Spying Controversy Blowback, The Rebekah Brooks Trial and Dianne Feinstein

Sun, 27 Oct 2013 17:00:00, newstips66, [post_tag: 60-minutes, post_tag: autogreenblog-com, post_tag: barack-obama, post_tag: bob-woodward, post_tag: bribery, category: brotopia, post_tag: cbre, post_tag: cbre-obamacare, post_tag: corruption, post_tag: davis-ring, post_tag: dept-of-energy, post_tag: diane-feinstein, post_tag: dianne-feinstein, post_tag: doe-corruption, post_tag: elon-musk, post_tag: glenn-greenwald, category: google-alphabet, post_tag: google-barges, post_tag: google-cloud, post_tag: healthcare-gov, category: hired-assassins, category: idea-theft, post_tag: john-doerr, post_tag: ken-dilanian, post_tag: kleiner-perkins, post_tag: la-times, post_tag: nasdaq-tsla, post_tag: new-york-times, post_tag: randy-munsley, post_tag: rebekah-brooks, post_tag: secret-google-barges, post_tag: security, post_tag: solyndra, post_tag: solyndra-scandal, category: sony_pictures, post_tag: spying-controversy, post_tag: steve-spinner, post_tag: tesla-kleiner, post_tag: tesla-stock, post_tag: the-rebekah-brooks-trial, post_tag: throw-them-all-out, post_tag: tsla, post_tag: wall-street-journal-investigation, post_tag: washington-corruption-investigation, category: worldnews]

SHOCKER:

Guardian and Daily Mail researchers now believe that the Brooks hacking trial in England will expose that the Prime Minister's Communications Director, Coulsen was trading tabloid tips for character assassinations against the Prime Ministers opponents, at the direction of the PM, while in office, and that a duplicate program run by U.S. Communications Director's Robert Gibbs and Jay Carney exists in the USA. The USA team taught the British office how to do it. Watch the testimony in the trail unfold at:
http://www.theguardian.com/uk/rebekah-brooks-trial

Spying Controversy Blowback

Now that the entire planet knows that spy doors are embedded in every computer, mobile device, electronic system, network, credit card and you-name-it; the realization has created some additional secondary blowback for bad guys including those who ran the TARP/DOE scam.

In addition to the regular spies, journalists world-wide are reporting on black-market spies that you hire through sites like the (now closed) Silk Road and many clones and pay with cloudy transactions like Paypal, Bitcoin, Omni dollars and other fuzzy currency. There are over 150,000 of these hacker spies working out of China, Malaysia, the Ukraine and other exotic locations. They are able to get into the not-so-secret back-doors built into Cisco and other famous networking hardware, just as well as the regular spies. They steal and sell secrets.

Most spying is used to target people who are saying things unfriendly about the group in power in each country and to sabotage business interests who compete with the business interests of those in power. Only a portion of spying is used to catch actual criminals. Some spies work really hard to do the right thing and stop bad guys while other spires work really hard to do the wrong thing and make profits for their handlers.

Now, many of them are stealing secrets on other bad guys and selling them to law enforcement. The growth of the networked world is endless, bad guys are endless; thus, some of them work together.

In the course of this, great fun has been had by these hackers in uncovering huge corruption scams.

It seems that some of them had sourced up information and leaked it to various world-wide publications about exact and specific documentation regarding big car companies buying intelligence in order to damage competing interests and control the market. Here is an example of a “bad use” of spying:

Example: Big Car or Big Oil company sees that some journalist has found out that they bribed many people to hide a massive corruption effort in Mexico or Ecuador. The big company tells it’s “data development office” to “kill the journalist”. They don’t mean kill him dead, that would be gauche, they mean wipe out his credibility and resources. So the DD department calls the senior aides of the top 5 Senators that they most often bribe (err, I mean contribute to) and say: “hey, we have some information that so-and-so journalist might be a threat so we need to verify that, can you pop up a backgrounder so we can “prepare a report for your committee?” So the aide tells the Senator to make an agency request and the info comes back and gets passed to the corporation and they hit that Journalist hard with the inside info they got”

So you see how some corporations might enjoy all of the spying.

So you have good spies, bad spies and hacker spies. Which is which? Who knows.

But the who-bribed-who-and-what-did-they-get-out-of-it issue has been getting cleared up lately. Very detailed info seems to be available about how the crimes worked from start to finish.

So there might be some positive upside from all of the negative spying. These TARP and CAR money guys will soon find out that they didn't even come close to covering their tracks.

TA- LA Times (I don’t think the bosses are going to let me release this one so you guys get it)

In a world where everyone has equal access to the information, does that make it more of a fair fight or just creepier?

Danson

We are interested in having input on this and in talking to anybody who wants to discuss it from either perspective-

Davis- http://www.restorethefourth.net

The problem with the "bad spy hackers" is that they are poor. Being poor and driven makes one become crazy clever. They are often more clever than the office worker spy who is just trying to get his paycheck and not make trouble at work. There is a famous tale of an illegal online gambling group in Malta or Brazil that just went out and bought a room full of Sony Playstation game box systems and hooked them together and got as much computing power as a Cray super computer. Regular spies go home at 5PM, hacker spies stay up all night and day, they are more productive. They question of which is worse will be over ruled by the next technology revolution. Porn sites, gambling sites and all those types usually get the first, latest technology to start working functionally. If the feds really want to end all of this they just need to open the world's largest porn site! Problem Solved! Vivid Entertainment would have Obamacare's website working over-night and get 22 million subscribers in about an hour.

Tina C- DC

Tina, are you telling me that healthcare.gov is NOT a porn site? I'm shattered :-(

Dave

You can see if hackers have broken into your company network and are spying on you if you load and use, properly, these software analysis tools:

Process Explorer(tm) - This program will list all open processes and delineate between the parent processes and the processes that are spawned by the parent. This is a very useful program for seeing what programs are running on your computer and how they were launched.

Process Monitor(tm) - This program provides a real time display of all process, Windows Registry, and file activity on your computer. This is useful when you are concerned that a hacker may be currently connected to your computer and you wish to get a general idea as to what they are doing. This program can very quickly display a lot of information. Therefore, please play around with this program and setup filter to get a general feel on how it works.

Show Hidden(tm) - This is a tool written by BleepingComputer.com that will list all hidden folders, and files if you wish, on your computer. As many hackers hide their tools and files in a hidden folder, this tool will make it easier to find hidden folders that appear suspicious.

TCPView(tm) - TCPView is the real work horse for detecting if you have been hacked. This program will list all the programs on your computer that are connected to a remote computer or are waiting for a connection. The program will also list all the IP addresses that are connected and even perform reverse DNS on them so that you can get useful information on who is connected.

TreeSize Free(tm) - This program will scan your drive and easily show the folders on your hard drives that are using the most space. If you are concerned that your server was hacked to distribute copyrighted programs and videos, you can use this tool to search for large folders that you can then investigate.

Wireshark(tm) - Wireshark is a network sniffing tool that allows you to see the data that is flowing through your network. If you are concerned you are hacked, you can install and use Wireshark to look at the raw TCP/IP packets to see if any nefarious activity is taking place.

You can find them all online, with complete instructions, with a simple web search. I think they are all free. Plus, use tons of disinformation with anything you write online and you are all set. If your IT person does not already have all of these tools on hand and isn't running a daily and nightly check with each, fire them.

- A lowly Best Buy tech nerd-

I miss my old dial-up phone and notepad now. The Amish knew all this shit was coming. What does the NSA do about the Amish? They could be taking over the country as we speak and how would we know?

If the Amish secretly build electric cars in their barns they could get them out on the market before GM could find out and sabotage them... oh wait... hmmmmmm

---

So you might be reading some of the comments above and think that it is inconceivable that a sub rosa committee of corrupt individuals could conspire and operate within the White House, or the Prime Ministers's office, and coordinate a secret spy campaign and bribery of decision-making officials in order to control winners and losers in business and politics.

You might think this is just the suff of fantasy and conspiracy theory.

Really?

Almost every major and minor publication has, today, sent a journalist to the Old Bailey court in London where the trial of the century just began about how the head of the Prime Minister's press department worked with a tabloid to spy on people and to help destroy those people and control business opportunities using corporate spying. There is no doubt that it happened. People have been arrested. Every journalist and investigaror has confirmed it. Here is a little of the coverage:

http://www.theguardian.com/uk/rebekah-brooks-trial

http://www.dailymail.co.uk/debate/article-2431167/EPHRAIM-HARDCASTLE-Old-Bailey-trial-Rebekah-Charlie-Brooks-moved-month.html

http://www.policymic.com/articles/62661/rebekah-brooks-trial-9-questions-you-were-too-afraid-to-ask

So now let's say you replace the names in that article with, for example: Gibbs for the press secretary and Denton for the tabloid head. Then let's say you put all four of those names in a hat and shook it up and you found that all four of them actually had been connected, worked together and had multiple interactions and communications. Wouldn't that be, at least, a felony? Would that actually also be treason? Just curious. Is that why the Guardian newspaper was threatened? Did the Guardian out a business monopoly rigging program that had been found out?

D.- ProPublica, Researcher

UPDATE:

"Who watches the Watchmen"

First there was this:

ABC NEWS Reports: **Obama was unaware NSA was spying on allies, White House says.** President Obama did not know the NSA was eavesdropping on dozens of world leaders until the White House uncovered the operation this past summer, a new report says. Now, the disclosure of the spying operation is disrupting America's relations with some of its closest allies. CBS News White House correspondent Major Garrett reports at http://www.cbsnews.com/video/watch/?id=50158001n

YET,

my colleagues at LA Times just published:

White House OKd spying on allies, U.S. intelligence officials say
NSA and other U.S. intelligence agency staff members are said to be angry at President Obama for denying knowledge of the spying.

http://www.latimes.com/world/la-fg-spying-phones-

By Ken Dilanian and Janet Stobart

October 28, 2013, 7:25 p.m.- LA Times

WASHINGTON — The White House and State Department signed off on surveillance targeting phone conversations of friendly foreign leaders, current and former U.S. intelligence officials said Monday, pushing back against assertions that President Obama and his aides were unaware of the high-level eavesdropping.

Professional staff members at the National Security Agency and other U.S. intelligence agencies are angry, these officials say, believing the president has cast them adrift as he tries to distance himself from the disclosures by former NSA contractor Edward Snowden that have strained ties with close allies.

The resistance emerged as the White House said it would curtail foreign intelligence collection in some cases and two senior U.S. senators called for investigations of the practice.

France, Germany, Italy, Mexico and Sweden have all publicly complained about the NSA surveillance operations, which reportedly captured private cellphone conversations by German Chancellor Angela Merkel, among other foreign leaders.

On Monday, as Spain joined the protest, the fallout also spread to Capitol Hill.

Until now, members of Congress have chiefly focused their attention on Snowden's disclosures about the NSA's collection of U.S. telephone and email records under secret court orders.

"With respect to NSA collection of intelligence on leaders of U.S. allies — including France, Spain, Mexico and Germany — let me state unequivocally: I am totally opposed," said Sen. Dianne Feinstein (D-Calif.), who chairs the Senate Intelligence Committee.

"Unless the United States is engaged in hostilities against a country or there is an emergency need for this type of surveillance, I do not believe the United States should be collecting phone calls or emails of friendly presidents and prime ministers," she said in a statement.

Feinstein said the Intelligence Committee had not been told of "certain surveillance activities" for more than a decade, and she said she would initiate a major review of the NSA operation. She added that the White House had informed her that "collection on our allies will not continue," although other officials said most U.S. surveillance overseas would not be affected.

Sen. John McCain (R-Ariz.), ranking minority member of the Armed Services Committee, said Congress should consider creating a special select committee to examine U.S. eavesdropping on foreign leaders.

"Obviously, we're going to want to know exactly what the president knew and when he knew it," McCain told reporters in Chicago. "We have always eavesdropped on people around the world. But the advance of technology has given us enormous capabilities, and I think you might make an argument that some of this capability has been very offensive both to us and to our allies."

In Madrid, Spanish Foreign Ministry officials summoned the U.S. ambassador to object to the alleged NSA communications net in Spain. Citing documents leaked by Snowden, El Mundo, a major Spanish daily, said the U.S. spy agency had collected data on more than 60 million phone calls made in just 30 days, from early December 2012 to early January 2013.

Precisely how the surveillance is conducted is unclear. But if a foreign leader is targeted for eavesdropping, the relevant U.S. ambassador and the National Security Council staffer at the White House who deals with the country are given regular reports, said two former senior intelligence officials, who spoke on condition of anonymity in discussing classified information.

Obama may not have been specifically briefed on NSA operations targeting a foreign leader's cellphone or email communications, one of the officials said. "But certainly the National Security Council and senior people across the intelligence community knew exactly what was going on, and to suggest otherwise is ridiculous."

If U.S. spying on key foreign leaders was news to the White House, current and former officials said, then White House officials have not been reading their briefing books.

Some U.S. intelligence officials said they were being blamed by the White House for conducting surveillance that was authorized under the law and utilized at the White House.

"People are furious," said a senior intelligence official who would not be identified discussing classified information. "This is officially the White House cutting off the intelligence community."

Any decision to spy on friendly foreign leaders is made with input from the State Department, which considers the political risk, the official said. Any useful intelligence is then given to the president's counter-terrorism advisor, Lisa Monaco, among other White House officials.

Jay Carney, the White House press secretary, said Monday that Obama had ordered a review of surveillance capabilities, including those affecting America's closest foreign partners and allies.

"Our review is looking across the board at our intelligence gathering to ensure that as we gather intelligence, we are properly accounting for both the security of our citizens and our allies and the privacy concerns shared by Americans and citizens around the world," Carney said.

Caitlin Hayden, spokeswoman for the National Security Council, said the review would examine "whether we have the appropriate posture when it comes to heads of state, how we coordinate with our closest allies and partners, and what further guiding principles or constraints might be appropriate for our efforts."

She said the review should be completed this year.

Citing documents from Snowden, the German news magazine Der Spiegel reported last week that the NSA's Special Collection Service had monitored Merkel's cellphone since 2002. Obama subsequently called Merkel and told her he was not aware her phone had been hacked, U.S. officials said.

Intelligence officials also disputed a Wall Street Journal article Monday that said the White House had learned only this summer — during a review of surveillance operations that might be exposed by Snowden — about an NSA program to monitor communications of 35 world leaders. Since then, officials said, several of the eavesdropping operations have been stopped because of political sensitivities.

ken.dilanian@latimes.com

Stobart is a news assistant in The Times' London bureau. Chicago Tribune writer Rick Pearson contributed to this report.

It seems NSA has an equal mix of Democrats AND Republicans working there.
TA- LA Times

Who is **Dianne Feinstein**?

If you were in the Senate and you had been involved in **corruption** things, you would want to try to get yourself on the Senate Intelligence Committee so you could use, and monitor, agency information and resources to make sure nobody found out about the corruption things you and your husband were doing. Let's take **Dianne Feinstein** and her husband **Richard Blum** and his **CBRE** and vast other stealth companies and funds.

When she was mayor of San Francisco, the San Francisco newspapers were rife with charges of corruption and cronyism about her. Her associate, **Roger Boas**, went to federal prison for corruption in City Hall AND for **child prostitutes**. Police reports show that he used child prostitutes plus sent prositutes out to buy favors for City Hall corrupt winner/loser rigged selections.

She personally interceded in getting **Solyndra** funded from taxpayer dollars and getting them to build the Solyndra buildings where it benefited her husbands business connections. Her Family made profits off of Solyndra getting picked as a DOE funding "winner".

She personally interceded in getting **Tesla** funded from taxpayer dollars, and getting them to acquire buildings (physically next to Solyndra in the boondocks of Fremont, California) and equipment where it benefited her husbands business connections. Her Family made profits off of Tesla getting picked as a DOE funding "winner".

Guardian staff report that her husband has made multiple trips to Mongolia transporting cash for deals and now holds business interests there on mining companies that make materials for electric car batteries and other interests that she fought for bill or budget passage on. They have airport records, travel expense reports and photographs of him in Mongolia meeting with sketchy Chinese and Asian Business men. They state that he took suitcases full of cash to Mongolia. Why did Feinstein not properly document this in her disclosures? What intelligence did Blum get near, or to, China?

Richard Blum got a group of Silicon Valley VC's to buy votes, get out the vote for her and push votes to get her on Committee when she was hanging by a thread from previous near-catches of their misdeeds according to a former reporter from ValleyWag.

Feinstein wrote laws regarding the Regents of California which benefited her husband.

If you web search their names and "Corruption" or "Crony" you will find a vast number of stories about all kinds of kickbacks that the Feinstein/Blums have been charged with.

And a person like this has acess to all the secret files?

When you chart out all of the front companies, fake family trusts under other trusts, Blum offshore accounts in Belize, The Caymans and other interesting places, companies behind other companies between her and Mr. Blum, you have a facade of misdirection and phoney business names that would make any spy envious. Feinstein's bills and budgets tie back to more false front organizations that benefit her family interests than almost any other person in the Senate per the latest research from The Guardian.

If you were someone like that you would certainly try to get yourself on the intelligence committee so you could have the first clue when you were about to get caught and to steer investigations away from your crony deals. You would certainly support domestic phone-tapping because you would order such taps on your public-interest agency enemies like the ACLU and BigGovernment.com and The Schweizer team in order to keep an eye on them. Of course she is fighting ***on behalf*** of ongoing domestic spying. It is how she covers her ass.

UPDATE:

Here is a teeny, tiny selection of the many corruption charges against Feinstein:

https://www.sodahead.com/united-states/dianne-feinstein-the-most-corrupt-person-in-congress-routes-even-more-money-to-husbands-firm/question-3651127/

http://capoliticalnews.com/2013/06/03/more-dianne-feinstein-corruption-husband-given-exclusive-to-sell-56-post-offices-6-commission/

http://www.blacklistednews.com/Senator_Feinstein%E2%80%99s_Husband_Stands_to_Make_Millions_from_USPS_Contract/26454/0/38/38/Y/M.html

https://vidrebel.wordpress.com/2013/01/06/dianne-feinstein-thy-name-is-corruption/

http://www.salon.com/2012/07/24/dianne_feinsteins_espionage/

http://www.activistpost.com/2013/06/keeping-it-in-family-senator-feinsteins.html

http://www.libertynewsonline.com/article_301_33364.php

http://newsbusters.org/node/12481

http://foundsf.org/index.php?title=Richard_C._Blum_and_Dianne_Feinstein:_The_Power_Couple_of_California

http://www.truth-out.org/opinion/item/19023-sen-feinstein-wants-to-strip-independent-journalists-rights

http://www.thenewamerican.com/usnews/crime/item/15579-snopes-misses-larger-story-on-sales-of-post-offices-by-california-sen-feinstein-s-husband-s-company

http://ridgecrest.blogspot.de/2007/04/feinstein-corruption-scandal.html

http://littlecountrylost.blogspot.de/2007/12/diane-feinstein-corrupt-war-profiteer.html

https://spotlightoncorruption.wordpress.com/tag/dianne-feinstein/

http://www.conservapedia.com/Dianne_Feinstein

http://dcclothesline.com/2013/01/25/why-america-can-not-trust-the-motives-of-dianne-feinstein/

and thousands more...

How is it even remotely possible that this person is in a public office?

D. - Portland Obs.

Who do we trust anymore? Didn't we hire these people to go Washington to serve each individual living in America? Am I confused on the concept? I thought getting elected was like winning the best student award so you could go impress us with great deeds as opposed to winning American Idol where you can go impress us with great greed!

Debbie K.

"A Massive Surveillance State": **Glenn Greenwald** Exposes ...
GLENN GREENWALD: I think **Dianne Feinstein** may be the most Orwellian political official in Washington. It is hard to imagine having a government more secretive than the United States. Virtually everything that government does, ...

democracynow.org/2013/6/7/a_massive_surveillance_state_g...

Glenn Greenwald

Now Feinstein is trying to cover her tracks and act like she thinks spying on American's who were trying to end cronyism was "unacceptable". Don't buy her sudden change of tone. It is all a cover, just like all of her husbands vast network of cover organizations and secret VC kickback networks. If you want to do really big crimes in Washington, you get Feinstein to watch the databases to make sure nobody gets wind of it. **It is like the one bank robber that sits in the car to listen to the police scanner during the bank robbery.**

GG

If Feinstein's husband turns out to be a spy for China, wouldn't that just suck the big one? How can she have so many nasty news articles about her online in very detailed stories by very famous journalists and Washington has never held an investigation on her?

Julie Lentin

Husband's Business Ties to China Dog Feinstein - Los Angeles ...
For years, international financier **Richard** C. **Blum's** vast business portfolio has persisted as a nettlesome issue for his wife, Sen. Dianne Feinstein (D-Calif.), a vocal proponent of increased **China** trade. Three years ago, he vowed to turn over any profits from his **China** investments to ...

articles.latimes.com/2000/oct/20/news/mn-39450

http://articles.latimes.com/2000/oct/20/news/mn-39450

Ok, Here is the most extreme theory ever, but it is amusing:

"Google, Twitter and Facebook are actually spy agency sting operations and were originally created as such. They conduited the money through Kleiner Perkins offices to launder it. They paid Kleiner's people off by giving them monopolies on the electric car and battery industries and associated mining interests."

I saw that on a blog and just had to repost it.
How about them Apples? One of the original founders of Twitter is running around saying it wasn't what he had in mind. Even though they are supposed to be competitors you usually see their "join" or "login as" buttons clumped together on other sites and they sell ads for each other secretly. Those "Google Barges" could just be international waters scrutiny evasion systems. While it sounds crazy, with all the related news coming out this week, it could almost be true. ;-)

H.T.

See more Feinstein updates HERE

This will be a very sad Christmas for the auto and consumer electronics industry. Nobody wants to buy a new cell phone, tablet or other electronics for Christmas because they fear the backdoors and spy chips in them. Nobody wants one of the new networked or wired cars because they could be just a giant bugging device. Apple's product line has crashed from demand drop. Consumer electronics groups are having emergency meetings. Huwaei cell phones are being un-ordered in droves. Overseas companies are cancelling Cisco orders. One of the biggest blowbacks of the spying controversy will be economic and it will cost many jobs and much industry revenue. **Losses will be in the billions.**GH- LAT

Ha! They are going to have Google fix the healthcare system. There certainly won't be any privacy issues with that!

GH- NY

Aside from the NSA and FBI having all of the communications from the scandal, there's also the hackers....

Can You Hack It?

Everything electronic you own—iPhone to subway card to power strip—can be hacked. So how to defend yourself?

By Amy Webb For Slate.com

Wherever you're sitting right now, take a moment to note the connected devices around you. In your pocket or handbag, you probably have an electronic key fob and perhaps a rechargeable subway card embedded with RFID. You likely have a smartphone, which is connected to a Wi-Fi network and also has voice-mail service. You might be wearing a Nike FuelBand, or a Fitbit, or possibly even a new pair of Google Glass. Maybe you can spot a traffic light or an orange highway sign out of your window. A power strip is likely not too far away.

All of these devices share one thing in common: They can be hacked.

As we herald the coming Internet of Things, it's easy to forget that our ever expanding tech playground is mostly unsupervised. There is no playground teacher to blow a whistle when another kid takes control of your Bluetooth headset. There is no Norton antivirus software for your garage door opener. If you can plug it in or connect it to a network, your device—no matter what it is—can be harnessed by someone else. And that someone doesn't have to be a Chinese superhacker to do some serious damage with it, either on purpose or by accident. It can be your Uncle Roger, who doesn't have his new iPhone figured out and is cluelessly turning your lights on and off via your Belkin WeMo.I'm a hobbyist. Because I study emerging technlogy and the future of media, I'm often tinkering, breaking things, and putting them back together. Once, I wanted to see if I could break into the protected Wi-Fi network we set up for my daughter at home. Less than an hour later, I'd failed to penetrate her network but managed to shut down the main network for our house. Which I knew, because of my husband's sudden yelling upstairs: "Why is the IRS website redirecting to Sesame Street?!"Part of what makes new technology so exciting is that, unlike the old days, it works right out of the box. You no longer need to know how to build a computer, connect a modem, run a terminal emulator, and install bulletin board stystem, or BBS, software in order to send a racy message to a co-worker. Now any tech idiot can download Snapchat and accidentally send a racy photo to his sister-in-law. The tech playground is more accessible and, as a result, increasingly problematic.Just after the annual Black Hat Internet security convention a few months ago in Las Vegas, I asked a group of my friends—a Navy engineer, a professional hacker, and a hobbyist—to help me come up with a quick list of devices that will be vulnerable during the next few years as the Internet of Things becomes widespread.

Here's our **(incomplete)** list. (Entries with a * are those we've tried hacking at home, for fun.):

Obvious
smartwatches*
smartphones*
computers*
tablets and phablets*
home computer locks*
the cloud (services, storage, software)
ATMs at banks
printers
GPS devices*
Wi-Fi routers*
webcams*
thumb and portable USB drives
hotel and gym safes (they tend to use a single default passcode)
cable box or DVR
voice mail (especially those with a global call-in number that doesn't lock out

after successive failed attempts—we saw this with the News of the World scandal)

Less Obvious
power strips (can be infected with malware)
power cords for your devices (code can be implanted)
luggage trackers (such as the Trakdot)
connected glasses (Google Glass, Oculus Rift. As of now, Google's QR barcodes for Wi-Fi store the full access point name and password as plain text)
gaming consoles: PS3, Kinect, Nintendo*
refrigerators (such as Samsung)
cars with computer operating systems
smart pens (like the Livescribe)
gesture control devices (such as the Leap)*
SD cards
cameras
smart alarm clocks*
coffee makers
key fobs
light switches*

moisture sensors*
kitchen and pantry trackers (such as Egg Minder)
insurance driving monitors, such as Progressive's Snapshot device
traffic lights (MIRT transmitters can change lights to green in two to three seconds)
highway signs that spell out text

...And we didn't even get into medical devices, which are frighteningly exposed to mischief.The proliferation of all this technology creates a constant need to keep devices updated and secure. Perhaps the most vulnerable object in any American house is the cable box, because it is so rarely updated.

If what I'm saying makes you uneasy, you're not alone. There are plenty of new products exploiting the fears of techno-theft, promising to keep you locked down and safe, such as this neck security wallet from REI, which says it'll block criminals from scanning the RFID chip in your passport. I travel to a lot of different countries every year for work. I've had zero attacks on my passport. On the other hand, I've had two laptops and an iPhone compromised.So how should we think about our constant vulnerability? I make a daily assumption that everything I do is hackable, but almost nothing I do is worth hacking. I have an awareness of potential vulnerabilities, and I'm trying to develop an evolving set of street smarts. You should, too.For example, since I do a lot of work on the road while I travel, I now carry my own Wi-Fi hotspot. I can use a secure virtual private network to send and receive email and to access content that I have stored in the cloud. (To be sure, that network can be hacked, too, but at least I can watch the logs of what's coming and going and attempt to fight off intruders.)I also keep this network cloaked, meaning that I haven't named it "Amy Webb's Hotspot." I routinely look at networks, just for fun, and I'm astonished at how many people use their own names or the names of their companies. Instead, I've changed the names of all of my devices to my mobile phone number. That way, if my laptop is lost or stolen, someone will see a phone number rather than my name, which I hope means there will be less of an incentive to poke around my machine to see what's there.My passwords are easy to remember but difficult to crack. According to my hacker friend, you're best off with a long phrase that also includes numbers and at least one capital letter. Something like "Iwant99pizzasand12beersfordinnertonight" is actually more secure than "Gx1U2y," because the algorithms that are used to crack passwords have to process many more computations the longer a password is, and as of now they're mostly not using natural language processing. Speaking of passwords, I change them weekly. It should go without saying that each one of your networks and devices should have a different password. When was the last time you changed yours? Because I know you're wondering: There is no workaround for this and no way to game the management of your own passwords.Another good rule is to turn off your peripherals when they're not in use. Don't leave your nanny cam on all day long. Same goes for non essentials on your network, such as additional computers, game consoles, and the like. The more things you have plugged in, the more opportunities there are for penetration. Be cognizant of who's plugging what into your network and connected devices. An innocent-looking thumb drive can destroy your computer within seconds. I'm not preaching abstinence here, but I am saying that computer viruses can be as menacing as sexually transmitted diseases: invisible to the naked eye, but most of the time totally preventable with the right precautions taken in advance.More importantly, I'd argue that all this hacking isn't necessarily a bad thing. A lack of rules is actually helpful for our burgeoning Internet of Things. I'd much rather that we all come to a good understanding of how our machines work than to start imposing regulations and restricting access. Sometimes, a collaborative hacking effort yields beneficial results for all. For example, the city of Philadelphia launched a contest and invited hackers to create apps and widgets to help citizens receive updates on emergencies and city news and to contact city administration. During Superstorm Sandy, Philly311 was the 33rd most-downloaded app in the country. The city since partnered with Random Hacks of Kindness and Code for America to bring local hackers together with residents, share knowledge, and build more resources.The tech playground is open to all, offering a fantastic opportunity to teach kids how to use and control the many devices that are inextricably tied to their futures. The more they break, the more they'll learn how to collaborate, fix, and innovate. Organizations like SparkFun Electronics are using next-generation open-source code to show everyone how to build and hack our Internet of Things.
Open networks are vital to innovation, even if they aren't totally secure.
Personally, I'm looking forward to 50 years from now when I think the wrong sequence while looking at the light fixture in my grandchild's house and accidentally cause a blackout.

China will offer to sell any journalist a whole set of transcripts from this, and other scandals.
