THURSDAY MORNING: TABOO YOU

Still on spring break around here. If I was legit on a road trip some place warm right now, you'd find me lounging in the sun, sipping fruity cocktails at all hours, listening to some cheesy exotica like this Arthur Lyman piece I've shared here.

Though horribly appropriative and colonialist, it's hard not to like exotica for its in-your-face corniness. I think my favorite remains Martin Denny's Quiet Village. It brings back memories from the early 1960s, when life was pretty simple.

Let's have a mai tai for breakfast and get on with our day.

Urgent: Increasing number of hospitals held ransom
Last month it was just one hospital – Hollywood Presbyterian Medical Center paid out bitcoin ransom.

Last week it was three – two Prime Healthcare Management hospitals in California and a Methodist Hospital in Kentucky held hostage.

Now, an entire chain of hospitals has been attacked by ransomware, this time affecting the servers of 10 related facilities in Maryland and Washington DC. The FBI is involved in the case. Is this simple extortion or terrorism? The patients diverted from the facilities to other hospitals' emergency rooms probably don't care which it is – this latest attack interfered with getting care as quickly as possible. Let's hope none of the diverted patients, or those already admitted into the MedStar Union Memorial Hospital chain, have been directly injured by ransomware's impact on the system.

The MedStar cases spawns many questions:

- Was any patient's physical

health care negatively affected by the ransomware attack?

- Given the risks to human health, why aren't hospitals better prepared against ransomware?
- Have hospitals across the country treated ransomware as a potential HIPAA violation?
- Was MedStar targeted because of its proximity to Washington DC?
- Was Hollywood Presbyterian Medical Center targeted because its owner, CHA Medical Center, is South Korean?
- Were any patients being treated at MedStar also affected by the OPM data breach, or other health insurance data breaches?
- How much will ransomware affect U.S. healthcare costs this year and next?

Bet you can think of a couple more questions, too, maybe more than a couple after reading this:

> Hospitals are considered critical infrastructure, but unless patient data is impacted there is no requirement to disclose such hackings even if operations are disrupted.
>
> Computer security of the hospital industry is generally regarded as poor,

> and the federal Health and Human Services Department regularly publishes a list of health care providers that have been hacked with patient information stolen. The agency said Monday it was aware of the MedStar incident.

Apple iPhone cases emerge

After the San Bernardino #AppleVsFBI case, more law enforcement investigations relying on iPhones are surfacing in the media.

- L.A. police crack open iPhone with fingerprints obtained under warrant (Forbes);
- FBI will assist county prosecutor in Arkansas with iPhone belonging to alleged teen killer (Los Angeles Times); the method may be the same hack used on the San Bernardino phone, which was supposed to be a one-off (Network World);
- ACLU found 63 other cases in which FBI used All Writs Act to obtain iPhone/Android smartphone data from Apple and Google (The Register).

Stupid stuff

- In spite of screwing up not once but twice by releasing its racist, obnoxious Tay AI chatbot, Microsoft tripled down on a future full of chatbots you can build

yourself with their tools. (Ars Technica) – Ugh. The stupid…

- UK's Ministry of Defense awarded funding to Massive Analytics for work on "Artificial precognition and decision-making support for persistent surveillance-based tactical support" (Gov.UK) – OMG Precog in warfare. Human-free drone attacks. What could go wrong?
- Rich white guys queue up outside Tesla dealerships for days waiting to pre-order the new Tesla 3 (Vancity Buzz) – Vancouver, Sydney, probably other places I'm too arsed to bother with, because rich white guys.

That's quite enough. Back to pretending I'm lying under a cerulean sky, baking my tuchis, cold drink in hand.

WEDNESDAY MORNING: BREAKING SPRING

> *In the Spring a livelier iris changes on the burnish'd dove;*
> *In the Spring a young man's fancy lightly turns to thoughts of love.*

> — excerpt, Locksley Hall by Alfred, Lord Tennyson

Welcome to spring break. And by break, I mean schedules are broken around here. Nothing like waiting up until the wee hours for a young man whose fancy not-so-lightly turned to love, because spring.

~yawn~

While the teenager lies abed yet, mom here will caffeinate and scratch out a post. It may be early afternoon by the time I get over this spring-induced sleep deprivation and hit the publish button.

Apple blossoms — iPhones and iPads, that is
Not much blooming on the #AppleVsFBI front, where Apple now seeks information about the FBI's method for breaking into the San Bernardino shooter's iPhone 5C. The chances are slim to none that the FBI will tell Apple anything. Hackday offers a snappy postmortem about this case with an appropriate amount of skepticism.

I wonder what Apple's disclosure will look like about this entire situation in its next mandatory filing with the SEC? Will iPhone 5C users upgrade to ditch the undisclosed vulnerability?

What if any effect will the iPhone 5C case have on other criminal cases where iPhones are involved — like the drug case Brooklyn? Apple asked for a delay in that case, to assess its position after the iPhone 5C case. We'll have to wait until April 11 for the next move in this unfolding crypto-chess match.

In the meantime, spring also means baseball, where new business blossoms for Apple. Major League Baseball has now signed with Apple for iPads in the dugout. Did the snafu with Microsoft's Surface tablets during the NFL's AFC championship game persuade the MLB to go with Apple?

Volkswagen coasting

It's downhill all the way for VW, which missed last week its court-imposed 30-day deadline to offer a technical solution on its emissions standards cheating "clean diesel" passenger vehicles. If there was such a thing as "clean diesel," VW would have met the deadline; as I said before, there's no such thing as "clean diesel" technology. The judge allowed a 30-day extension to April 24, but my money is on another missed deadline. Too bad there's not a diesel engine equivalent of Cellebrite, willing to offer a quick fix to VW or the court, huh?

Of note: former FBI director Robert Mueller has been named "special master" on this case by Judge Charles Breyer; Mueller has been meeting with all the parties involved. What the heck is a "special master"? We may not have a ready answer, but at least there's a special website set up for this case, In re: Volkswagen "Clean Diesel" MDL.

The cherry on top of this merde sundae is the Federal Trade Commission's lawsuit filed yesterday against VW for false advertising promoting its "clean diesel" passenger cars.

With no bottom yet in sight, some are wondering if VW will simply exit the U.S. market.

Automotive odd lot

- Jury says GM's ignition switch was bad, but not at fault in a 2014 accident in New Orleans (Reuters) – Keep an eye on media representation of this case. Headline on this one focused on the switch, not the jury's decision.
- Car-to-car communications will be road tested soon (MIT Technology Review) –

This technology might have prevented Google's self-driving car from getting crunched by a bus recently.

- Dude demonstrates his hack of Alexa + Raspberry Pi + OBDLink to remote start his car (Gizmodo) — What. even.

Did Tennyson write anything about spring spawning naps? Because I feel like I need one. Hope we're back in the groove soon. See you in the morning.

THE STUXNET TEAM REUNION

On Thursday, DOJ had a big dog and pony show over the indictment of 7 Iranians in connection with cyberattacks on US banks and a small dam in suburban NY.

> A grand jury in the Southern District of New York indicted seven Iranian individuals who were employed by two Iran-based computer companies, ITSecTeam (ITSEC) and Mersad Company (MERSAD), that performed work on behalf of the Iranian Government, including the Islamic Revolutionary Guard Corps, on computer hacking charges related to their involvement in an extensive campaign of over 176 days of distributed denial of service (DDoS) attacks.
>
> Ahmad Fathi, 37; Hamid Firoozi,

> 34; Amin Shokohi, 25; Sadegh Ahmadzadegan, aka Nitr0jen26, 23; Omid Ghaffarinia, aka PLuS, 25; Sina Keissar, 25; and Nader Saedi, aka Turk Server, 26, launched DDoS attacks against 46 victims, primarily in the U.S financial sector, between late 2011 and mid-2013. The attacks disabled victim bank websites, prevented customers from accessing their accounts online and collectively cost the victims tens of millions of dollars in remediation costs as they worked to neutralize and mitigate the attacks on their servers. In addition, Firoozi is charged with obtaining unauthorized access into the Supervisory Control and Data Acquisition (SCADA) systems of the Bowman Dam, located in Rye, New York, in August and September of 2013.

I agree with Jack Goldsmith about this: It's pretty comical that the country that disrupted major installments in Iran is now indicting Iranians for DDOS attacks on instruments of power that the US used to attack Iran, the nation's banks. It invites a similarly theatrical indictment of Keith Alexander.

> The U.S. indictment is not premised on an international law violation. It is based on violation of U.S. law for harm the Iranians caused inside the United States. The Iranians could invoke precisely the same principle: An Iran indictment for the U.S. cyberattacks would be based on a violation of

> Iranian domestic law for harm caused in Iran by U.S. officers. In short, the cyberattacks from each nation violated the criminal laws of the other nation.
>
> The United States is likely less concerned with charges of hypocrisy than with deterring attacks on its financial infrastructure. Attorney General Lynch said yesterday that the indictment sends "a powerful message: that we will not allow any individual, group, or nation to sabotage American financial institutions or undermine the integrity of fair competition in the operation of the free market." FBI Director James B. Comey added: "By calling out the individuals and nations who use cyber-attacks to threaten American enterprise, as we have done in this indictment, we will change behavior."
>
> But will the indictments change behavior? The Iranians will almost certainly never appear in the United States and thus never go to trial. John Carlin, the Justice Department's top national security lawyer, argued late last year that indictments for cybercrimes can contribute to deterrence even if the defendants are never prosecuted because they expose the responsible actors and demonstrate more broadly that the United States has powerful tools to discover and identify those behind cyberattacks. "The world is small, and our

> memories are long," Director Comey said yesterday, explaining the government's deterrence logic. "People often like to travel for vacation or education, and we want them looking over their shoulder."
>
> It is hard to assess whether the deterrence effect of the indictments will be large enough to stop further attacks on financial infrastructure or so small that they invite more attacks. Moreover, any deterrence achieved by the indictments comes at the cost of exposing U.S. intelligence capabilities and inviting similarly theatric retaliatory indictments.

The timing of this particular theatrical indictment is all the more interesting given that – as Josh Gerstein points out – the actual indictment was handed up in January, just after the nuclear deal and prisoner swap with Iran was finalized.

> The indictment, handed up by a grand jury in Manhattan on Jan. 21 and unsealed Thursday, charges seven Iranian nationals with launching a cyber assault that impaired the computer systems of major U.S. financial institutions in 2012. One of the defendants is also charged with attempting to take over the controls of a dam in Rye, N.Y.
>
> On the weekend of Jan. 16, the U.S. and Iran implemented the intensely negotiated nuclear deal and carried out a prisoner

> swap. Under the pact, at least four Americans were released from Iranian prisons, including Washington Post reporter Jason Rezaian. President Barack Obama signed pardons or commutations for seven Iranian nationals who were the subject of U.S. criminal cases alleging export violations. Cases were dropped against 14 other Iranians U.S. officials said were unlikely ever to be brought to justice in American courts.

All the more so given this news: last week (apparently after Thursday), Admiral Mike Rogers had a "secret" meeting with Israel's Intelligence Corps Unit 8200, the unit CyberCom partnered with on the StuxNet attack.

> The senior Israeli official noted that one of the subjects that Rogers discussed in Israel was cooperation in the field of cyber defense, particularly in the face of attacks from Iran and Hezbollah. A few days before Rogers' arrival in Israel, the U.S. Justice Department filed indictments for the first time against a group of Iranian hackers on charges of carrying out cyber attacks on banks and essential infrastructure in the U.S. three years ago at the behest of the Iranian Revolutionary Guards. Israel has also faced cyber attacks from Iran and Hezbollah, which according to senior IDF officers were prominent during the fighting with Hamas and its allies in Gaza in the summer of 2014, but

> have risen in intensity in recent months.

It seems, then, unsealing the indictment is not so much about deterrence, as it is a show (though I'm unclear on the audience — the international public? or the Israelis themselves?) as Israel and the US prepare to ratchet up the cyberwar against Iran.

Reminder: We shut down some functionality in an attempt to isolate the issues that crashed the site last Thursday. We're getting closer but still have comments shut down. Bear with us!

DOJ CLAIMS THE CYBERSECURITY RELATED OLC MEMO IS ALSO A STELLAR WIND MEMO

I've written a bunch of times about an OLC memo Ron Wyden keeps pointing to, suggesting it should be declassified so we all can know what outrageous claims DOJ made about common commercial service agreements. Here's my most complete summary from Caroline Krass' confirmation process:

> Ron Wyden raised a problematic OLC opinion he has mentioned in unclassified settings at least twice in the last year (he also wrote a letter to Eric Holder

about it in summer 2012): once in a letter to John Brennan, where he described it as "an opinion that interprets common commercial service agreements [that] has direct relevance to ongoing congressional debates regarding cybersecurity legislation." And then again in Questions for the Record in September.

Having been ignored by Eric Holder for at least a year and a half (probably closer to 3 years) on this front and apparently concerned about the memo as we continue to discuss legislation that pertains to cybersecurity, he used Krass' confirmation hearing to get more details on why DOJ won't withdraw the memo and what it would take to be withdrawn.

> Wyden: The other matter I want to ask you about dealt with this matter of the OLC opinion, and we talked about this in the office as well. This is a particularly opinion in the Office of Legal Counsel I've been concerned about — I think the reasoning is inconsistent with the public's understanding of the law and as I indicated I believe it needs to be withdrawn. As we talked about, you were familiar with it. And my first question — as I indicated I would ask — as a senior

> government attorney, would you rely on the legal reasoning contained in this opinion?
>
> Krass: Senator, at your request I did review that opinion from 2003, and based on the age of the opinion and the fact that it addressed at the time what it described as an issue of first impression, as well as the evolving technology that that opinion was discussing, as well as the evolution of case law, I would not rely on that opinion if I were—
>
> Wyden: I appreciate that, and again your candor is helpful, because we talked about this. So that's encouraging. But I want to make sure nobody else ever relies on that particular opinion and I'm concerned that a different attorney could take a different view and argue that the opinion is still legally valid because it's not been withdrawn. Now, we have tried to get Attorney General Holder to withdraw it, and I'm trying to figure out — he has not answered our letters — who at the Justice Department has

the authority to withdraw the opinion. Do you currently have the authority to withdraw the opinion?

Krass: No I do not currently have that authority.

Wyden: Okay. Who does, at the Justice Department?

Krass: Well, for an OLC opinion to be withdrawn, on OLC's own initiative or on the initiative of the Attorney General would be extremely unusual. That happens only in extraordinary circumstances. Normally what happens is if there is an opinion which has been given to a particular agency for example, if that agency would like OLC to reconsider the opinion or if another component of the executive branch who has been affected by the advice would like OLC to reconsider the opinion they will come to OLC and say, look, this is why we think you were wrong and why we believe the opinion should be corrected. And they will be doing that when they have a practical need for the opinion because of particular

> > operational activities that they would like to conduct. I have been thinking about your question because I understand your serious concerns about this opinion, and one approach that seems possible to me is that you could ask for an assurance from the relevant elements of the Intelligence Community that they would not rely on the opinion. I can give you my assurance that if I were confirmed I would not rely on the opinion at the CIA.
>
> > Wyden: I appreciate that and you were very straightforward in saying that. What concerns me is unless the opinion is withdrawn, at some point somebody else might be tempted to reach the opposite conclusion. So, again, I appreciate the way you've handled a sensitive matter and I'm going to continue to prosecute the case for getting this opinion withdrawn.

The big piece of news here — from Krass, not Wyden — is that the opinion dates to 2003, which dates it to the transition period bridging Jay

> Bybee/John Yoo and Jack Goldsmith's tenure at OLC, and also the period when the Bush Administration was running its illegal wiretap program under a series of dodgy OLC opinions. She also notes that it was a memo on first impression — something there was purportedly no law or prior opinion on — on new technology.

Back in November, ACLU sued to get that memo. The government recently moved for summary judgment based on the claim that a judge in DC rejected another ACLU effort to FOIA the document, which is a referral to ACLU's 2006 FOIA lawsuit for documents underlying what was then called the "Terrorist Surveillance Program" and which we now know as Stellar Wind. Here's the key passage of that argument.

> The judgment in EPIC precludes the ACLU's claim here. First, EPIC was an adjudication on the merits that involved the district court's reviewing in camera the same document that is at issue in this litigation, and granting summary judgment to the government after finding that the government had properly asserted Exemptions One, Three, and Five — the same exemptions asserted here — to withhold the document. See Colborn Decl. ¶ 13; EPIC, 2014 WL 1279280, at *1. Second, the ACLU was a plaintiff in EPIC. Id. Finally, the claims asserted in this action were, or could have been, asserted in EPIC. The FOIA claim at issue in EPIC arose from a series of

> requests that effectively sought all OLC memoranda concerning surveillance by Executive Branch agencies directed at communications to or from U.S. citizens.2at See id. Even if the ACLU did not know that this specific memorandum was included among the documents reviewed in camera by the EPIC court, the ACLU had a full and fair opportunity to make any and all arguments in seeking disclosure of that document. Indeed, in EPIC, the government's assertion of exemptions received the highest level of scrutiny available to a plaintiff in FOIA litigation—the district court issued its decision after reviewing the document in camera and determining that the government's assertions of Exemptions One, Three, and Five were proper. Colborn Decl. ¶ 13. The ACLU's claim in this lawsuit is therefore barred by claim preclusion.
>
> 2 One of the FOIA requests at issue in EPIC sought "[a]ll memoranda, legal opinions, directives or instructions from [DOJ departments] issued between September 11, 2001, and December 21, 2005, regarding the government's legal authority for surveillance activity, wiretapping, eavesdropping, and other signals intelligence operations directed communications to or from U.S. citizens." Elec. Privacy Information Ctr. v. Dep't of Justice, 511 F. Supp.

> 2d 56, 63 (D.D.C. 2007).

Wyden just sent a letter to Loretta Lynch disputing some claim made in DOJ's memorandum of law.

> I encourage you to direct DOJ officials to comply with the pending FOIA request.
>
> Additionally, I am greatly concerned that the DOJ's March 7, 2016 memorandum of law contains a key assertion which is inaccurate. This assertion appears to be central to the DOJ's legal arguments, and I would urge you to take action to ensure that this error is corrected.
>
> I am enclosing a classified attachment which discusses this inaccurate assertion in more detail.

Here are some thoughts about what the key inaccurate assertion might be:

ACLU never had a chance to argue for this document as a cybersecurity document

Even the section I've included here pulls a bit of a fast one. It points to EPIC's FOIA request (these requests got consolidated), which asked for OLC memos in generalized fashion, as proof that the plaintiffs in the earlier suit had had a chance to argue for this document.

But ACLU did not. *They* asked for "legal reviews of [TSP] and its legal rationale." In other words, back in 2006 and back in 2014, ACLU was focused on Stellar Wind, not on cybersecurity spying (which Wyden has strongly suggested this memo implicates). So they should be able to make a bid for this OLC memo as something affecting domestic spying for a cybersecurity purpose.

DOJ claimed only Wyden had commented publicly about the document, not Caroline Krass

DOJ makes a preemptive effort to discount the possibility that Ron Wyden's repeated efforts to draw attention to this document might constitute new facts for the ACLU to point to to claim they should get the document.

> Nor is there any evidence the memorandum has been expressly adopted as agency policy or publicly disclosed. Colborn Decl. ¶¶ 23-24. Although the ACLU's complaint points to statements about the document by Senator Wyden, he is not an Executive Branch official, and his statements cannot effect any adoption or waiver
>
> [snip]
>
> The ACLU may argue that statements made by Senator Ron Wyden regarding the document, including in letters to the

> Attorney General, constitute new facts or changed circumstances. See Compl. ¶ 2 ("In letters sent to then–Attorney General Eric Holder, Senator Wyden suggested that the executive branch has relied on the Opinion in the past and cautioned that the OLC's secret interpretation could be relied on in the future as a basis for policy."). But such statements do not constitute new facts or changed circumstances material to the ACLU's FOIA claim because they do not evince any change of the Executive Branch's position vis-à-vis the document or otherwise affect its status under FOIA. See Drake, 291 F.3d at 66; Am. Civil Liberties Union, 321 F. Supp. 2d at 34. As the Senator is not an Executive Branch official, his statements about the document do not reflect the policy or position of any Executive Branch agency. See Brennan Center v. DOJ, 697 F.3d 184, 195, 206 (2d Cir. 2012); Nat'l Council of La Raza v. DOJ, 411 F.3d 350, 356-59 (2d Cir. 2005); infra at 11-12. Senator Wyden's statements are simply not relevant to whether the document has been properly withheld under Exemptions One, Three, and Five, and do not undermine the applicability of any of those exemptions. Additionally, the Senator has made similar statements regarding the document at issue in letters sent during at least the last four years. Compl. ¶

> 2. Thus, the Senator's statements regarding the document are not new facts since they were available to Plaintiffs well before the district court ruled in EPIC.

That's all well and good. But the entire discussion ignores that then Acting OLC head and current CIA General Counsel Caroline Krass commented more extensively on the memo than anyone ever has on December 17, 2013 (see my transcript above). This is a still-active memo, but the then acting OLC head said this about the memo in particular.

> I have been thinking about your question because I understand your serious concerns about this opinion, and one approach that seems possible to me is that you could ask for an assurance from the relevant elements of the Intelligence Community that they would not rely on the opinion. I can give you my assurance that if I were confirmed I would not rely on the opinion at the CIA.

That seems to be new information from the Executive branch (albeit before the March 31, 2014, final judgment in that other suit).

I'd say this detail is the most likely possibility for DOJ's inaccuracy, except that Krass' comments are in the public domain, and have been been written about by other outlets. It wouldn't seem that Wyden would need to identify this detail in secret.

(I think it's possible some of the

newly declassified language in Stellar Wind materials may be relevant to, but I will have to return to that.)

The document may be a different document

DOJ's memo and the Paul Colborn declaration describe this as a March 30, 2003 memo written by John Yoo.

> The withheld document is a 19-page OLC legal advice memorandum to the General Counsel of an executive branch agency, drafted at the request of the General Counsel, dated March 30, 2003 and signed by OLC Deputy Assistant Attorney General John Yoo. The memorandum was written in response to confidential communications from an executive branch client soliciting legal advice from OLC attorneys. As with all such OLC legal advice memoranda, the document contains confidential client communications made for the purpose of seeking legal advice and predecisional legal advice from OLC attorneys transmitted to an executive branch client as part of government deliberative processes. In light of the fact that the document's general subject matter is publicly known, the identity of the recipient agency is itself confidential client information protected by the attorney-client privilege.

But their claim that ACLU has already been denied this document under FOIA is based on the claim that this document is the same document as one identified in a Steven Bradbury declaration submitted in the Stellar Wind suit. Here's how he described the document.

> DAG 42 is a 19-page memorandum, dated May 30, 2003, from a Deputy Assistant Attorney General in OLC to the General Counsel of another Executive Branch agency. This document is withheld under FOIA Exemptions One, Three, and Five.

This may be an error (if so, Bradbury is probably correct, as March 30, 2003 was a Sunday), but a document dated March 30, 2003 cannot be the same document as one dated May 30, 2003. If it's not a simple error in dates, it may suggest that the document the DC court reviewed was a later revision, perhaps one making less outrageous claims. Moreover, as I'll show in my post on newly learned Stellar Wind information, the change in date (as well as the confirmation that Yoo wrote the memo) make the circumstances surrounding this memo far more interesting.

Update: In Ron Wyden's amicus in this case, he made it clear the correct date is May 30, 2003.

The document may not have been properly classified

As noted, this is a March 2003 OLC memo written by John Yoo. That's important not just because Yoo was freelancing on

certain memos at the time. But more importantly, because a memo he completed just 16 days earlier violated all guidelines on classification. Here's what former ISOO head Bill Leonard had to say about John Yoo's March 14, 2003 torture memo.

> The March 14, 2003, memorandum on interrogation of enemy combatants was written by DoJ's Office of Legal Counsel (OLC) to the General Counsel of the DoD. By virtue of the memorandum's classification markings, the American people were initially denied access to it. Only after the document was declassified were my fellow citizens and I able to review it for the first time. Upon doing so, I was profoundly disappointed because this memorandum represents one of the worst abuses of the classification process that I had seen during my career, including the past five years when I had the authority to access more classified information than almost any other person in the Executive branch. The memorandum is purely a legal analysis – it is not operational in nature. Its author was quoted as describing it as "near boilerplate."! To learn that such a document was classified had the same effect on me as waking up one morning and learning that after all these years, there is a "secret" Article to the Constitution that the American people do not even know about.
>
> [snip]

> In this instance, the OLC memo did not contain the identity of the official who designated this information as classified in the first instance, even though this is a fundamental requirement of the President's classification system. In addition, the memo contained neither declassification instructions nor a concise reason for classification, likewise basic requirements. Equally disturbing, the official who designated this memo as classified did not fulfill the clear requirement to indicate which portions are classified and which portions are unclassified, leading the reader to question whether this official truly believes a discussion of patently unclassified issues such as the President's Commander-in-Chief authorities or a discussion of the applicability to enemy combatants of the Fifth or Eighth Amendment would cause identifiable harm to our national security. Furthermore, it is exceedingly irregular that this memorandum was declassified by DoD even though it was written, and presumably classified, by DoJ.

Given that Yoo broke all the rules of classification on March 14, it seems appropriate to question whether he broke all rules of classification on March 30, 16 days later, especially given some squirrelly language in the current declarations about the memo.

Here's what Colborn has to say about

the classification of this memo (which I find to be curious language), after having made a far more extensive withholding argument on a deliberative process basis.

> OLC does not have original classification authority, but when it receives or makes use of classified information provided to it by its clients, OLC is required to mark and treat that information as derivatively classified to the same extent as its clients have identified such information as classified. Accordingly, all classified information in OLC's possession or incorporated into its products has been classified by another agency or component with original classifying authority.
>
> The document at issue in this case is marked as classified because it contains information OLC received from another agency that was marked as classified. OLC has also been informed by the relevant agency that information contained in the document is protected from disclosure under FOIA by statute.

As far as the memo of law, it relegates the discussion of the classified nature of this memo to a classified declaration by someone whose identity remains secret.

> As explained in the classified declaration submitted for the Court's ex parte, in camera review,1 this information is also classified and protected

> from disclosure by statute.

Remember, *this memo is about* some secret interpretation of common commercial service agreements. Wyden believes it should be "declassified and released to the public, so that anyone who is a party to one of these agreements can consider whether their agreement should be revised or modified."

If this is something that affects average citizens relationships with service providers, it seems remarkable that it can, at the same time, be that secret (and remain in force). While Wyden certainly seems to treat the memo as classified, I'd really love to see whether it was, indeed, properly classified, or whether Yoo was just making stuff up again during a period when he is known to have secretly made stuff up.

In any case, given DOJ's continued efforts to either withdraw or disclose this memo, I'd safe it's safe to assume they're still using it.

FBI CLAIMED IT CONSULTED A MANUAL RATHER THAN CELLEBRITE DIRECTLY

Yesterday, I suggested that the initial docket pertaining to efforts to search Syed Rizwan Farook's Lexus and the work

phone found in it is consistent with FBI first asking Cellebrite (or some other outside party) to break into the phone before asking the court to use an All Writs Act to compel Apple to help.

In an article today in the wake of possibly incorrect reports the outside entity now helping FBI is Cellebrite, the NYT claims that FBI did try them.

> The F.B.I. has tried many ways to get into the iPhone used by Mr. Farook, such as exploiting a previous bug that allowed unsigned code to be loaded and run on the device, Stacey Perino, an electronics engineer with the F.B.I. has said in a court filing in the case.
>
> The F.B.I. also tried tools made by the agency and a mobile forensics company, Cellebrite, which let older iPhones load and run code that could crack a device passcode, Ms. Perino wrote. Cellebrite describes itself on its website as a subsidiary of Sun Corporation, a publicly traded Japanese company; it has done work for a number of government agencies.
>
> Yet none of those tools worked, Ms. Perino wrote in the court document that was filed March 10.

I think this misreads Perino's declaration, which in the section in question basically repeats what she found in the standard law enforcement tool UFED manual.

> Those previous tools that are available cannot be used on the Subject Device because they are

> not signed by Apple, and the current chain of trust on the Subject Device requires Apple to have signed any software that will be allowed to run
>
> [snip]
>
> From this open source research, several forensic tools were developed that combined (1) the boot ROM code signing defeat, and (2) brute-force passcode guessing. Examples include the Cellebrite UFED tool and an FBI-developed tool. Both the Cellebrite13 and FBI tools utilize the boot ROM exploit, allowing iPhone 3GS and iPhone 4 devices to load and boot an unsigned RAMdisk containing code to brute force the device passcode. The passcode recovery process operated from RAM, and did not alter the system or user data area
>
> [snip]
>
> Apple addressed the bug, and subsequently a jailbreak (i.e., allowing code unsigned by Apple) could only occur on an iPhone after it had been booted and unlocked.
>
> 13Cellebrite is a private company that makes forensic data recovery tools for mobile devices. While I have not examined the source code for the UFED tool, based on the Cellebrite Physical Extraction Manual for iPhone and iPad (Rev 1.3) and the fact that the Cellebrite tool no longer supports iPhone 4S and later devices, I believe the UFED

> tool relied on the same ROM exploit. The manual states: "The extraction application does not load iOS but instead loads a special forensic utility to the device. This utility is loaded to the device's memory (RAM) and runs directly from there." The utility is loaded from recovery mode.

It does not reveal that DOJ agencies continue to request Cellebrite's help on more sophisticated phones, nor that Cellebrite advertises the ability to crack iOS 8 phones (which is still an earlier operating system than Farook's phone runs).

Perino's passage is one that Apple's Erik Neuenschwander discussed, dismissively, at length.

> 21. Paragraphs 25 through 28 of the Perino Declaration describe supposedly already existing software that Mr. Perino suggests Apple use as a starting point to create GovtOS. For example, Mr. Perino points to a security exploit that supposedly allowed an iPhone to load a minimal operating system in RAM that had not been signed by Apple, which is what the government is requesting here. Similarly, Mr. Perino points to a hacking tool the FBI created that supposedly allowed it to brute force the device passcode on older iPhones.
>
> *22. These descriptions show that the FBI, along with its partners, currently have, and*

> *have had in the past, the capability to develop the types of code that Apple is being asked to create.*
>
> 23. Mr. Perino is incorrect, however, in his suggestion that Apple can use these third-party items, add Apple's signature, and load the finished product on to the subject device to accomplish the result that the government seeks with less effort than what I described in my initial declaration.
>
> 24. Using the allegedly already existing software code that Mr. Perino identifies would not be an appropriate way to accomplish what the government wants. Setting aside the legal question of whether Apple can incorporate a software tool created by some other party (such as the Cellebrite UFED tool Mr. Perino identifies) for this purpose, Apple would not save time and effort by incorporating unfamiliar third-party code that has never been used and deployed by Apple before, and it would introduce a host of new issues and potential risks that would need to be addressed. [my emphasis]

Of particular note, Neuenschwander noted that "FBI, along with its partners, currently have…the capability to develop the types of code that Apple is being asked to create." Cellebrite was the only partner listed by name.

Neuenschwander went on to note that the jailbreaking Perino described is precisely why Apple works so hard to

improve its security.

The NYT wants to claim FBI researched all possibilities before repeatedly claiming, more than 19 times (I did not include Perino's declaration in my count), that only the FBI or Apple could open this phone.

But Perino's declaration understates what Cellebrite itself claims to be able to do — and that DOJ asks Cellebrite to do.

That still doesn't mean Cellebrite is the entity now helping FBI crack the phone. It does mean FBI and DOJ engaged in affirmatively misleading briefing on whether Cellebrite might be able to do so.

THURSDAY MORNING: TWO TOO GOOD

I would post this video every week if I could get away with it. It's a favorite in my household where three of us play string instruments. I've blown out speakers cranking these guys up as far as I can (shhh…don't tell the dude in charge of speaker maintenance here).

You'll note this post is pushed down the page as Marcy's last two posts about #AppleVsFBI (here and here) have been picked up by several news outlets. Let's let new readers have the rail for a bit.

NC and GA state legislatures wreaking bigoted havoc

Regressive bills allowing open practice of anti-LGBT bigotry have been working their way through states' legislatures in the wake of *Burwell v. Hobby Lobby Stores, Inc.* Indiana and Arizona are two examples where bills using a template based on the federal Religious Freedom Restoration Act (RFRA) have been passed. Arizona's governor Jan Brewer made an unusually rational move and vetoed the bill. Indiana did not, and many organizations protested until an amendment was passed modifying SB 101's worst component.

Georgia's legislature passed their own spin on RFRA, The Free Exercise Protection Act; the bill is now in the hands of Gov. Nathan Deal, who has until the first week of May to sign it into law. The state has an emerging film and TV production industry, home to popular shows like AMC's The Walking Dead. Disney and its subsidiary Marvel yesterday announced they would yank production out of Georgia if Gov. Deal signed the bill. AMC followed suit and announced it too would pull out of Georgia. Other corporations with business interests in GA, like The Dow Chemical Company, are also unhappy. How many more companies will it take before Deal wises up and vetoes the bill or demands amendment?

Sadly, North Carolina's GOP-led legislature rushed through a bill yesterday with a slightly different spin – like a proof-of-concept for the rest of the states where RFRA bills have been unable to gain traction while avoiding the potential for boycotting leveraged against the governor. Anti-transgender fear-mongering was used to force HB2-Public Facilities Privacy & Security Act through while avoiding "religious freedom" as a promotional

feature. It was signed into law yesterday by NC's jackass governor, Pat McCrory, who tweeted,

> Ordinance defied common sense, allowing men to use women's bathroom/locker room for instance. That's why I signed bipartisan bill to stop it.
>
> I signed bipartisan legislation to stop the breach of basic privacy and etiquette, ensure privacy in bathrooms and locker rooms.

Except that HB2 not only overturns local ordinances protecting LGBT persons, it prevents transpersons from using the facilities appropriate to their transgender, and it allows businesses to post notices they will not serve groups. Welcome back, Jim Fucking Crow.

The bill was not truly bipartisan, either. Although 14 idiotic state house Democrats voted for the bill, the entire Democratic state senate caucus walked out in protest rather than vote on the bill at all. Methinks NC Dem Party discipline needs a little work, and state house members need a little less bigotry.

Speaking of which, DNC was typically ineffectual, offering a bunch of jargon instead of straight talk about NC's discrimination. Are there any groups at all the DNC under its current leadership will really extend any effort except for corporations?

The speed at which the bill passed through NC's legislature during an "emergency" session – because making sure the body parts align with the identity on the bathroom door is an

emergency! – may have prevented the state's largest employers from responding appropriately. Let's see if NC's largest employers, including University of North Carolina, Time Warner Cable, Duke Energy, Bank of America, Wells Fargo, Merrill Lynch, and the many sci-tech companies of Research Triangle, will wise up and demand an end to the ignorance and bigotry of Public Facilities Privacy & Security Act.

Finished digging out here after a late season snow storm, now serving up a hot dish brunch casserole made with a mess of oddments.

- Diebold buys German competitor Wincor Nixdorf (Bloomberg) – wonder how this industry shakes out as mobile payment systems become more popular and more widely accepted.
- Speaking of mobile payment systems: Apple Pay expected to expand to apps and websites before Christmas shopping season (FastCompany) – expected to take a bite out of PayPal's market share, but if transactions are conducted online, this could eat into other payment processing

systems. Need the importance of encryption be pointed out yet again, too?

- Apple’s new, smaller iPhone SE available for pre-orders today (BusinessInsider) – also iPad Pro. Already hearing strong interest from a lot of women about the smaller phone; they’ve been unhappy with the increasing size of iPhones.
- Nielsen TV ratings data will begin tracking streaming equipment brands (FastCompany) – their data will be based on 40,000 households, though. Apparently sales of streaming equipment like Apple TV, Chromecast, Roku aren’t granular enough for firms acquiring content consumption data. Wonder how long before Nielsen itself is replaced by network sniffing?
- Related? Funny how Iran is the focus of the first, but not

mentioned in the second:

- USDOJ charging Iranian hackers for alleged cyber attacks on banks and Wall street (Bloomberg); and
- U.S. military wants additional cybersecurity for nuclear and other WMDs (Bloomberg)

- AI-written novel survives first round in Japanese literature contest (DigitalTrends) – and you thought it was just the news that was generated by robots.

That's a wrap, catch you tomorrow morning!

DID FBI ASK CELLEBRITE TO OPEN FAROOK'S PHONE BEFORE

GETTING AN AWA ORDER?

In this post, I note that DOJ obtained a warrant to search (among other things) an iPhone 6 using Cellebrite's assistance on the same day as it obtained an All Writs Act order to Apple to help crack Syed Rizwan Farook's iPhone 5C. That other warrant demonstrates not only that DOJ was at least willing to *try* opening a late model iPhone with Cellebrite's help during the same period it was claiming it could only do so with Apple's help, but it also shows us what it would look like if DOJ tried to enlist Cellebrite's help.

I'd like to look at the underlying "warrant" such as it exists for this phone. There are two dockets in this case. 5:15-mj-00451, the docket under which DOJ got a search warrant for Farook's (actually, his mother's) Lexus. And 5:16-cm-00010, where the fight with Apple lives. The order for an All Writs Act actually lives in the earlier docket, with the first numerical docket item in the newer one is the government's motion to compel.

Technically, we have never seen any free-standing warrant for Farook's phone. Rather, what got attached to the AWA order application was actually the warrant for the Lexus. That warrant includes a bunch of boilerplate language about any devices found in the car, which basically permit authorities to search a device to find out if it contains any items covered by the search warrant, but requiring further legal order to keep that information.

> g. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of items to be seized, the government may retain forensic copies of the digital device but may not access them (after the time for searching the device has expired) absent further court order.

Obviously, FBI hasn't gotten to the point where they've found the phone includes evidence relating to the crime, because they haven't yet been able to search the phone, so they haven't gotten the point where they'd need this "further court order." Moreover, the phone doesn't belong to Farook, it belongs to San Bernardino County, and they've consented to any search (but you can't get an AWA unless you have a search warrant).

But it appears DOJ covered their asses, given the following entries in the original docket.

12/21/2015	5	Search and Seizure Warrant Returned Executed on 12/21/15 (Case terminated.) (ja) (Entered: 12/22/2015)
01/26/2016	6	GOVERNMENT'S EX PARTE APPLICATION for Order Sealing Document Filed by Plaintiff USA. (ad) (mrgo). (Entered: 01/27/2016)
01/26/2016	7	ORDER SEALING DOCUMENT by Magistrate Judge Sheri Pym. (ad) (mrgo). Modified on 2/25/2016 (ad). (Entered: 01/27/2016)
01/26/2016	8	GOVERNMENT'S EX PARTE APPLICATION for Order Unsealing Search and Seizure Warrant and Attachments A, A-2 and B Filed by Plaintiff USA. (ad) (mrgo). (Entered: 01/27/2016)
01/26/2016	9	ORDER UNSEALING Search and Seizure Warrant and Attachments A, A-2 and B ONLY by Magistrate Judge Sheri Pym. (ad) (mrgo). Modified on 2/25/2016 (ad). (Entered: 01/27/2016)
01/29/2016	10	EX PARTE APPLICATION for First Extension of Time Within Which to Retain and Search Digital Devices Filed by Plaintiff USA as to Defendant Black Lexus IS300 California License Plate 5KGD203, handicap placard 360466F, Vehicle Identification Number JTHBD192X50094434. (mrgo) (Entered: 02/02/2016)
01/29/2016	11	ORDER by Magistrate Judge Sheri Pym: granting 10 EX PARTE APPLICATION for Order as to Black Lexus IS300 California License Plate 5KGD203, handicap placard 360466F, Vehicle Identification Number JTHBD192X50094434 (1). (mrgo) (Entered: 02/02/2016)
01/29/2016	12	EX PARTE APPLICATION FOR ORDER SEALING DOCUMENTS as to Defendant Black Lexus IS300 California License Plate 5KGD203, handicap placard 360466 Vehicle Identification Number JTHBD192X50094434, Filed by Plaintiff USA as to Defendant Black Lexus IS300 California License Plate 5KGD203, handicap placard 360466F, Vehicle Identification Number JTHBD192X50094434. (mrgo) (Entered: 02/02/2016)
01/29/2016	13	ORDER by Magistrate Judge Sheri Pym: granting 12 EX PARTE APPLICATION to Seal Document as to Black Lexus IS300 California License Plate 5KGD203, handicap placard 360466F, Vehicle Identification Number JTHBD192X50094434 (1). (mrgo) (Entered: 02/02/2016)
02/02/2016	14	GOVERNMENT'S EX PARTE APPLICATION FOR ORDER SEALING DOCUMENT Filed. (ad) (Entered: 02/04/2016)
02/02/2016	15	ORDER SEALING DOCUMENT by Magistrate Judge David T. Bristow. (ad) (Entered: 02/04/2016)
02/02/2016	16	GOVERNMENT'S AMENDED EX PARTE APPLICATION FOR ORDER UNSEALING THIS MATTER, Specifically the Search Warrant and Attachments, All Else Remain Under Seal Filed. (ad) (Entered: 02/04/2016)
02/02/2016	17	ORDER UNSEALING THIS MATTER, SPECIFICALLY THE SEARCH WARRANT AND ATTACHMENTS, ALL ELSE TO REMAIN UNDER SEAL by Magistra Judge David T. Bristow. (ad) (Entered: 02/04/2016)

As I understand it, this warrant docket was terminated on December 21. But then on January 26, it got active again, with the government sealing a document, then unsealing the parts of the search warrant. Then, on January 29, the government applied for and got and then sealed an extension of time on the original warrant, but noting they just needed an extension for devices related to it (that is, for Farook's phone). Then on February 2, they submitted and got sealed another document. Finally, they got parts of the original warrant that had been unsealed in part days earlier unsealed (again?) so they could get the AWA, which they did.

I'm interested in all this for several reasons. First, if they closed this docket in December, *after they had already obtained the content of Farook's iMessage account*, does that indicate they had determined the phone had no evidence relating to the crime? That's consistent with what everyone believes. But it would also seriously undermine their claims that they do need the information (especially since the claims they made in their AWA application are inconsistent with that they've claimed in later documents).

I also suspect that FBI asked Cellebrite to open this phone. If I'm reading the docket correctly, the parts of the search warrant pertaining to the phone have been unsealed twice, the latter time for the AWA. I suspect the earlier activity in the docket pertained to a Cellebrite request, in which case the February 2 docket document might resemble the method of search language, naming Cellebrite, found in the February 16 warrant for the iPhone 6 in the other case.

The thing is, Judge Pym may know that, if that's the case, because she's the one who signed off on the January 26 and 29 activity. Which is interesting given that, in the phone hearing on whether to vacate the hearing yesterday, she suggested FBI might need to brief on what this effort was.

> I'm not — to some extent I'm not sure how much difference it makes whether the order is vacated at this point or not, because if it turns out, after exploring this possibility, that the FBI believes it won't work, you know, I would be inclined to go forward without

> really — and there might need to be some additional briefing, supplemental submissions, with respect to this effort, but I think the matter's been fully briefed.

She may be less willing to decide for FBI if she knows that Cellebrite is actively working on a solution that would solve FBI's needs, which she may already know.

In any case, given the import of this case, citizens really deserve to know what the government was asking for at the end of January, particularly if their first effort to get into the phone involved a request to Cellebrite that has now been answered.

ON FEBRUARY 16, DOJ GOT A WARRANT TO OPEN AN IPHONE 6 USING CELLEBRITE

As a number of outlets are reporting, the Israeli security firm Cellebrite is the source the FBI is using to attempt to break into Syed Rizwan Farook's phone.

> Israel's Cellebrite, a provider of mobile forensic software, is helping the U.S. Federal Bureau of Investigation's attempt to unlock an iPhone used by one of the San Bernardino, California

> shooters, the*Yedioth Ahronoth* newspaper reported on Wednesday.
>
> If Cellebrite succeeds, then the FBI will no longer need the help of Apple Inc, the Israeli daily said, citing unnamed industry sources.
>
> Cellebrite officials declined to comment on the matter.

According to the narrative the government is currently telling, it means 33 days after DOJ obtained an All Writs Act on February 16 ordering Apple to help unlock Farook's phone, and 108 days after FBI first seized the phone on December 3 — during which entire period the FBI *now* claims they were diligently researching how to crack the phone — on March 20, Cellebrite contacted the FBI out of the blue and told them they can help.

That's interesting, especially given this search warrant, approved (as coinkydink would have it) on February 16, the very same day DOJ got its AWA in California.

Among the phones DEA obtained a warrant to search was an iPhone 6, a later model than Farook's phone with default encryption (though running unknown iOS). Here's what DEA Task Force Officer Shane Lettau had to say about how he (might) access the contents of this iPhone 6.

Apple iPhone, Model A1549, bearing IMEI: 359296065756836, FCC ID# BCG-E2816A; (A photograph of the cellular phone appears in Attachment A2). The device will be charged and powered on. The device and all readable and searchable contents will be attempted to be downloaded to a "CellBrite" device. The "CellBrite" device allows the user to bypass any password protected utility on the phone. The contents downloaded on the CellBrite device will then be copied to a readable computer disc and reviewed by your affiant. However, your affiant knows through experience that Apple devices hold a unique encryption that typically only Apple Inc. can bypass. Therefore, it is possible that your affiant may have to send the SED to Apple Inc. located in California for the search. A search warrant return will be provided to the Court thereafter.

To be sure, these phones aren't the same, nor is the agency. Farook's is a 5C running iOS 9, this is a 6, and we don't know what iOS it is running. But if Cellebrite can break into a 6 they presumably can break into a 5C. FBI is seeking access in CA, whereas this MD phone is in DEA's possession.

The point is, however, that it is inconceivable to claim, as DOJ did 19 times, that the only way they could get into Farook's phone was with Apple's help when DOJ was at the same time participating in DEA's discussions with Cellebrite about whether they could crack a later model phone. It may be that Cellebrite only perfected their technique with iOS 8 and later model phones in recent weeks, or that they could not crack an iOS 9 in December or February but have since perfected that, but DOJ still shouldn't have been submitting sworn declarations pretending that Cellebrite was not a possible option.

Update: I originally said Farook's phone was a 5S. I've corrected the post to say it is a 5C, h/t JC.

Update: FBI signed a contract with Cellebrite on the same day it announced it had found a solution, though I think it's for license renewals for 7 machines in Cook County.

WEDNESDAY MORNING: WICKED WEARY WORLD

Let’s have a brunch-time salute to Belgium, which produced this fine young artist Loic Nottet. Too bad there’s not much well-produced content in YouTube yet by this youngster. He has incredible upper range reach with great potential because of the power behind his voice. Hope to hear more by him soon; he’s a sweet antidote to bitter wickedness.

All in the family
Hope you’ve read Marcy’s piece already this morning on the relevance of nuclear family units to terrorism. In addition to suicide bombers El Bakraoui brothers Marcy mentioned, it’s worth examining the other links between the November 13 attacks in Paris and the attacks in Belgium yesterday. Note the familial relationships and their first-degree network:

Brahim Abdelslam – older brother of Salah, blew himself up in Paris during the November 15 attacks. (Dead)
Salah Abdelslam – captured last Friday March 18, has admitted he ‘had planned to target Brussels.’ His location was flagged by an unusual number of pizzas delivered to an apartment where power and water had been shut off. (In custody)

Abaid Aberkan – characterized as a relation of the Abdelslams, carried Brahim’s casket at the funeral last week. (~~NOT a terror suspect~~ *Edit: Le*

Monde indicates Aberkan was arrested during Friday's raid, but name spelled 'Abid.') (In custody)
Aberkan's mother – renter/owner of Molenbeek apartment in which Salah was hiding when captured last week. (NOT a terror suspect)

Mohamed Belkaid – killed in a raid last Tuesday at an apartment in Forest district; Salah fled the apartment. (Dead)

Mohamed Abrini – A childhood friend and neighbor of Salah, his younger brother Suleymane died fighting in an Islamist militia under the direction of Abdelhamid Abaaoud. Abaaoud, the leader of the Paris attacks, died on November 18 during a police raid. Abrini had traveled with both of the Abdelslam brothers the week before the attacks in Paris. He is now on the run and sought in relation to yesterday's attack. (Suspect)

Najim Laachraoui – traveled with Salah and Belkaid last September, under the name Soufiane Kayal. His DNA was found in three different locations: on explosives in Paris, and at two other hide-outs used by attackers. He is now sought in relation to yesterday's attack. (Suspect)

Though we'll hear arguments for increased internet surveillance, it's easy to see that traditional police work could identify a terrorist network of family and friends in the same way members of an organized crime syndicate centered around a family are revealed. (Sources for the above: The Guardian and The Australian)

Other stuff going on…

- 'Flash Crash' trader

to be extradited to the U.S., rule British judges (France24)

- Sextortionist Michael Ford, who ran a criminal enterprise from his work computer while employed at U.S. embassy, sentenced to four years and nine months in prison (Ars Technica) — BoingBoing notes the hypocrisy of a government demanding backdoors while failing to note such a massive misuse of its own network.
- Another hospital held hostage by ransomware, this time in Kentucky (Krebs on Security) — STOP OPENING LINKS IN EMAIL at work, for starters. Isolating email systems from all other networked operations would be better.
- 24 car models by 19 automakers vulnerable to keyless entry hack (WIRED—mind the ad-block hate) — Mostly foreign models affected due to the radio frequency used.

Better luck tomorrow, gang. See you in the morning.

HOW TO PROTECT AGAINST TERRORISM: ELIMINATE THE VALUABLE TERRORIST TECHNOLOGY, THE NUCLEAR FAMILY

In addition to catching the third Brussels airport bomber,~~Najim Laachraoui,~~ ~~a known Salah Abdelslam associate,~~ authorities in Europe have also revealed that the other two airport bombers were brothers, Khalid and Ibrahim El Bakraoui.

> Police sources earlier told NBC News that Khalid El Bakraoui, 27, and 30-year-old sibling Ibrahim blew themselves up. Both had been convicted of violent crimes in the past and had links to one of the Paris attackers.

The El Bakraouis join an increasingly long list of recent terrorists who partner within their nuclear family (the Boston Marathon attack, Charlie Hebdo attack, and Paris attack were all carried out by brothers, and the San

Bernardino attack was carried out by spouses). As New America noted in November (that is before several more family launched attacks), 30% of the fighters they've identified had family ties to jihad.

> One-third of Western fighters have a familial connection to jihad, whether through relatives currently fighting in Syria or Iraq, marriage, or some other link to jihadists from prior conflicts or attacks. Of those with a familial link, almost two-thirds have a relative fighting in this conflict and almost one-third are connected through marriage, many of them new marriages conducted after arriving in Syria.

There has been less attention (though there has been some) about the operational advantages organizing attacks among family members offers. Not only would there be far more face-to-face conversations in any case (which you'd need a physical bug to collect), but even electronic communications metadata might not attract any attention, except insofar as helping to geolocate the parties. It'd be hard to distinguish, from metadata, between brothers or spouses discussing taking care of their kids from the same family members plotting to blow something up.

Family ties then, along with a reportedly difficult Moroccan dialect, may function to provide as much security as any (limited, given the reports) use of encryption. And all that's on top of the cell's extensive use of burner phones.

Using Jim Comey, um, logic, we might consider eliminating this threat by eliminating the nuclear family. Sure, the overwhelming majority of people who use it are law-abiding people obtaining valuable benefit from nuclear family. Sure, for the most vulnerable, family ties provide the most valuable kind of support to keep someone healthy. But bad guys exploit it too, and we can't have that.

I mean, perhaps there should be an honest public discussion about the proportional value the nuclear family gives to terrorists and to others. But why would we have that discussion for the nuclear family and not for encryption?

Update: as soon as I posted this I saw notice that Belgian press (and with them NBC, apparently) got the identity of the third hijacker wrong, so I've crossed out and/or taken out those references.