside I'm wondering if they know what a paradox that is).

Only lately I'm beginning to think all the obsequiousness preached by the H.R. and business/marketing people is exactly what's killing this country.

 [Reply](#)

klynn January 14th, 2010 at 8:55 am

[69](#)

In response to [Jeff Kaye @ 25](#)

That's an interesting perspective.

Could make for a good post.

BTW, great post yesterday.

 [Reply](#)

netmaker January 14th, 2010 at 9:01 am

[70](#)

Bmaz@0

"Internal intercept [systems]" may sound ominous but the fact that they are A) internal and B) used to support the legal department's need to be responsive is actually a good sign relative to previous discussions about the government just hoovering everything up.

Rayne@10

In comparison, Microsoft's Hotmail has https off by default even for the login credentials. Nasty.

BoxTurtle@5

There's no indication that the intercept system is routinely made available to outside parties. That the system(s) was called an "internal intercept [systems]" would be one indication that it/they are not. That the system is used by Google's legal department also suggests a likely vector of attack. A legeg employee compromises their workstation by opening a .PDF file and then their activities are keylogged which compromises the intercept system.

Arbusto@21

Google has fought the government in court over their access to an individual's information. Don't be so ready to write them off.

Rayne@30

A certain large American hardware manufacturer (IBM) was routinely using FUD marketing and sales techniques long before a certain large American software manufacturer even existed. Those techniques are

most likely far more ancient in their origin than that – lol.

Klynn@44

Google's Chinese market share is not that significant relative to Baidu and given the Chinese gov's policy of actively supporting domestic firms its marketshare is more likely to decrease than to increase.

 [Reply](#)

ondelette January 14th, 2010 at 9:05 am

[71](#)

In response to [fatster @ 67](#)

False choice. You have to be on the optimal curve in the family before choices like that are required.

 [Reply](#)

[Rayne](#) January 14th, 2010 at 9:14 am

[72](#)

In response to [ondelette @ 68](#)

So how does somebody get in the door at Google if you don't fit their youngsters' groupthink model?

Make something they want to acquire.

For somebody in cognitive products, I think the answer is related to [this concept](#), which was [recently released](#) as open source. Can you think of intersections between cognitive products and this technology? I sure can — especially when it comes to privacy.

 [Reply](#)

Linnaeus January 14th, 2010 at 9:17 am

[73](#)

In response to [ondelette @ 68](#)

Sorry to go OT, but I've been following this particular exchange, because as one in my late 30s, I'm beginning to worry about this notion that I'm getting too old to do certain jobs.

This might also be related to my training. In my field (history), you typically don't reach your "peak" (if one believes in such a thing) until you're in your 40s and it's not unusual at all for historians to remain productive until well into their 60s or even 70s.

Of course, there are many more jobs in IT-related fields than history.

 [Reply](#)

[Rayne](#) January 14th, 2010 at 9:25 am

[74](#)

In response to [netmaker @ 70](#)

IBM's FUD was bush league, standard marketing taught in business school. We're talking about a whole 'nother animal, a mutant on crack beginning with the Halloween memo

But it's also wrong to say that a particular software company had a monopoly in the FUD market — they had help from a couple other sizable firms when their interests aligned with that software company's interests.

 [Reply](#)

robspierre January 14th, 2010 at 10:37 am

[75](#)

In response to [Rayne @ 17](#)

I looked at the security alert you cite and see nothing new to be alarmed about. As far as I know, PDF files are not vulnerable as such. They are still basically text files (normalized PostScript) with embedded, non-executable graphics. The problem is with Acrobat Reader, which is vulnerable in the same way that web browsers are vulnerable and for the same reasons.

The only reason PDF files have security implications is that they can contain JavaScript that Adobe Reader can execute when you allow it to function as a Web browser. The JavaScript can carry out some limited actions on the local, client machine, none of which are very dangerous in themselves. But embedded JavaScript code can use Acrobat's web-browser functionality to access the internet and, potentially, download malicious executables that can do a lot more than the script itself.

You can block this behavior by simply disabling JavaScript in the Acrobat Reader preferences. If you are very security conscious, deny Acrobat the ability open links to the internet as well—another preference, as I recall. As more and more embedded, multimedia widgets become available (like Flash animation), you may want to disable them as well.

If Acrobat Reader cannot execute script, run embedded executables, or open web pages, it can't hurt you.

Overall, the most important things you can do for client security are:

* a fully up-to-date operating system and applications, including all of the latest security patches/service packs

* shut down any and all network services/ports that are not actually in use (see Gibson Research at [grc.com](#) for free information and some tools)

* do not browse the 'net while logged in as a privileged user (an "Administrator" on Windows, an "administrator", "admin", or "root" on the other OS)

* have a fully stealthed firewall installed on the client

* use a less-popular, less virus-prone operating system such as Mac OS X, Linux, Free BSD, or Open Solaris

* have antivirus software installed if you are on a Windows machine

* have Network Address Translation (NAT) and hardware firewalls set up on all routers between you and the internet

* use the Mozilla FireFox browser and install the NoScript add-on on (selectively controls JavaScript execution)

I'm an informed amateur—no doubt security professionals can add extra hints.

Interested people might want to look in to open-source, internet community efforts to undermine Chinese censorship attempts. These include onion-routing, encryption, and steganographic computing. I don't understand a lot of it. But it is interesting.



[Reply](#)

ondelette January 14th, 2010 at 10:44 am

[76](#)

In response to [Rayne @ 72](#)

Actually, it's a nice idea, and it will be nicer if Media Lab (a.k.a. Demo Factory) gets it further than most of their stuff. It will be even nicer if some next generation search companies can generate the necessary infrastructure to make it more than just a shopping tool. So it would be nice for Google to stop killing them, along with all the newspapers in the country, while they're working on that elderly labor problem thingy.

Linnaeus: You're in for a ride. Did you know that companies actually can fire you for your health insurance costs? You thought HIPAA protected you? Think again. If your company is self-insured, they can see all the claims. Or that they can snoop through enough of your personal records to get you committed rather than risk losing their group insurance policy for expensive claims? Seen that one happen too. A company in court seeking involuntary admission of a (by then) former employee on ground that he was delusional about stomach cancer — case declared moot after said employee died of stomach cancer. And you get to understand why people are worried about not being insured because of being denied for pre-existing conditions. Oh, you know, stuff like being 30 pounds overweight, or refusing to take statins. Or did you think pre-existing conditions were something serious?

About the only thing anyone gets out of anti-age discrimination legislation is that here in my state, after the age of 40, I get nine days to back out of a contract, on grounds that I may have been too feeble-minded and senile to understand what I was signing and might need a few days drooling in my wheelchair facing a nursing home wall to reconsider.



[Reply](#)

robspierre January 14th, 2010 at 10:46 am

[77](#)

In response to [fatster @ 20](#)

Sounds like fun to me:

1. We make up conspiracies, the loonier the better.
2. "They" infiltrate and supplement our conspiracy theories with government propaganda.
3. We respond with both new and ugmented conspiracy theories.
4. The tech sector comes bounding back after the latest huge government orders for servers, storage devices, and networking equipment.
5. Robspierre gets job security and a raise due to (3), makes tuition payments, fixes up the house, eats out more, etc.
5. Repeat (1-5) until the Security State chokes to death on its own output and the economy recovers.

Did I mention that the entity calling itself "Robspierre" is actually a invasive colony of alien life forms disguised as a human being and bent on total world domination? Be afraid.



[Reply](#)

JohnLopresti January 14th, 2010 at 10:48 am

[78](#)

A quick glimpse at DeepLinks, besides the https gmail default newly implemented, adds the suggestion in a post [yesterday](#), that goog might evaluate the possibility of encryption of searchstrings. Ostensibly the goog plea bargain several years ago was 1 MM strings but stripped of originator coords; Yah et all had supplied much more than goog was willing to do initially. The current international dispute seems to illustrate the attractiveness of trying the fidelity of the dominant portal which goog is. My take on the auto typeahead searchstring feature goog has implemented for a year already was it represented some conscious attempt on googles part to demonstrate to its visitors that individual profile algorithms refine the celerity of its noble

searchengine. Got to isolate the legal database, however from googls various sorts of *dashboards*; there could be *dashboards of interest*.

 [Reply](#)

JohnLopresti January 14th, 2010 at 11:00 am

[79](#)

re@78: More accurate [permalink](#) at eff.

 [Reply](#)

MarkH January 14th, 2010 at 11:15 am

[80](#)

In response to [Rayne @ 49](#)

My immediate impression is they are like a child who has been raised by very rigid parents who keep them in at 8pm and never let them go to the dance, but then those parents die in an accident and they go to live with very permissive step-parents (or other relatives). They only view the morality and behavior of the new parents through the lens filter of their prior experiences. Understanding another culture, and one which is evolving quickly, can be a challenge even for anyone.

A country like China is rapidly evolving and it's difficult for them. The size and diversity of the country would be challenging even if it were 300BC and nothing changed for 50 years. In today's world it must be incredibly difficult for political, commercial and other kinds of national leaders to understand where they are, much less where they're going or where they should intervene to make sure the best direction is taken.

Can you imagine the difficult there when a much smaller country like Israel is in tremendous turmoil and we all are confused by it?

This is one reason we are hesitant to propose any kind of big change for a country such as N. Korea and we are cautious with Iran and we respect and carry a very small stick with a country like China.

In general I think the direction China and Israel (as two examples) are moving is very good for their people. Some in America may be irritated the change is taking a very long time. We're so used to a fast pace of change that we have difficulty accepting other countries as they are.

But, that's part of having a smaller world where communications, commerce, politics and many other things are not just the local power boss checking in on the farmers.

 [Reply](#)

MarkH January 14th, 2010 at 11:20 am

[81](#)

In response to [Nate @ 62](#)

If there is this one cost of doing business I have to wonder if there are other 'concessions' they've made, like opening up e-mail to the Chinese.

Enquiring minds want to know.

 [Reply](#)

robspierre January 14th, 2010 at 11:30 am

[82](#)

An intrusion based on the TSP is real news—thanks for the heads up on this.

Such intrusions illustrate a larger problem with Security State thinking: the more security apparatus you have and the more centralized it is, the more potential there is for major security breaches. TSP introduces a single point of access to heterogeneous networks with heterogeneous security measures that would be tedious to crack separately. This is the intent—TSP makes it easy for the government to intrude on multiple networks in a convenient standardized way. So with TSP, the Chinese (or the Russian Mafia, Al Qaeda, the Sinaloa cartel, etc.) doesn't have to spend thousands of man hours cracking Google security, ATT security, Yahoo security, IBM security, Cisco security, etc. piecemeal. With TSP, they don't have to risk discovery every time they hack a different network. They have one-stop shopping, with all the risks and difficulties in one place.

This is a broader problem. Consider national identity cards: they make it easy for the ticket agent or immigration officer to "verify" identity. But they also simplify the problem of masquerading as someone else. At one time, for example, you verified your identity with a driver's license (that usually lacked a picture) and an additional document that usually had a picture (such as a college ID) or two additional documents that lacked pictures (credit card, utility bill, birth certificate). Security depended on cross-correlating between multiple documents from independent sources, none of which were designed for identity verification and none of which used the same format, ink, etc. To verify my undergrad college ID (which had a college-proprietary ID number NOT a Social Security number), you had to contact the Cornell registrar. To verify my driver's license, you had to contact the PA Dept. of Motor Vehicles. Forging either of these IDs was easy enough. But getting all of them forged consistently was hard—at some point, one of the calls to the university registrar, the DMV, etc. was not going to correlate with the others. Now, in our more Security-Conscious world, identify is more centralized. My photo driver's license has a fingerprint and social security number on it, both pre-verified by my current DMV with a birth certificate, passport, and credit card, etc. So no cross-correlation is necessary. Forging the driver's license is harder. But, once I pull that off, the payoff is huge: my identity goes unquestioned. This convenient, centralized, single-stop, proof-of-identity becomes a potential security hole.

Centralized credit-reporting and criminal databases suffer from the same problems.

When data was dispersed across multiple sources and protected by multiple gatekeepers, it was more, not less secure. Once data is consolidated in a centralized, infallible, secure "system", misusing it is easier and more attractive.

Judges, warrants, and probable cause are thus properly seen as security measures in themselves. Judicial due process, serving warrants, and waiting for respondents to comply may inconvenience Federal law enforcement from time to time. But they also subject potential intruders to scrutiny and gave legitimate authorities a monopoly of sorts on access to private information that they must now share with the Chinese, the Russian mob, the Sinaloa cartel, and anyone else with the time and money to crack a single security system.

 [Reply](#)

ondelette January 14th, 2010 at 11:42 am

[83](#)

In response to [MarkH @ 80](#)

China is very much a mixed bag. For instance, 889,000 female children between the ages of 0-4 went missing in Shanghai province in a ten year period in the 1980s-1990s. The government allows people talking to foreigners to lament it and say it was a bad policy, but further discussion needs to take place in careful circumstances, and no guides translate the blue signs in the villages that say "Daughters can inherit your land, too."

 [Reply](#)

fatster January 14th, 2010 at 12:08 pm

[84](#)

In response to [robspierre @ 77](#)

Oh, man, where do I sign up to become part of this great, creative enterprise you envision? Appeals to the old Yippie in me, for sure.

 [Reply](#)

bmaz January 14th, 2010 at 12:09 pm

[85](#)

In response to [netmaker @ 70](#)

May be, but Google's responsiveness to the government is not really the issue here; rather the issue is the fact that foreign state actors are apparently easily hacking into swaths of data germane to national security. Fairly ironic that the US government blithely asserts the state secrets privilege/immunity to keep harmed American citizens from discovering the details behind putatively illegal segments of the Terrorist Surveillance Program, but the Chinese had carte blanche to it.

 [Reply](#)

robspierre January 14th, 2010 at 12:30 pm

[86](#)

In response to [MarkH @ 80](#)

Use of TSP for network intrusions is major news--thanks for the heads up.

This highlights a flaw in our current Security-State thinking: while centralized information gathering and processing make surveillance more convenient, they actually undermine overall security. Without TSP, an intruder would have to expend lots of man hours penetrating multiple networks, each with its own heterogeneous security measures and network and server implementations. Multiple attempts increase the risk of detection. But with TSP, intruders have one-stop shopping. Even if the security around TSP were better than that around the target networks, cracking it would still be safer and less risky than piecemeal hacks.

This time, the attacker is the Chinese government. But it might just as easily be Al Qaeda, the Sinaloa cartel, the Russian mafia, North Korean intelligence, a renegade Ukrainian atomic arms dealer, or a gang of Chinese movie pirates.

TSP is convenient because it also bypasses legal barriers between government functionaries and information. The government does not have to go to a judge, show probable cause, specify targets, get and serve a warrant or subpoena, and wait for respondents to supply the required material. No one gets a chance to contest the government's case in court.

This convenience also comes at the cost of security. By decentralizing the process of authorizing access to information and breaking it out into multiple parts, the legal system makes it harder for illegitimate users to access information. It does so, moreover, in ways that are much harder to circumvent than anything you can do with passwords. The legal system, in effect, gives legitimate authority a monopoly over privileged access to private information. If Qwest Communications cannot let someone tap your phone without a warrant, then only the police, FBI, DEA, and similar agencies can have taps. Even a crooked cop working for a drug cartel will have problems, because he has to correlate his request with other parts of the legal system, such as his supervisor, the district attorney's office, and a judge. The Chinese government and the Sinaloa cartel are never going to get the same kind of access.

So, in summary, China's Google intrusion shows that there is no free lunch when it comes to security. Trying to increase national security by eavesdropping for possible plots the security of private communications in the US decreases security elsewhere--in this case the security of private communications in the US. And since exposing private individual and corporate communications to third parties can compromise national security in various unanticipated ways, we shouldn't be doing so informally and thoughtlessly, as we have been. We have long-established legal mechanisms for securing the country. We

should use them.

 [Reply](#)

robspierre January 14th, 2010 at 12:31 pm

[87](#)

Sorry for the double-post. I was getting a “database” error and didn’t see it posted.

 [Reply](#)

Rayne January 14th, 2010 at 12:38 pm

[88](#)

In response to [robspierre @ 75](#)

I think Adobe’s security problem has been a little more challenging than you have characterized.

It’s virtually impossible in enterprise environments to do what you’ve described and actually be secure, because Adobe products are nearly ubiquitous in the way that Microsoft’s operating system and office suite have been for the last 15 years. Until the patch came out today, no enterprise could really be secure; if it was merely a simple patch against Javascript exploits, they would have patched it last month.

But what do I know, being a consultant who does business intelligence in this area...

 [Reply](#)

netmaker January 14th, 2010 at 1:41 pm

[89](#)

Bmaz@85

Actually, Google being an intermediary between the gov’t and the data is pertinent. It suggests that the system that was accessed was not part of the TSP (at least as I understand the TSP) as the gov’t was using legal means to gain access to the data. There’s no indication that the Chinese had access to information that the gov’t has been shielding using the state secrets privilege.

That the intercept system is even being discussed in public by a Google employee is a strong indication that it is not part of the TSP or being used to illegally access information. Spooks are not in the habit of discussing classified systems with the press.

 [Reply](#)

robspierre January 14th, 2010 at 1:58 pm

[90](#)

In response to [Rayne @ 88](#)

I’m not questioning your business-intelligence expertise. I’m a technical writer and programmer myself—not a security expert. But I am reasonably experienced with PDF.

The Acrobat security issue may or may not be more complex than I suggest, depending on the nature of the plugins supported and particular programming errors in new versions of the browser (such as potential buffer overruns). I can only say that all PDF security issues that I am aware of to date involve the Acrobat Reader and its configuration. PDF files are not executable at the operating system level. To execute code inside a PDF file, you have to load the file into an Acrobat Reader so that the latter can locate and run any supported code.

Since the mid-1990s, I’ve worked intimately with PDF and, up to a point, with the security of PDF files. Early Acrobat browsers could execute operating system commands or run arbitrary executable programs based on instructions embedded in PDF files. But this “feature” did not make it our of beta testing (I and about 49000 other beta testers flagged this as a horrible bug, literally within minutes of its release). Since then, Acrobat has had mostly the same capabilities and presented pretty much the same risks as a web browser. It can only execute certain coded instructions, in certain supported languages (such as JavaScript), and under specified conditions.

This means that an evil entity like the Chinese secret police can insert some commands in JavaScript and a few other languages that will do things. Most are pretty basic, like forwarding information that you enter into the document to an undisclosed location (“Type your name here and click ENTER”). But the script might also be able to surreptitiously access a web site, download an executable program, and then trick you into executing the program by clicking on a button labeled in some innocuous, misleading way (“Click here for details”). None of this is much different from the dangers presented by current web browsers or email clients.

A security patch can fix security issues that do not involve script embedded in a file, but these have nothing to do with anything in the file itself. Since the Acrobat Reader can serve as a web browser (if you allow it to do so), its security can also be compromised by programming errors—bugs. This has nothing to do with the PDF file itself or with viruses. Instead, when Acrobat is acting as a web browser, with or without a PDF file open, it may be possible for a remote user to log on directly to your system via the Acrobat session. This shouldn’t happen normally. But a buggy release of any network software application can let a malicious user trick the software into giving the malicious user more access to the client operating system than the original programmer intended. One way it can do this is to crash the program by returning excessive or unexpected data and then hope that programming errors will let it see the operating system command line. If so, it can do most anything.

Denying Acrobat the right to access the internet (using the Trust Manager of the Acrobat preferences) greatly limits the scope of JavaScript attacks and eliminates the chances that a remote user will take over your system via Acrobat, as described in the preceding paragraph.

Enterprise security is another issue entirely. The security of the whole is ALWAYS vulnerable to individual ignorance, laxity, or malice. But securing Acrobat as I describe above can easily be done in the IT department. Your IT department can, for instance, supply Acrobat as part of a standardized, preconfigured ISO image that contains the approved software "stack" and operating system. This can be preloaded on workstations and laptops, pushed by IT over the network, downloaded by the user, or distributed on CDs. Or you can give users a thin client and install the software on a central server. In either case, you can deny users permission to install or reconfigure software.

I've encountered all of the above approaches in my career. The downside is loss of flexibility and limits on user initiative. So, on balance, most IT departments allow some degree of user customization when it comes to software. They view the risk from Acrobat, Internet browsers, and email clients as manageable—WHEN users are reasonably knowledgeable and diligent.

So the problem is not whether things can be secured. The problem is whether they ARE secured.

 [Reply](#)

robspierre January 14th, 2010 at 2:03 pm

[91](#)

In response to [fatster @ 84](#)

Google and Wikipedia are your friends. Look for "steganography", "Anonymizing proxy server", "onion routing", "Tor Project", "trusted operating systems", and "gnupg". I'd provide some starter links, but, if you are truly paranoid, you should probably do your own searches. Afterall, "Robspierre" might be an NSA front instead of or as well as an alien invader.

Remember: the fact that you are paranoid does not mean that they are not out to get you.

 [Reply](#)

fatster January 14th, 2010 at 2:41 pm

[92](#)

In response to [robspierre @ 91](#)

Didn't know I was displaying paranoia; your idea intrigued because it was so creative and playful. Thanks for the links, though.

 [Reply](#)

bmaz January 14th, 2010 at 2:54 pm

[93](#)

In response to [netmaker @ 89](#)

If we are assuming the information and extrapolation therefrom is correct, which we both seem to be for purposes of this discussion, then the hackers would have had access to the base of information pertaining to Google's participation in the TSP and participation in other analogous modalities including traditional Article III court orders and warrants, FISA orders and warrants, national security letter matters etc. And, yes, that is exactly the kind of information that the government has routinely asserted state secrets to protect (well at least as to FISA and NSLs) as used in the terrorist program. I never said they had hacked into the government servers.

 [Reply](#)

robspierre January 14th, 2010 at 4:07 pm

[94](#)

In response to [fatster @ 92](#)

My remarks about paranoia were meant playfully. Though, that also does not mean that they are not out to get both of us.

 [Reply](#)

ondelette January 14th, 2010 at 4:41 pm

[95](#)

Is Google still threatening to shut off their censoring in China?

 [Reply](#)

robspierre January 14th, 2010 at 4:54 pm

[96](#)

In response to [bmaz @ 93](#)

I am rapidly exceeding my competence on this topic, but I am always willing to speculate wildly. I suspect that the truth is somewhere between where you and netmaker are placing it.

My guess is that Google provided access to email, subscriber information, and/or the tracking data that it maintains on search-engine users. I'm guessing that it did so in either of two ways:

* It implemented a custom gateway and interfaces that manage and streamline government access to Google databases, but probably not logs or live network traffic.

* Or it implemented a standard interface devised by the government for ISP and/or telco use that would allow government servers to communicate with and query Google servers in a structured, predefined way.

Either way, barring major implementation bugs, such an interface would not give access to anything on the

government side, such as NSLs, FISA warrants, or the like. For security reasons that are established practice with banks and intelligence services, the government networks that store such things are probably not connected to the internet at all. Government operatives would just log in to the portal and run queries on the interfaces, either targeted searches or dragnet data mining. The Google interface might store such queries and could thus expose so-called “sources-and-methods” intelligence to an intruder. A hacker with control of the Google portal might also be able to install malware on the government browsers that access the portal, gaining access to things like email. But the government databases and secure networks should remain secure.

That said, giving all comers backdoor access to private US communications is not a minor security issue, in my inexpert opinion. With enough data, you might be able to deduce commercial or even military secrets from sources that are not supposed to be sensitive. In my brief stint as an opposition researcher, for instance, I was able to assemble enough information from press releases and public web pages to accurately diagnose the failure of a competitor’s upcoming offering. An enemy also might get lucky. People who do not understand email sometimes reveal information that they should never communicate over an outside channel. Remember when that Raygun-era Navy secretary was ducking out of submarine-procurement meetings to make insider stock trades via his mistress over a public pay phone? I wouldn’t be surprised to find classified subjects researched via Google searches. When you search for work as often as I do, you sometimes find surprising things by accident, like digests of internal corporate email stored on servers that are in plain view on the internet.

Compared to normal Google applications, an interface of the kind I’m suggesting would have two significant security problems: it would be secret (and thus not subject to the scrutiny of a broad community) and it would probably be insufficiently tested, since it is used by a comparatively tiny user base. In all probability, the portal would also be outside Google’s corporate firewall, in its own, less tested and less comprehensively maintained little sandbox (Google probably wouldn’t trust the Feds inside its datacenter any more than you and I would, and Google has more money on the line).

 [Reply](#)

[Rayne](#) January 14th, 2010 at 5:17 pm

[97](#)

In response to [robspierre @ 90](#)

Take very careful note of what Adobe says in its patch release. You will not find the word Javascript anywhere, only that the patch addresses certain identified vulnerabilities — doesn’t say they are/aren’t also addressing other unspecified vulnerabilities.

The persons/entities credited with finding exploits which drove the patch are thanked, but again, no mention that the exploits targeted by the patch were Javascript-based.

The ability to use plug-ins and the interactive application communications feature is as likely a problem — more so — than Javascript, even if Javascript has been indicated by non-Adobe entities as problematic. Both the plug-in feature and the IAC could have been deployed and launched a user’s browser to prompt for more information to gain access to the system and network. Neither of these are Javascript.

If it was only Javascript, Adobe could have patched that months ago. And I mean months ago because some of the earliest reports of problems were in October or earlier. If it was Javascript, MSFT might have easily offered a patch to discourage the launch of IE — the most commonly used browser on large enterprise systems. But instead, at least one official at MSFT made a rather cryptic comment within the last month about not bothering to fix another application’s security problems. (Plural.)

And if it was merely a Javascript exploit, the targeted enterprises named to date could have implemented a patch themselves on their firewall apps to ask for explicit authorization of Javascript. I’m certain that at least one of them had the security people to do so.

One of the other key features here is that the affected companies named so far are most likely to use a standardized, customized stack of commercial applications across their enterprise. That also provides a clue: it didn’t need to be a platform-agnostic app but one that would be readily used by the standardized stack. Like a Windows environment with IE and Adobe. I won’t even get into all the stupid crap that users do with USB devices and ad hoc networks to put non-standard stuff on their systems which could breach security. It’s the very uniformity of corporate enterprise systems which worked against them.

[edit: should also point out that most commercial antivirus packages couldn’t see the Javascript exploits reported. Chances are they couldn’t see any IAC or plug-in either if they looked like a part of Adobe. A typical enterprise stack might have had all the latest security bells and whistles and still not have protected against this.]

 [Reply](#)

[bmaz](#) January 14th, 2010 at 5:39 pm

[98](#)

In response to [robspierre @ 96](#)

I never said it would access the government side; however, if they are able to get at the Google legal depository then they can certainly access the pertinent documents and interactions with the government, communications that would be protected, that have occurred with respect to Google. That could be quite a lot. Were this a different entity, such as one of the telcos — say for instance AT&T — there could have been access to documents pertinent to the surveillance of al-Haramain. These are documents that the government will not let the plaintiffs see under a state secrets assertion, but if it had been Google involved, the Chinese may have had access. This is strictly a hypothetical analogy, but I have a little experience with the kinds of records that carrier legal offices keep and how they work and, trust me, there is a lot of interesting stuff there.



[Reply](#)
Rayne January 14th, 2010 at 5:42 pm
[99](#)

In response to [ondelette @ 95](#)

Yes, in fact I think they actually said they are not going to filter any longer — not a threat, a promise. China's next move might be to block Google altogether, but that's a victory for Google who says they can't work this way, takes a write-down and exits the country.



[Reply](#)
ondelette January 14th, 2010 at 7:22 pm
[100](#)

In response to [Rayne @ 99](#)

I've got two friends working for Google in China, I guess I should find out what's up.

By the way, thought everybody would like to see this one, too. India got attacked by Chinese hackers:
<http://indiatoday.intoday.in/site/Story/79215/Chinese+hackers+target+PMO+computers+.html>



[Reply](#)
robspierre January 14th, 2010 at 7:35 pm
[101](#)

In response to [Rayne @ 97](#)

This is so off topic, we probably shouldn't carry it too much farther. But I'll try to clear up what at least sounds like some misconceptions about JavaScript.

Bugs in the way Acrobat processes JavaScript are inevitable and no doubt happen regularly. Patches correct those things, as they do with any piece of software. So stay up to date on your security patches.

The fundamental JavaScript security issue can't be addressed by an Adobe patch, however, because JavaScript is a feature, not a bug. Acrobat either can or cannot run JavaScript code, depending on how you configure the Acrobat Reader. You use the functionality and accept some risk or you do not. Acrobat has no way of knowing what a given piece of JavaScript code will do. Scripts can be written to do good things or bad things. But Acrobat runs them either way.

Happily, the bad things that scripts can manage are fairly modest. JavaScript is designed to be a very limited programming language. The scripts run "sandboxed", which means that:

- * they can only run under another application and cannot execute themselves
- * they are restricted to performing specified operations that are appropriate to the web, and cannot, for instance, create files, format your hardisk, or create operating system login accounts
- * they are specific to a given URL and cannot access data such as user names or passwords that you send to a different URL or cookies that are set by another URL.

Nonetheless, once you enable JavaScript in a browser or in Acrobat, you run some risk of compromising your system each time that you download a document that contains script.

A firewall cannot help with JavaScript-related security issues, as near as I know: JavaScript executes on the client (the user computer) under the user's software applications, so it always runs inside the firewall. An authorized user on a trusted client downloads the script as part of a web page, email, or PDF file. At this point, the script is basically just text, indistinguishable from HTML markup, content text, or PostScript code. Firewalls generally work by restricting network ports. All HTTP (web) traffic (including HTML files and PDF), for instance, crosses the firewall via the same network port (port 80 by default). So you can't prevent people from downloading files that may contain JavaScript unless you block all HTTP traffic and lose web access entirely (the same is true of HTTPS, except that HTTPS uses a different port number).

You thus have to block execution of JavaScript at the application level, not at the network or operating system level. You can disable JavaScript altogether in the browser, email client, or Acrobat Reader application. Or, if the application supports a filtering plugin like NoScript, you can block JavaScript selectively, by URL or by rejecting scripts that appear to exploit known bugs (such as cross-site scripting attacks).

The bottom line is that you can protect against exploits that depend on bugs by keeping your software up-to-date with the latest patches. But patches can't protect you against scripting. You can't know what a malicious script author (a "script kiddie") will do until he does it. The danger is not great. I take the danger more seriously than some because I work in IT product development with highly proprietary information and because I have seen actual malware infections that originated in JavaScripts. If I were a Chinese dissident, I'd definitely disable it.



[Reply](#)
robspierre January 14th, 2010 at 7:42 pm
[102](#)

In response to [bmaz @ 98](#)

I am also being hypothetical, but I am suggesting that Google would be unlikely to make unfettered access to its network available to anyone, including the government. The hypothetical interface I described would host a clone of the desired data on a secure internet server that is, nonetheless, outside the Google firewall and thus off its network. Google would update the data store periodically by uploading a snapshot to the government portal. But that would be a one-way process. The government interface would provide no

methods capable of doing anything Google did not authorize.

For example, I can modify this FDL page by using the “Leave your response” interface. But I can’t surreptitiously edit your main article or the comments of other users, even though all of the text is stored in the same database.

 [Reply](#)

klynn January 15th, 2010 at 6:56 am

[103](#)

Here’s an [interesting read](#) fro down under.

ECONOMICALLY, China is the greatest beneficiary and the leading driver of globalisation. Politically, it is the chief champion of traditional nationalism.

Both are at play in the extraordinary saga – which has only just begun – of Google’s quixotic attempt to open up Beijing’s internet boundaries, to demolish the Great Firewall of China.

The company was yesterday attempting to play down what has been happening since chief legal officer David Drummond stunned the world with his announcement two days before.

He said that after a cyber attack on Google and 20 other big companies operating in the internet, finance, technology, media and chemical sectors that Google attributes to Chinese agents, “we are no longer willing to continue censoring results” on google.cn, the company’s Chinese website.

Its English site, google.com, is censored by the Chinese `net police, but not with the company’s collaboration.

The article is an interesting read.

 [Reply](#)

Rayne January 15th, 2010 at 8:08 am

[104](#)

In response to [robspierre @ 101](#).

Look, Adobe could lock down its product and prevent any insertion of Javascript. It could refuse to run anything which wasn’t proprietary code.

And when Secunia rates the Javascript problem as “extreme,” I’ll trust their judgment.

I see it’s still [just a minor Javascript error that’s all Google’s fault](#).

/snark

 [Reply](#)

Sorry but the comments are closed on this post

[« Liveblogging Prop 8 Trial: Day Three. Wednesday PM Two \(Thirteen\)](#)

[Liveblogging Prop 8 Trial: Day Four. Thursday AM One \(Fourteen\) »](#)



We're launching a campaign to raise \$150,000 to support Marcy Wheeler. All the money [donated on this page](#) will go directly to those efforts.

PROP 8 TRIAL COVERAGE



Read liveblogs and other coverage from Firedoglake's Marcy Wheeler, Bmaz and Teddy Partridge at the Prop 8 trial in California.

[» Click here to see the latest from the trial](#)

FROM THE BLOGS

FDL TV	Obama Wants Republican Victory in November. Politico Reporter Tells Hardball	FDL Movie Night: From Big Easy to Big Empty	Food for Thought: United Nations Names Official Space Alien Liaison	The Roundup	When There's Nothing Else To Mash Up	VIDEO: Obama Gives Not-So-Subtle Hint to Rahm "Thing That Wouldn't Leave" Emanuel	Prop 23: CA Voters Set to Reject Big Oil's Attempt to Suspend Climate Change Law

TOOLBOX

- [Register](#)
- [Support this site!](#)
- [Subscribe to the newsletter](#)
- [Advertise on Firedoglake](#)
- [Send us your tips](#)
- [Make us your homepage](#)
- [About Emptywheel](#)

Join the conversation

emptywheel
emptywheel

Love it. RT @owillis: what if we had a day where nobody in new york city or washington dc was allowed to write/report the news?
about 1 hour ago

So maybe it's unsurprising so few see the danger of unilateral power to kill so-called terrorists.
2 hours ago

But then, press isn't covering raids on peace activists (just days after DOJ's IG exposed stupid earlier harrassment of peace activists).
2 hours ago

On the day Obama declared the right to kill anyone Geithner says is a terrorist, the Admin accused peace activists of supporting terror.
2 hours ago

Join the conversation

Follow Emptywheel on Twitter





LATEST POSTS



[Is this How the Yemeni-American Partnership Works?](#)
[As Axe Slams Rahm from One Side, Greg Craig Slams from the Other](#)
[Obama's Panopticon](#)
[The Secrets They're ~~Keeping~~ Selectively Leaking about Anwar al-Awlaki](#)
[Sharktopus Live Extravaganza!](#)
[Obama Doesn't Know Why the Fuck He's Entitled to Kill Al-Awlaki, He Just Is, Damn it](#)
[Trash Talkin Texas Style](#)
[Witt Reinstated To The Air Force; Wittless In The White House](#)
[FBI's Lies about Anti-War Surveillance Also Protected CIFA](#)
[Ongoing Investigation of Anti-War Activists](#)

BLOG ROLL

- [Anonymous Liberal](#)
- [Balkinization](#)
- [RawStory](#)
- [Secrecy News](#)
- [Calculated Risk](#)
- [POGO](#)
- [Consumerist](#)
- [CREW](#)
- [Congress Matters](#)
- [Suburban Guerrilla](#)
- [First Draft](#)
- [The Gavel](#)
- [War and Piece](#)
- [Danger Room](#)

Timeline Collection

[Anthrax Investigation Timeline](#)

[Ghorbanifar Meetings Timeline](#)

[Exigent Letter Timeline](#)

[Iran NIE Timeline](#)

[Torture Document Dump](#)

[Torture Timeline](#)

[Warrantless Wiretap Memos Timeline](#)

[White House Emails Timeline](#)

 [RSS/XML Feed](#) | [Login](#) | [Register](#) | [Newsletter](#) | [Contact](#) | [Privacy](#)

