MONDAY: GOTTA' CATCH 'EM ALL

[*NB: Embedded video contains adult language NSFW*]

I had a very disturbing conversation with some 18-to-20-somethings this weekend about privacy and networked communications. I can't decide if I'm pissed off or terrified that these particular youngsters believed:

- Most young people their age don't care if their privacy has been compromised;
- If they care at all, they believe it's not a big deal, there's little danger because they can just shut off the GPS/location and voice features on their phones;
- This is the way it is with technology and there's no way to change the status quo.

I know for certain not all youngsters in this age group feel this way, but what set this particular group apart is their privilege. They are going to school in business and education at some of the best schools in the country. Their educations are paid for in full and they know they have jobs waiting for them. Their political heritage is conservative – anti-tax, pro-business, with a Christian fundamentalist spin. They are the next generation of elected officials because they can afford to run for office.

They are what a well-to-do public school district created, and what will come out of a top ten business school: people who don't give a

shit about anybody else's needs for privacy, because they simply don't see any risks to their way of life.

The entire conversation began because they were questioning my opsec habit of covering my cellphone camera lenses. When I pushed back about their habit of waving their phones around without any respect for others' privacy, the topic rapidly went south. It didn't matter, nobody was following them, they didn't need to worry; whoever wanted to track them already had all their information anyhow. And still not a lick of concern about anybody else's privacy, safety and security, free speech, freedom from unwarranted seizure…

And now comes Pokémon Go, the augmented reality mobile device game which this particular cohort had yet to play with on their cellphones. I'm sure they've since loaded on their phones without a second thought about the gross failure of Pokémon Go's privacy policy let alone its ridiculously broad request for device permissions.

Stay away from me, kids. Far, far away. Go ahead and give me a hard time again about protecting privacy rights. Treat me like an old lady yelling at you to stay off my lawn, and I'll find somebody to tell your super-conservative mother what kind of porn you've surfed while you claim you're at the library studying on her dime. I'm sure I can get somebody to do it for the price of a Pokéstop lure and a Clefairy water Pokémon.

Meanwhile, protesters documenting civil rights abuses by hyper-militarized police have risked their freedom and lives doing so. Like the protesters and reporters seen in the short video taken of Baton Rouge Police arresting protesters gathered peacefully on private property yesterday, forcing their way into a private home and pushing around its residents. Or Ramsey Orta, who videoed the chokehold death of Eric Garner, harassed repeatedly by NYPD since then and jailed, or Chris LeDay's suspicious arrest

after he posted video of Alton Sterling's murder by Baton Rouge police. These citizens and the journalists who covered them are surely concerned about their privacy and the chilling effect on their free speech a lack of privacy protections will cause for them as individuals and as activist groups and news outlets.

And it's these people those privileged 18-to-20-somethings I spoke with will never consider as they navigate their way through the rest of college and into the business world. It's no wonder they believe there's no way to change the status quo; they aren't taught to think outside the tight confines of their safe little world nor do they face any threats inside their narrow groove.

I grieve for the future.

FIVE DAYS

That's all that's left for in-session days on the U.S. House calendar for July. I see nothing in the remaining schedule directly related to the Flint Water Crisis. Only California's ongoing water shortage will have a hearing. While the House fiddles, Flint area nonprofits continue to raise money to buy bottled water for city residents. The city water system is allegedly safe, but we all know the entire city is riddled with damaged pipe causing one Boil Water Notice so far this summer. Lead pipes continue to service homes. The roughly 8000 children poisoned so far don't need even a smidgen more lead from those water lines. But All Lives Matter, right?

I hope every journalist covering an incumbent's House or Senate campaign will ask what the candidate has done while in office to address both Flint's ~~GOP-inflicted~~ man-made catastrophe and future crises of a similar nature given underfunded EPA mandates for clean drinking water and equally underfunded infrastructure replacement.

Don't even get me started on Congress' weak gestures on Zika, especially after the first

Zika-related death in the U.S. this past week and ~1133 patients who've tested positive for Zika, including ~320 pregnant women. Zero effort to encourage birth control among at-risk population, let alone adequate warning to the public that unprotected sex as well as mosquitoes spread the disease.

Po po no no

- Suspect fires on Houston police during 7-hour showdown; SWAT team subdues him using gas (KTRK) – Look, ma, no deadly force! Gee, I wonder what the suspect's race/ethnicity is?
- Tiny study without peer review based on unreliable data claims whites shot as often as blacks by police (NYT) – Harvard researcher looked at 1,332 shootings by 10 police departments in Florida, Texas, and California across fifteen years to come up with this swagged conclusion. There was so much wrong with this I don't even know where to begin. Even the lead researcher's personal experience suggests there's a problem with the data. The New York Times simply regurgitates this without any push back. After all the video evidence we've seen since Ferguson, should we

really believe police-supplied data from such a small sample of nearly 18,000 police departments? We really need a mandatory collection of data from all police departments based on standardized methods combined with an audit. There's more accountability in banking than there is in police use of force – and we all know how that turned out after 2008's crash.

- Dallas shooter was 'changed' by military service (The Blaze) – Once interested in becoming a police officer, formerly happy extrovert Micah Johnson became withdrawn, disappointed during his military service. Wonder if he suffered from untreated PTSD and depression after leaving the military? Wonder how many law enforcement officers likewise were former military who sublimated their post-service frustrations? Are we doing enough to help former service persons ease back into civilian life?

Enough. I'm already wishing for Tuesday.

FRIDAY (SOMEWHERE): WHY

More stuff broken and worse than I expected.

Rather an understatement, that. This week has been a massive case of broken.

Other broken things

- Polarized Congress damaging oversight? (CSMonitor) – Hyper-partisanship at fault? Perhaps. But it's awfully weird when the current FBI Director, who served under a Republican president as Deputy Attorney General, doesn't give a GOP-dominated House what it wants. Maybe something else is broken, too?
- Android's user credentials and crypto keys storage system is broken (Threatpost) – Researchers say KeyStore's encryption is exploitable; hackers could store forged keys. Yikes.
- White male celebrity's sentence too light – in South Africa (Herald Sun) – U.S. is not the only place where sentencing is broken, as the case of Oscar Pistorius shows. Six years

is utterly ridiculous.

- Train derailment exposes critical flaw in inspection methodology (Oregon Local) – Because inspectors drive the tracks rather than walk them, broken bolts were missed. Federal Railroad Administration said Union Pacific is at fault for the derailment and explosion of a 94-car train carrying oil, caused by the broken bolts. And yet the FRA doesn't require walking track as part of mandatory inspection processes, nor does the FRA inspect track that rigorously. More than bolts were broken here.
- FOX's Roger Ailes wants Gretchen Carlson's sexual harassment suit to go to arbitration (LA Times) – Ailes claims Carlson's contract specifies arbitration. Hell, no. This isn't a contract dispute, bonehead. It's a violation of her civil rights under Title VII of the Civil Rights Act of 1964 and that's not subject to arbitration. I'd like to break my foot off on this one.

Wishing us all a better weekend. Be kind to each other and fix something broken.

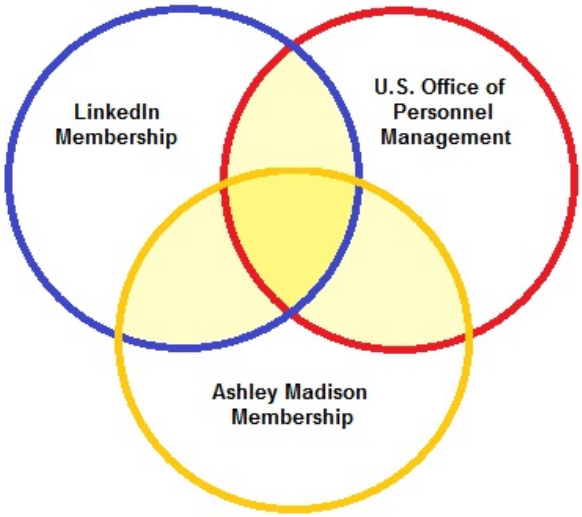
WEDNESDAY: MEND

Repair Day here, can't spend much time reading or writing as I'll be tied up mending things. Enjoy a little mellow Foo Fighters' tune – can't handle metal rock today or I'll end up HULK SMASHing things I'm supposed to fix.

Here's a range of topics which deserve more attention:

• UK's Chilcot report released today (Guardian-UK) – [*Insert lengthy string of epithets here, circa 2003*] I'm sure one of the other team members here at emptywheel will elaborate more effectively on the ugliness in the report and on former Prime Minister Tony Blair's continued ~~lies~~ rationalizations for military intervention in Iraq over alleged 9/11 terrorists and non-existent nuclear weapons. His self-flagellation and tepid mea culpa are pathetic, like watching a wee gnat flailing on an elephant's ass. Thirteen years later, Iraq has become a training ground for terrorists. Self-fulfilling prophecy, much?

The full Chilcot report can be found here. The Guardian is working on a collaborative evaluation of the same.



• Hookup site Ashley Madison under investigation by FTC (Reuters) – Not clear exactly what FTC's focus is, whether they are looking primarily at the data breach or if they are looking into the misleading use of "fembot" AI to chat up potential customers. Though the article's characterization of the business as a "discreet dating site" cracks me up, I'm still concerned about the potential risks involved with a breach, especially since other breached data make Ashley Madison's data more valuable. Like in this Venn diagram; if you were a foreign agent, which breached data would you mine most carefully?

• French Parliament released its inquiry into November terrorist attacks (20 Minutes) – Six months after the attack at the Bataclan and in the streets of Paris, representatives of the Parliamentary inquiry spoke yesterday about the inquiry's findings:

- Poor cooperation between intelligence functions – In spite of consolidation of General Intelligence and Directorate of Territorial Surveillance under the Central Directorate of Internal Intelligence in 2008 and then the Directorate General of

Internal Security (ISB) in 2014, there were gaps in hand-offs between functions.

- Ineffective collection and sharing of prison intelligence – The ISB did not have information from Justice (the prison service) about the relationships between incarcerated radical Islamists nor information about targets' release from custody.
- Poor cooperation between EU members and EU system gaps – Fake Syrian passports should have been caught by the EU's Frontex at external borders to EU, and Frontex has no access to data collected by police and intelligence services internal to the EU.
- Gaps in jurisdiction – Not all law enforcement was engaged as they should have been during the November attack, and when engaged, not where they should have been.
- Victims and families treated inadequately – Some families were told they were "ineligible" to be notified of their relatives' deaths. Forensic Institute was swamped by the volume of work. At least one victim

> tried to call the police; they hung up on the victim because she whispered on the phone.

It’s not clear what steps the French will take next to fix these problems identified after looking at 2015’s January and November terrorist attacks, though it is reassuring to see a relatively detailed evaluation. Some of the suspects involved in both the November attacks in Paris and in Brussels are still being rounded up and bound over for prosecution; two were handed over by Belgium to France just this week. The full Parliamentary inquiry report will be released next week.

• NHTSA informed by Tesla of self-driving car accident 9 days later (Reuters) – The delay in reporting may have misled investors in advance of Tesla’s offer for SolarCity suggest reports, including one by Fortune magazine. To be fair, I don’t think all the details about the accident were fully known immediately. Look at the condition of the vehicle in the Reuters’ report and the Florida Highway Patrol report; the FHP’s sketch of the accident site doesn’t automatically lead one to think the accident was induced by distracted driving or by auto-pilot. Can’t find the report now, but a DVD player was found much later; it was this device which revealed the driver’s last activities. How did the FHP’s report make its way to Tesla? And as Tesla responded, with one million auto accidents a year, not every accident is reported to the NHTSA. Begs the question: should all self-driving car accidents be automatically reported to the NHTSA and their automakers, and why?

• ‘Zero Days’ documentary on Stuxnet out this Friday (Flavorwire) – If director Alex Gibney can make this subject exciting to the average non-technical schmoe, hats off. It’s a challenge to make the tedium of coding exciting to non-coders, let alone fluff process control equipment. This is a really important story with

a very long tail; hope Gibney was able to do it justice.

EIGHT DAYS in session left in U.S. House of Representatives' July calendar. Hearing about EPA scheduled this morning, but I don't think it had anything to do whatsoever with Flint Water Crisis.

Okay, that's enough to get you over the hump, just don't break anything on the way down. I'm off to go fix stuff.

TUESDAY: RUBBISH

This won't be everybody's cup of matcha and may not offer an optimum listening experience for most business offices. Today's kick-in-the-seat to start the week is a Japanese rock genre at the intersection of glam rock and black metal. *Visual kei* rock combines glam's signature elements with black metal's dark, heaviness. Some say punk influences *visual kei* but I really don't see or hear it. Depending on the song, death metal is far more likely to leak through both in sound and appearance.

For a little lighter variant – more pure metal than glam or black – try this live performance from Vistlip. The relationship between *visual kei* and both anime and video games is quite obvious. Want a little estrogen-loaded *visual kei*? Try exist trace's Daybreak; it, too, is not as dark and heavy, though the band can still hammer really black tunes.

Now that the kick in the ass has been locked and loaded…

NINE DAYS
Including today, that's the total number of days booked as in session on the U.S. House of Representatives' business calendar for July, of which only six days have events scheduled.

Can’t see anything farther out. And of the events booked so far, nothing appears for the benefit of the Flint Water Crisis. Roughly 8000 lead-poisoned kids completely forgotten.

Michigan’s state house has a mess of stuff on the calendar, but none of it clearly marked in reference to Flint Water Crisis. I imagine that hack Rep. Pscholka may have something buried in the items labeled “zero budget.”

Brexit buffoonery

Whenever I get really upset with the condition of our state and federal governance, I can just take a look across the pond. The back-stabbing drama surrounding the future leadership of the Conservative Party and the Prime Minister’s office looks like a mashup of House of Cards and Game of Thrones minus dragons. I’ll let Christoph Waltz speak for me about the resignation of Ukip’s Nigel Farage this weekend. I fear, though, that U.S. politics will take the Brexit debacle as a prompt going into the general election.

- Pound fell to lowest level post-Brexit vote (France24) — The perceived inability for either the Conservatives or Labour parties to organize its leadership let alone steer out of Brexit weighs on business. Let’s say Marcy’s right and the Brits manage to put the brakes on this: when and how will that happen? The lack of direction and specificity between now and sometime after September’s next UK election costs money.
- Apple stock could take a hit because of Brexit

(Bloomberg) – Folks may update their iPhones more slowly due to economic pressures, says Citigroup analyst. IMO, it's not the updates that will hurt Apple's income as much as currency fluctuations. Was Apple able to hedge its financial holdings adequately against the abrupt drop in GBP value?

- EU to spend $2B on public+private cybersecurity efforts (The Register) – Will UK be omitted from this spending plan altogether, AND will the EU begin to treat the UK as a potential cybersecurity risk in whatever plans it develops?

Automotive Uh-oh

- German Federal Cartel Office raids six auto industry firms investigating steel price collusion (FAZ.net) – The largest automakers Volkswagen, Daimler and BMW as well as suppliers ZF and Bosch were targeted. German news reports only provide these five company names and not a sixth. Reuters reported GM's Opel division was not included in the raids. Volkswagen was

already smarting badly after the nearly $15B settlement with the U.S. announced last week.

- Electric car maker Tesla hits a speedbump on output (Bloomberg) – Market should have seen this coming. There's no way to smoothly scale up the amount of output buyers want from where Tesla's been without a few hiccups. Stock price took a hit.

Cyberia

- Second "Fappening" hacker will plead guilty (NYMag) – Finally! It only took two years reach this point in prosecution of hacker who phished celebrities accounts for nude photos. But phishing corporations is a threat to the public's security, while phishing women's Gmail and iCloud accounts isn't a threat to anybody, right? Because women's bodies and personal information aren't valuable nor is systematically invading their privacy terrorizing. Ugh. Gender bias in law enforcement.
- Advocacy groups file rulemaking petition with FCC

on automakers' use of Direct Short Range Communication (DSRC) (PublicKnowledge.org) — Automakers are standardizing AI systems around DSRC; two groups want the FCC to

> • Limit DSRC to life and safety uses only. The auto industry plans to take spectrum allocated for safety of life and monetize it with advertising and mobile payments. This compromises cybersecurity and potentially violates the privacy of every driver and passenger.
> • Require automakers to file a cybersecurity plan before activating DSRC systems. This plan should not only show that auto manufacturers have taken appropriate precautions today, but explain how they will update security over the life of the vehicle.
> • Data transparency and breach notification. Auto manufacturers must inform purchasers of DSRC-equipped cars what personal information they collect and how they will use that information. In the event of a data breach, the manufacturer collecting the information must notify the customer.

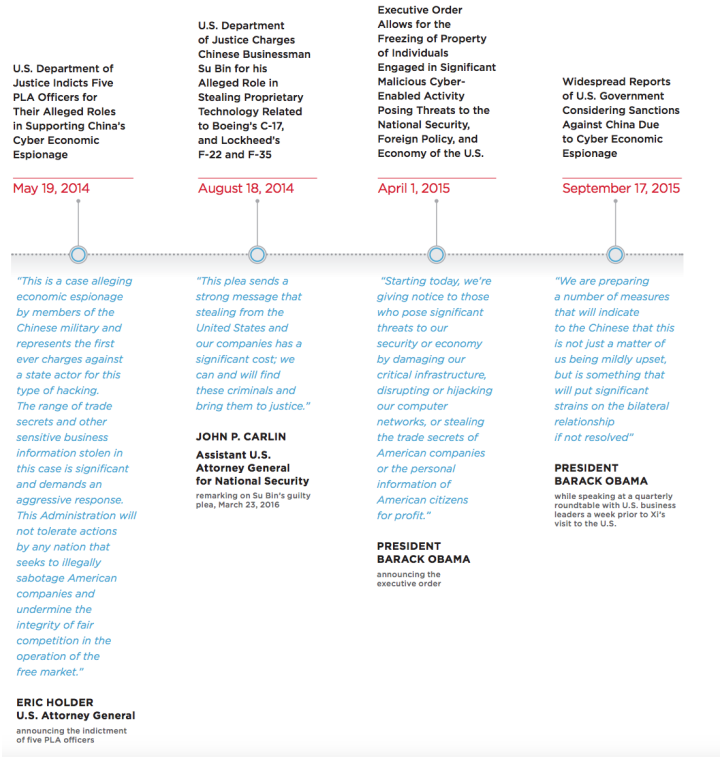
- Conficker malware found widely in internet-enabled medical equipment (Threatpost) — Medical facilities still aren't

> taking adequate measures to ensure internet-enabled equipment remains unattached from the internet, safe from other forms of injection (like USB ports), and free of malware. Devices like dialysis pumps and diagnostic equipment for MRIs and CT scans are infected. Same security gaps also led to leak of 655,000 patients' data over the internet two weeks ago.

Man, even in this heat this snowball just doesn't want to stop once it starts rolling down the hill. At least it's a short week. See you tomorrow!

CYBER-GOGGLES: WHEN CHINA'S TOOL BOX LOOKS LIKE A PILE OF CYBER-HAMMERS

Last week, the cybersecurity firm FireEye released a report largely declaring victory over Chinese cyberspying. The report itself is suspect. It spends two pages talking about internal issues – such as Xi Jinpeng's efforts to consolidate power in China – then throws in a timeline designed to suggest actions the US has done has led to a decline in spying.



The timeline itself is problematic as it suggests both indictments — of some People's Liberation Army hackers targeting industrial companies and one union, and of Chinese businessman Su Bin — as IP hacks.

> In May 2014, the U.S. Department of Justice indicted five PLA officers, marking the first time that the U.S. Government has charged foreign government personnel with crimes related to commercial cyber espionage. Although China warned that the move "jeopardizes China U.S. cooperation," the Department of Justice indicted another Chinese national, Su Bin, the following August for allegedly orchestrating a cyber-enabled economic espionage operation targeting U.S. defense companies.

Neither should be classified so easily (though the press has irresponsibly done so, especially with respect to the PLA indictment). As I have laid out, with one exception the PLA indictment treated the theft of information pertaining to ongoing trade negotiations — something the US engages in aggressively — with the exception

being the theft of trade information that China might have gotten anyone as part of a long-standing nuclear technology transfer deal with the target, Westinghouse. And while Su personally profited off his spying (or that's what he said as part of pleading guilty), the targeted items all have a military purpose.

Without any internal evidence to back the case, FireEye declares that these indictments (the former of which, at least, relies on intelligence shared by FireEye division Mandiant) had an effect in China.

> In 2014, the U.S. Government began taking punitive measures against China, from indicting members of the PLA to raising the possibility of sanctions. These unprecedented measures, though met with skepticism in the U.S., have probably been taken much more seriously in Beijing.
>
> [snip]
>
> In 2013, when we released the APT1 report exposing a PLA cyber espionage operation, it seemed like a quixotic effort to impede a persistent, well-resourced military operation targeting global corporations. Three years later, we see a threat that is less voluminous but more focused, calculated, and still

> successful in compromising corporate networks. Rather than viewing the Xi-Obama agreement as a watershed moment, we conclude that the agreement was one point amongst dramatic changes that had been taking place for years. We attribute the changes we have observed among China-based groups to factors including President Xi's military and political initiatives, the widespread exposure of Chinese cyber operations, and mounting pressure from the U.S. Government.

The report then shows an impressive decline of perceived attacks. But even there, there's no granularity given about where FireEye is seeing the decline (or whether these numbers might rise as it response to attacks on companies that will call FireEye in for hacks that started months or years ago). Again, in its description of the ongoing attacks, FireEye includes a lot of things that every country but the US would consider to be clear national defense hacks.

In the wake of the report, there has been some even more overheated victory laps about the success of the US-Chinese agreement in 2015, as well as this utterly absurd piece insisting that the US doesn't engage in economic espionage. The piece is particularly nonsensical for how it uses evidence from Snowden.

> More importantly, the U.S. does not steal information to give to its companies, as a rule. That none of the documents released from the vast trove of material pilfered by Edward Snowden points to this kind of commercial espionage is indicative. Those who control the Snowden documents are eager to release anything that would harm the U.S., yet they have not yet produced an example of information being given to a U.S. company.
>
> [snip]

> What we know of American espionage against foreign companies (thanks to Snowden) is that the intent of the espionage against commercial targets is to support other American policies: non-proliferation, sanctions compliance, trade negotiations, foreign corrupt practices, and perhaps to gain insight into foreign military technologies. The U.S. as well as other nations who care about such things regard these as legitimate targets for spying—legitimate in the sense that this kind of espionage would be consistent with international law and practice. This spying supports foreign policy goals shared by many countries, in theory if not always in practice.

I say that because there's no evidence from most domestic companies that NSA interacts with — not the Defense contractor targeted in a cyber powerpoint, and certainly not any of the telecoms that partner with the government. You would, by definition, not see evidence of what you're claiming. Moreover, ultimately, this is retreat back to a fetish, the description of certain things to be a national good (like the trade negotiations we've indicted China for), but not others.

Ultimately, American commentators on cybersecurity continue to misunderstand the degree to which our corporations — especially out federal partners — cannot and are not in practice separated from a vision of national good. Though discussions about the degree to which tech companies should be wiling to risk overseas customers to spy without bound is one area where that's assumed, even to the detriment of the tech company bottom lines.

Here's what all this misses. There is spying of the old sort: spying on official government figures. And then there are decisions supporting national well-being (largely economics) that all countries engage in, pushing the set of rules

that help them the most.

Discussions of China's cyberspying have *always* been too isolated for discussions of China's other national economic decisions. China steals just as much from US corporations located in China, but no one seems to care about that as a national security issue. And China *buys* a great deal, and has been buying a lot more of the things that it used to steal. The outcome is the same, yet we fetishize the method.

Which is why I find this so ironic.

A Chinese billionaire with party connections last year purchased the company, Wright USA, that insures a lot of national security officials in case they get sued or criminally investigated.

> The company, Wright USA, was quietly acquired late last year by Fosun Group, a Shanghai-based conglomerate led by Guo Guangchang, a billionaire known as "China's Warren Buffett" who has high-level Communist Party connections.
>
> The links between Guo and Wright USA came under scrutiny by the Treasury Department's Committee on Foreign Investment in the United States, as well as the Office of Director of National Intelligence, the coordinating body of all U.S. spy agencies, soon after Fosun announced the purchase of Wright's parent company last November. The FBI has also launched a criminal probe into whether the company made "unauthorized disclosures of government data to outsiders," according to a well-placed source, who like others, spoke to *Newsweek* on condition of anonymity because the information was sensitive.
>
> (The FBI declined to comment, and Fosun denies the FBI has asked it for any documents.)
>
> U.S. officials are concerned that the

> deal gave Chinese spy agencies a pipeline into the names, job titles, addresses and phone numbers of tens of thousands of American intelligence and counterterrorism officials—many working undercover—going back decades.

This happened after the Chinese acquired via the kind of cybertheft everyone seems to agree is old-fashioned spying the medical records and clearance records of most of Americans cleared personnel. And yet a Chinese firm was able to buy something equally compromising right out from underneath the spooks who oversee such things.

China will get what it wants via a variety of means: stealing domestically when Americans come to visit, stealing via hack, or simply buying. That we treat these differently is just a fetish, and one that seems to blind us to the multiple avenues of threat.

FBI STILL NOT COUNTING HOW OFTEN ENCRYPTION HINDERS THEIR INVESTIGATIONS

The annual wiretap report is out. The headline number is that wiretaps have gone up, and judges still don't deny any wiretap applications.

> The number of federal and state wiretaps reported in 2015 increased 17 percent from 2014. A total of 4,148 wiretaps were reported as authorized in 2015, with 1,403 authorized by federal judges and 2,745 authorized by state judges. Compared to the applications approved during 2014, the number approved by

> federal judges increased 10 percent in 2015, and the number approved by state judges increased 21 percent. No wiretap applications were reported as denied in 2015.

The press has focused more attention on the still very small number of times encryption thwarts a wiretap.

> The number of state wiretaps in which encryption was encountered decreased from 22 in 2014 to 7 in 2015. In all of these wiretaps, officials were unable to decipher the plain text of the messages. Six federal wiretaps were reported as being encrypted in 2015, of which four could not be decrypted. Encryption was also reported for one federal wiretap that was conducted during a previous year, but reported to the AO for the first time in 2015. Officials were not able to decipher the plain text of the communications in that intercept.

Discussing the number — which doesn't include data at rest — on Twitter got me to look at something that is perhaps more interesting.

Back in July 2015, 7 months into the period reported on today, Deputy Attorney General Sally Yates and FBI Director Jim Comey testified in a "Going Dark" hearing. Over the course of the hearing, they admitted that they simply don't have the numbers to show how big a problem encryption is for their investigations, and they appeared to promise to start counting that number.

Around January 26, 2016 (that's the date shown for document creation in the PDF) — significantly, right as FBI was prepping to go after Syed Rizwan Farook's phone, but before it had done so — Comey and Yates finally answered the Questions for the Record submitted after the

hearing. After claiming, in a response to a Grassley question on smart phones, “the data on the majority of the devices seized in the United States may no longer be accessible to law enforcement even with a court order or search warrant,” Comey then explained that they do not have the kind of statistical information Cy Vance claims to keep on phones they can’t access, explaining (over five months after promising to track such things),

> As with the “data-in-motion” problem, the FBI is working on improving enterprise-wide quantitative data collection to better explain the “data-at-rest” problem.”
>
> [snip]
>
> As noted above, the FBI is currently working on improving enterprise-wide quantitative data collection to better understand and explain the “data at rest” problem. This process includes adopting new business processes to help track when devices are encountered that cannot be decrypted, and when we believe leads have been lost or investigations impeded because of our inability to obtain data.
>
> [snip]
>
> We agree that the FBI must institute better methods to measure these challenges when they occur.
>
> [snip]
>
> The FBI is working to identify new mechanisms to better capture and convey the challenges encountered with lawful access to both data-in-motion and data-at =-rest.

Grassley specifically asked Yates about the Wiretap report. She admitted that DOJ was still not collecting the information it promised to back in July.

> The Wiretap Report only reflects the number of criminal applications that are sought, and not the many instances in which an investigator is dissuaded from pursuing a court order by the knowledge that the information obtained will be encrypted and unreadable. That is, the Wiretap Report does not include statistics on cases in which the investigator does not pursue an interception order because the provider has asserted that an intercept solution does not exist. Obtaining a wiretap order in criminal investigations is extremely resource-intensive as it requires a huge investment in agent and attorney time, and the review process is extensive. It is not prudent for agents and prosecutors to devote resources to this task if they know in advance the targeted communications cannot be intercepted. The Wiretap Report, which applies solely to approved wiretaps, records only those extremely rare instances where agents and prosecutors obtain a wiretap order and are surprised when encryption prevents the court-ordered interception. It is also important to note that the Wiretap Report does not include data for wiretaps authorized as part of national security investigations.

These two answers lay out why the numbers in the Wiretap Report are of limited value in assessing how big a problem encryption is.

But they also lay out how negligent DOJ has been in responding to the clear request from SJC back in July 2015.

HOUSE HOMELAND SECURITY COMMITTEE APPARENTLY KNOWS LITTLE ABOUT HOMELAND SECURITY

Here are the first 36 words of an otherwise useful House Homeland Security Committee report on encryption:

> Public engagement on encryption issues surged following the 2015 terrorist attacks in Paris and San Bernardino, particularly when it became clear that the attackers used encrypted communications to evade detection—a phenomenon known as "going dark."

The statement has grains of truth to it. It is true that engagement on encryption surged following the Paris attacks, largely because intelligence committee sources ran around assuming (and probably briefing the White House) that encryption must explain why those same intelligence committee sources had missed the attack. It surged further months later when FBI chose to pick a fight with Apple over Syed Rizwan Farook's work phone which — it was clear from the start — had no evidence relating to the attack on it.

It is also true that ISIS had been using Telegram leading up to the Paris attack; in its wake, the social media company shut down a bunch of channels tied to the group. But there has never been a public claim the plotters used Telegram to plan their attack.

It is also true that an ISIS recruit, arrested and interrogated months before the Paris attack, had told French authorities he had been trained to use a Truecrypt key and an elaborate dead drop method to communicate back to Syria.

But it is not true that the Paris attackers used encryption to hide their plot. They used a great many burner phones, a close-knit network (and with it face-to-face planning), an unusual dialect. But even the one phone that had an encrypted product loaded on it was not using that service.

It is also not true that the San Bernardino attackers used encryption to evade detection. They used physical tools to destroy the phones presumably used to plan the attack. They hid a hard drive via some other, unidentified means. But the only known use of encryption — the encryption that came standard on Farook's work phone — was shown, after the FBI paid to bypass it, not to be hiding anything at all.

Now it's possible there was encryption involved in these attacks we don't know about, that HLSC has gotten classified briefings on. But even if there was, it could not very well have led to a public surge of engagement last year, because it would not be public.

There are reasons to discuss encryption. But factually false claims about terrorists' use of encryption are not among those reasons.

h/t to Access Now's Nathaniel White, who pointed out this bogosity on Twitter.

Update: See this Grugq post laying out what little encryption ISIS has been known to use in any attack.

WEDNESDAY: WANDERING

> *All that is gold does not glitter; not all those who wander are lost.*
>
> — excerpt, The Lord of the Rings by J.

> R. R. Tolkien

It’s a lovely summer day here, cool and dry. Perfect to go walkabout, which I will do straight away after this post.

Hackety-hack-hack, Jack

- Spearphishing method used on HRC and DNC revealed by security firm (SecureWorks) – Here’s their report, but read this Twitter thread if you don’t think you can handle the more detailed version. In short, best practice: DON’T CLICK ON SHORTENED LINKS using services like Bitly, which mask the underlying URL.
- Researchers show speakerless computers can be hacked by listening to fans (arXiv.org) – Air-gapping a computer may not be enough if hackers can listen to fan operation to obtain information. I’ll have to check, but this may be the second such study.
- Another massive U.S. voter database breached (Naked Security) – This time 154 million voters’ data exposed, revealing all manner of details. 154M is larger than the number of voters in the 2012 general

election, though smaller than the 191M voters' records breached in December. At least this time the database owner slammed the breach shut once they were notified of the hole by researcher Chris Vickery. Nobody's fessed up to owning the database involved in the the December breach yet.

- Speaking of Vickery: Terrorism databased leaked (Reddit) – Thomson-Reuters' database used by governments and banks to identify and monitor terrorism suspects was leaked (left open?) by a third party. Vickery contacted Thomson-Reuters which responded promptly and closed the leak. Maybe some folks need to put Vickery on retainer…
- Different kind of hack: Trump campaign hitting up overseas MPs for cash? Or is he? (Scotsman) – There are reports that Trump's campaign sent fundraising emails received by elected representatives in the UK and Iceland. Based on what we know now about the spearphishing of HRC and DNC, has anybody thought to do forensics on these

emails, especially since government officials are so willing to share them widely? Using these kinds of emails would be a particularly productive method to spearphish government and media at the same time, as well as map relationships. Oh, and sow dissension inside the Trump family, urm, campaign. On the other hand, lack of response from Trump and team suggests it's all Trump.

Makers making, takers taking

- Apple granted a patent to block photo-taking (9to5Mac) – The technology relies on detecting infrared signals emitted when cameras are used. There's another use for the technology: content can be triggered to play when infrared signal is detected.
- Government suppressing inventions as military secrets (Bloomberg) – There's merit to this, preventing development of products which may undermine national security. But like bug bounties, it might be worth paying folks who identify methods to breach

security; it's a lot cheaper than an actual breach, and a bargain compared to research detecting the same.

- Google wants to make its own smartphone (Telegraph-UK) – This is an effort apart from development of the modular Ara device, and an odd move after ditching Motorola. Some tech industry folks say this doesn't make sense. IMO, there's one big reason why it'd be worth building a new smartphone from the ground up: security. Google can't buy an existing manufacturer without a security risk.
- Phonemaker ZTE's spanking for Iran sanction violations deferred (Reuters) – This seems kind of odd; U.S. Commerce department agreed to a reprieve if ZTE cooperated with the government. But then think about the issue of security in phone manufacturing and it makes some sense.

A-brisket, a Brexit

- EU health commissioner Andriukaitis' response to Nigel Farage's insulting remarks (European Commission) – Farage

prefaced his speech to European Commissioners yesterday by saying “Most of you have never done a proper day’s work in your life.” Nice way to win friends and influence people, huh? Dr. Vytenis Andriukaitis is kinder than racist wanker Farage deserves.

- Analysis of next couple years post-Brexit (Twitter) — Alex White, Director of Country Analysis at the Economist Intelligence Unit, offers what he says is “a moderate/constructive call” with “Risks definitely to the downside not to the upside.” It’s very ugly, hate to see what a more extreme view would look like. A pity so many Leave voters will never read him.

Follow-up: Facebook effery

Looks like Facebook’s thrown in the towel on users’ privacy altogether, opening personal profiles in a way that precludes anonymous browsing. Makes the flip-flop on users’ location look even more sketchy. (I can’t tell you anymore about this from personal experience because I gave up on Facebook several years ago.)

Happy hump day!

MONDAY: FIERCE DOG

> *Hunger and fear are the only realities in dog life: an empty stomach makes a fierce dog.*
>
> – excerpt, personal journal of Capt. Robert Falcon Scott

This short film by Aaron Dunleavy was inspired by his childhood in Blackburn, Lancashire UK. The script was improvised and cast using locals.

All districts in Lancashire voted Leave during last week's Brexit referendum, with 65% of Blackburn voters supporting Leave.

Worth noting an article in Lancashire Telegraph about an Aldi's store under construction. Aldi's is a German-owned grocery store chain; have to wonder if construction will be completed.

Brexit botch bits

- @shockproofbeats on Brexit's impact on Northern Ireland (Storify) – It's messy now and promises to be even uglier.
- Downside for China (and other foreign investors): Real estate purchases may be put on hold (SCMP) – Some deals in the works may be halted until the pound is more stable. On the other hand, Britain may step in and put the brakes on sales; too easy for overseas entities with big money to buy up property while pound is depressed.

- Upside for China (and other banking centers): Business could pick up in Hong Kong (SCMP) – London is the second largest trading center of yuan next to Hong Kong; some of the business could shift back to Hong Kong, especially if HSBC bank choose to relocate its headquarters to HK from London.
- No change in position on Brexit referendum since last Friday according to PM David Cameron (Independent-UK) – Though Cameron is now going to leave in September. He continued to push triggering of the Article 50 to his successor while taking pot shots at Labor Party over its purge this weekend. Not certain most Americans will notice just how Cameron has managed to shift the blame to both MPs and the people for a referendum he proposed, or how he has turned execution of Article 50 into a poisoned chalice. Lord Chancellor Secretary of State for Justice Michael Gove, Leave campaign proponent, was present at today's session in Parliament but said

nothing before disappearing. Boris Johnson, MP for Uxbridge and South Ruislip and Leave campaign proponent, was noticably absent. Wankers all three.

SCOTUS Week

Waiting around watching the court for good or ill until this morning is kind of like waiting for Shark Week – hey, it IS Shark Week! What a coincidence!

- Texas' HB2 ruled unconstitutional (WaPo) – Immensely restrictive state law which anti-abortion proponents claimed protected women struck down; majority justices saw through fallacious arguments. Usual suspects dissented (Robers/Thomas/Alito).
- Domestic abusers can be denied guns based on misdemeanor charges (NPR) – Now if only there was a universal background check law to ensure any gun seller could identify domestic abusers…Case before SCOTUS even more exceptional as Justice Thomas asked questions from the bench.
- Court turns away appeal on Montana state law limiting med marijuana sellers to 3 patients max (Billings Gazette) – What a nuisance

for folks like cancer patients who need medical marijuana in a such a rural state.

Miscellaneous trouble

- U.S. studied *Aedes aegypti* mosquitoes released in American neighborhoods (Atlas Obscura) – *Are you kidding me?!* The U.S. tested the same mosquitoes which carry Zika, dengue, and yellow fever by releasing them in residential neighborhoods – AFTER they had nearly been wiped out of the western hemisphere?
- Pin-based security system may end after IRS hacked again (Naked Security) – Looks like the weakest link is the e-File Pin for account access, same as in hacks before April 15th this year. The knowledge-based verification component was easily undermined by determined hackers who could look up information.

Promises to be a busy week ahead. Stay tuned!

WEDNESDAY: GET BACH

Summer bug laid me up. I'm indulging in the audio equivalent of tea with honey, lemon, and a shot of something to scare away the bug. A little cello playing by Yo-Yo Ma never fails to make me feel better.

This sweet video is enlightening, didn't realize Ma had an older sister who was an accomplished musician at a tender age. Worthwhile to watch this week considering the blizzard of arguments about immigrants and refugees here and abroad.

And then for good measure, a second favorite added in the mix – Yo-Yo Ma and Itzhak Perlman together, performing Beethoven's Triple Concerto Fantasy.

There. I feel a little better already.

Probably better than frustrated House Democrats led by Rep. John Lewis who are engaging in a sit-in protest on House floor demanding a vote on No-Fly-No-Buy gun control. If you want to watch the action, you'll have to check social media. It's said House GOP leadership ensured CSPAN cameras were shut off.

Diesel do you

- Volkswagen streamlining offerings to cut costs, 40 makes on the chopping block (Bloomberg) – This is the old General Motors play that eventually killed Oldsmobile and Pontiac to reduce costs related to duplicative brands. Makes sense, especially if this hatchet job kills passenger diesels. Note the story says a fix may come later – uh-huh,

like never? Because VW can't handle the volume of required repairs OR the lack of actual clean diesel technology, OR both?

- Testimony in S Korea: VW's upper management may have ordered regulatory cheats (The Hankyoreh) – Story is focused on emissions controls defeat and approval process, but sound controls were also an issue in South Korea. Were those likewise suppressed by order of VW's German head office?
- Former CEO under investigation for securities fraud (Reuters) – Big investors want to know why it took a year for Winterkorn to act after the emissions controls defeat were made public by researchers. Bet there's a link between Winterkorn's notification of researchers' findings and the destruction of emails.

Sigh, cyber, sigh

- Why the hell is PayPal asking a German cloud service provider to monitor its customers? (Fortune) – Seafile ditched PayPal as a payment service provider

after PayPal insisted Seafile must monitor its users' files. That's a violation of German privacy laws. But why did PayPal ask this in the first place? The argument about illicit file sharing is a stretch.

- Google's rolling out an easier Two-Factor Authentication tool (Google Apps Updates Blog) – Google's enterprise users will see this first, but all Google users should expect new prompts on the desktop and new apps using this new 2FA system. This should replace the 6-digit text message codes as well as verification codes.
- Facebook's ethical decision process for research projects still iffy (The Chronicle of Higher Education) – If you can't release all the details of the deliberative process, it looks pretty shady. What compromises were made? What points weren't covered or ignored? Who knows?
- Toothpic technology designed to detect photo theft (PetaPixel) – But the same well-meaning technology is based on fingerprinting a

> camera, identifying the user by camera. So much for privacy.

Wait, what?

Did you know Led Zeppelin is being sued over Stairway to Heaven? Allegedly a key riff in the famous 40-year-old tune was stolen, violating copyright. *Forty years.* ~smh~

Going back to a recumbent position. Stay braced for the outcome of the sit-in and Brexit vote tomorrow.