M^{3}AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

– Social Media Posting Allowed –

Tweeter, Facebook, LinkedIn, other social media posts are welcomed in this session if you:

- Only post comments made by the speakers or panelists
- Do not post comments or questions from the audience (but you can share the speakers' responses to questions)
- Do not post the name, position or company of other meeting attendees
- Do not post conversations with attendees
- M^{3}AAWG is not a deliverability conference; we are
  - An industry working group meeting
  - An anti-abuse conference, or
  - A gathering of security experts
- All of the M^{3}AAWG Membership, Trademarks and Logo guidelines apply (https://www.m3aawg.org/members/how-promote-m3aawg#TrademarkGuidelines)

Anti-Pervasive Monitoring Threat Models

Joe St Sauver, Ph.D. (stsauver@fsi.io or joe@stsauver.com)
M3AAWG Senior Technical Advisor and
Scientist, Farsight Security, Inc.

M3AAWG 37, Philadelphia PA
Thursday, June 16, 11:00-12:00

https://www.stsauver.com/joe/maawg-37-threat-models/

I. Beginning With Some Backfill:

The Origin of M^{3}AAWG's Anti-Pervasive Monitoring Work: Snowden's 2013 And Later Disclosures

Backfill For Those "Joining In Progress"

- M3AAWG's Anti-Pervasive Monitoring Work may be well known to some, perhaps many, of you. You know what we're doing, and why, and what's happened to-date.

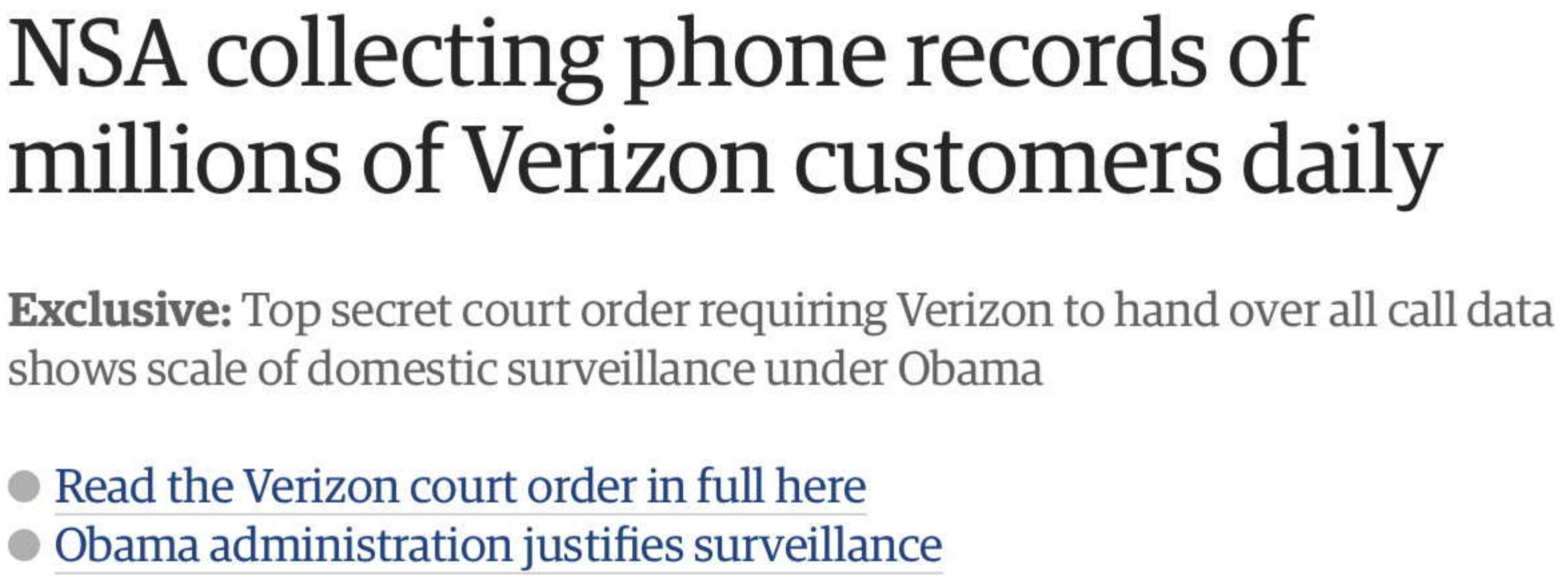
- For others of you, however, this may be your first M3AAWG, or you might not have attended previous anti-Pervasive Monitoring SIG-related sessions. Therefore, we're going to begin by providing some backfill for those who may not be "up to speed."

- In the time we have available, we can't cover "everything," but we can at least go over some highlights and provide pointers for those who may want to engage in self-directed "homework."

M^{3}AAWG 28 Was Being Held In Vienna, Austria, When The First Snowden Article Was Published

https://commons.wikimedia.org/wiki/File:Hotel_Hilton_Vienna_August_2006_001.jpg
https://commons.wikimedia.org/wiki/File:Au-map.png

Remember This Headline? I Surely Do...



NSA collecting phone records of millions of Verizon customers daily

Exclusive: Top secret court order requiring Verizon to hand over all call data shows scale of domestic surveillance under Obama

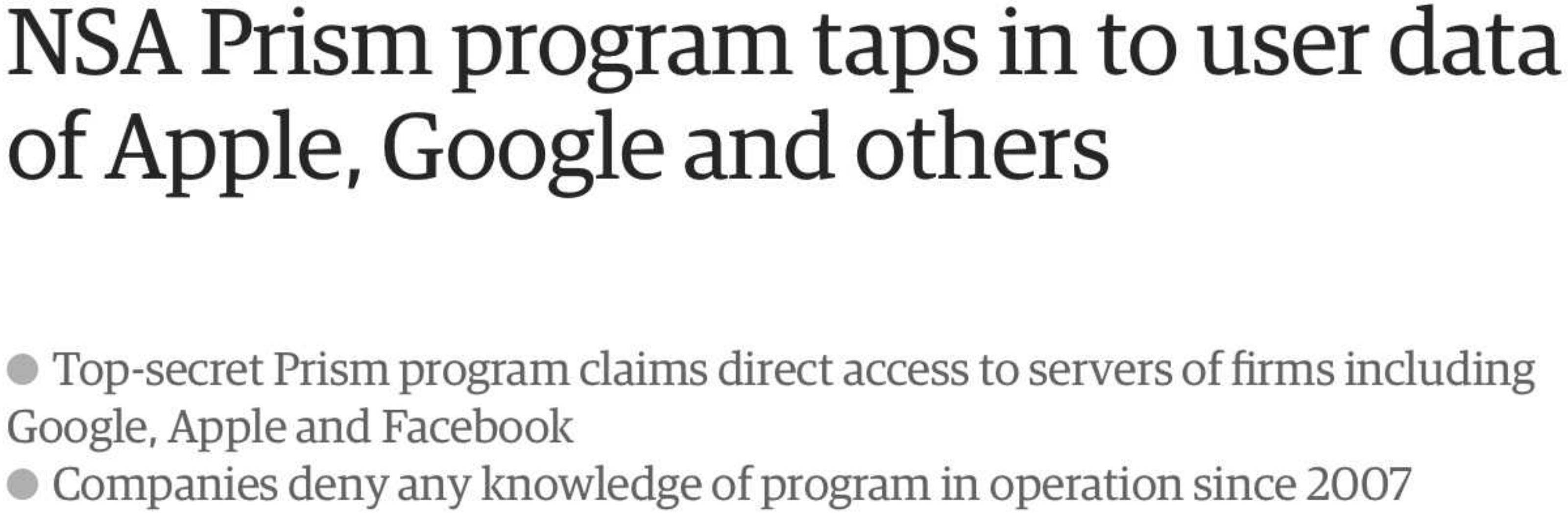
- Read the Verizon court order in full here
- Obama administration justifies surveillance

www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order [notwithstanding the URL, this article was actually published on the 5th of June, see http://www.theguardian.com/world/2013/jun/23/edward-snowden-nsa-files-timeline]

Reactions

- Many were angry, shocked, and dismayed over what was reported by *The Guardian* and other news outlets.
- ***Online pervasive monitoring of domestic customer metadata?*** What about Constitutional protections against unreasonable search and seizure? What about Americans' right to privacy?
- This pervasive monitoring was even viewed by some in the community as a ***personal affront.***
  - It takes a lot of effort to build and run complex Internet-scale systems. Technical people tend to throw themselves into their work and take great pride in how they build and operate their networks and systems, including the security and privacy thereof.
  - Having that undercut by the U.S. intelligence community felt **insulting, dismissive, and violative.**
- Many also worried that Snowden's disclosures would cause a **loss of customer confidence** and **be commercially damaging**.

Another Shoe Drops



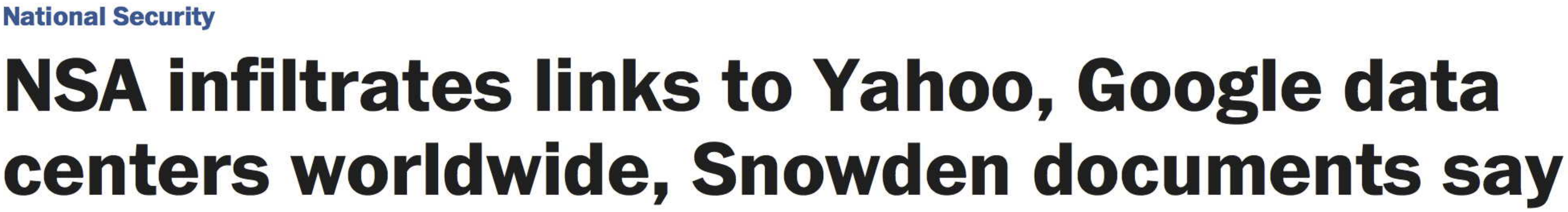
NSA Prism program taps in to user data of Apple, Google and others

- Top-secret Prism program claims direct access to servers of firms including Google, Apple and Facebook
- Companies deny any knowledge of program in operation since 2007

Source: http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

- The first Snowden revelation was about the bulk collection of domestic **metadata.** While metadata can be hugely revealing, most average users have little idea of just *how* revealing it can be. Eavesdropping on **full message contents,** on the other hand, (Snowden's 2nd revelation, as shown here) is the troubling sort of behavior that even non-technical users can readily "get."

A Third Release (They Just Kept Coming!), The Week After M^{3}AAWG 29 In Montreal, Oct 21st-24th



National Security

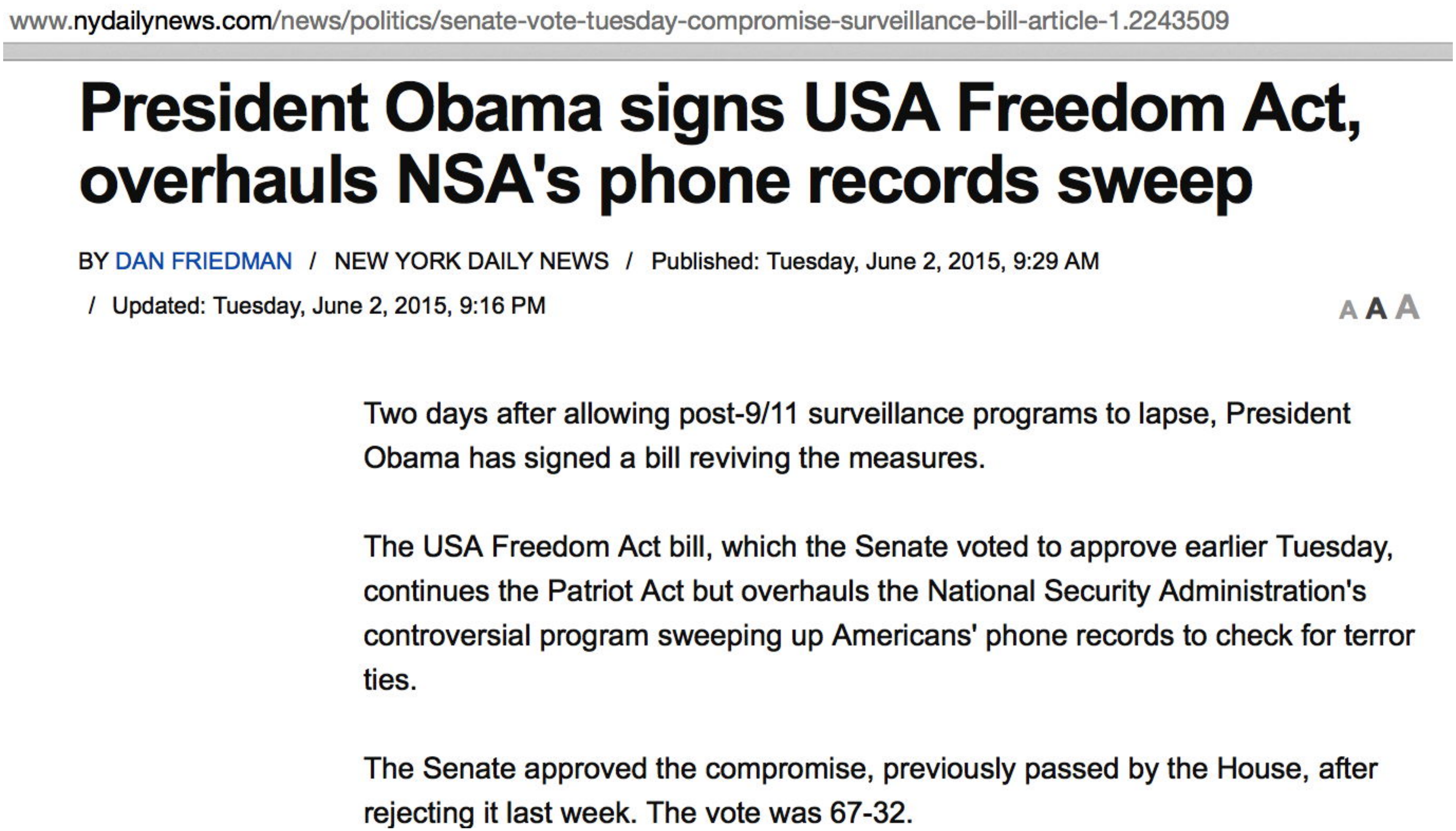
NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say

Source: Washington Post, October 30th, 2013.

II. 'But Joe! That Was Years Ago. Pervasive Monitoring In The US Has Been "Reformed"... Hasn't It?'

(AKA, Do We *REALLY* Have To Keep Fighting This Fight?)

Well, There Was/Is The USA Freedom Act...



www.nydailynews.com/news/politics/senate-vote-tuesday-compromise-surveillance-bill-article-1.2243509

President Obama signs USA Freedom Act, overhauls NSA's phone records sweep

BY DAN FRIEDMAN / NEW YORK DAILY NEWS / Published: Tuesday, June 2, 2015, 9:29 AM / Updated: Tuesday, June 2, 2015, 9:16 PM

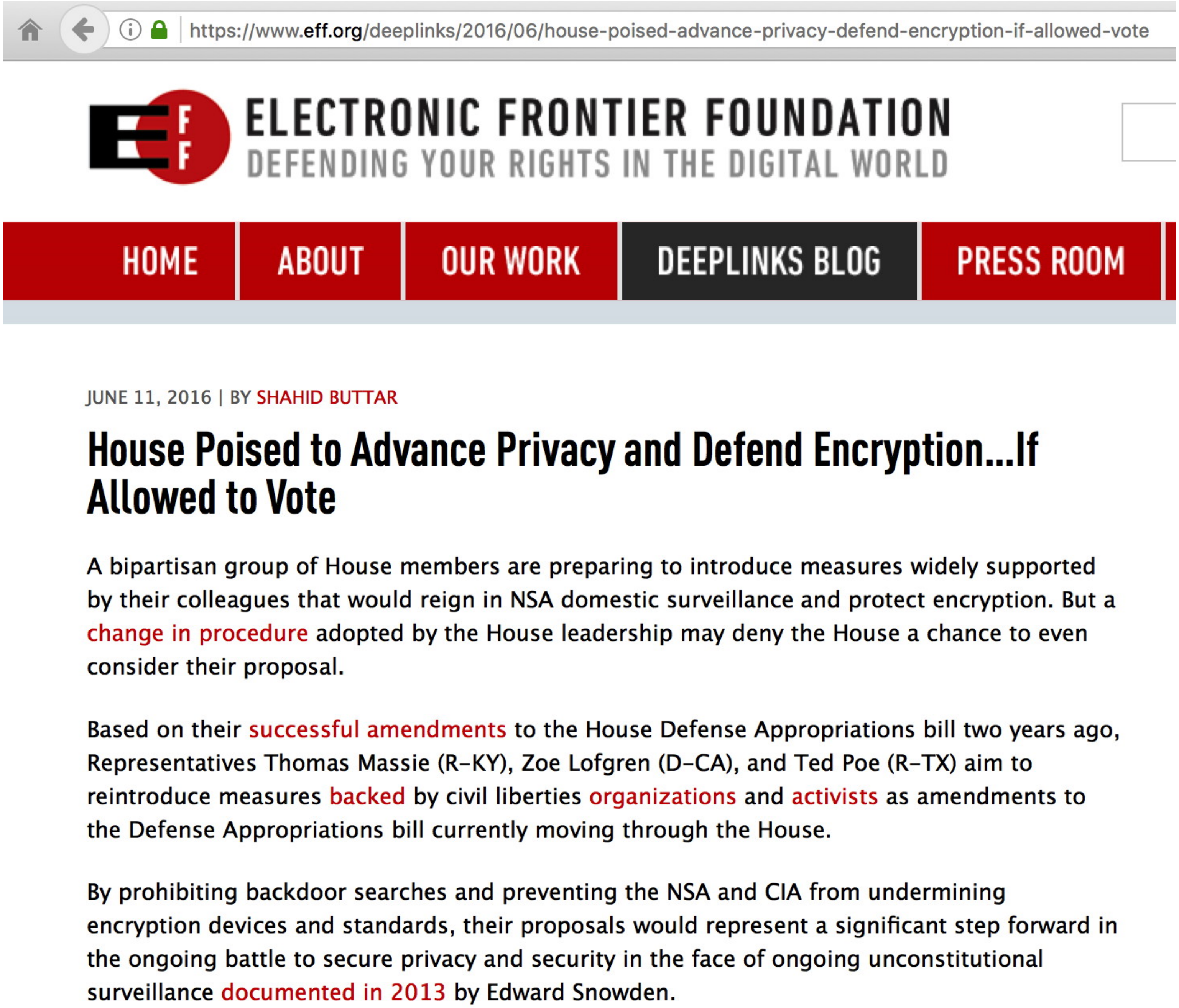
Two days after allowing post-9/11 surveillance programs to lapse, President Obama has signed a bill reviving the measures.

The USA Freedom Act bill, which the Senate voted to approve earlier Tuesday, continues the Patriot Act but overhauls the National Security Administration's controversial program sweeping up Americans' phone records to check for terror ties.

The Senate approved the compromise, previously passed by the House, after rejecting it last week. The vote was 67-32.

That Act Was/Is A Step In The Right Direction

- It took time and effort from many people, but eventually many in Washington DC came to see that dragnet-style warrantless bulk surveillance of its own citizens just wasn't the answer.
- Many of the people in **this room** may have ended up having to assume new responsibilities given the way government surveillance powers have been refactored (with metadata-keeping obligations transferred to service providers).
- M3AAWG should continue to pay close attention to the requirements of the USA Freedom Act and how they may impact ISP member companies.
- **Additional reforms are still under discussion, see for example the proposed reforms that the EFF is currently supporting...**



https://www.eff.org/deeplinks/2016/06/house-poised-advance-privacy-defend-encryption-if-allowed-vote
EFF
ELECTRONIC FRONTIER FOUNDATION
DEFENDING YOUR RIGHTS IN THE DIGITAL WORLD
HOME
ABOUT
OUR WORK
DEEPLINKS BLOG
PRESS ROOM

JUNE 11, 2016 | BY SHAHID BUTTAR

House Poised to Advance Privacy and Defend Encryption...If Allowed to Vote

A bipartisan group of House members are preparing to introduce measures widely supported by their colleagues that would reign in NSA domestic surveillance and protect encryption. But a change in procedure adopted by the House leadership may deny the House a chance to even consider their proposal.

Based on their successful amendments to the House Defense Appropriations bill two years ago, Representatives Thomas Massie (R-KY), Zoe Lofgren (D-CA), and Ted Poe (R-TX) aim to reintroduce measures backed by civil liberties organizations and activists as amendments to the Defense Appropriations bill currently moving through the House.

By prohibiting backdoor searches and preventing the NSA and CIA from undermining encryption devices and standards, their proposals would represent a significant step forward in the ongoing battle to secure privacy and security in the face of ongoing unconstitutional surveillance documented in 2013 by Edward Snowden.

Attempts to Re-establish Or Even Expand Domestic Intelligence Collection Are ALSO Taking Place

- At the same time civil liberties organizations are pressing for more controls over domestic intelligence collection, the Intelligence Community is making a determined play to backfill the domestic intelligence they feel they need.

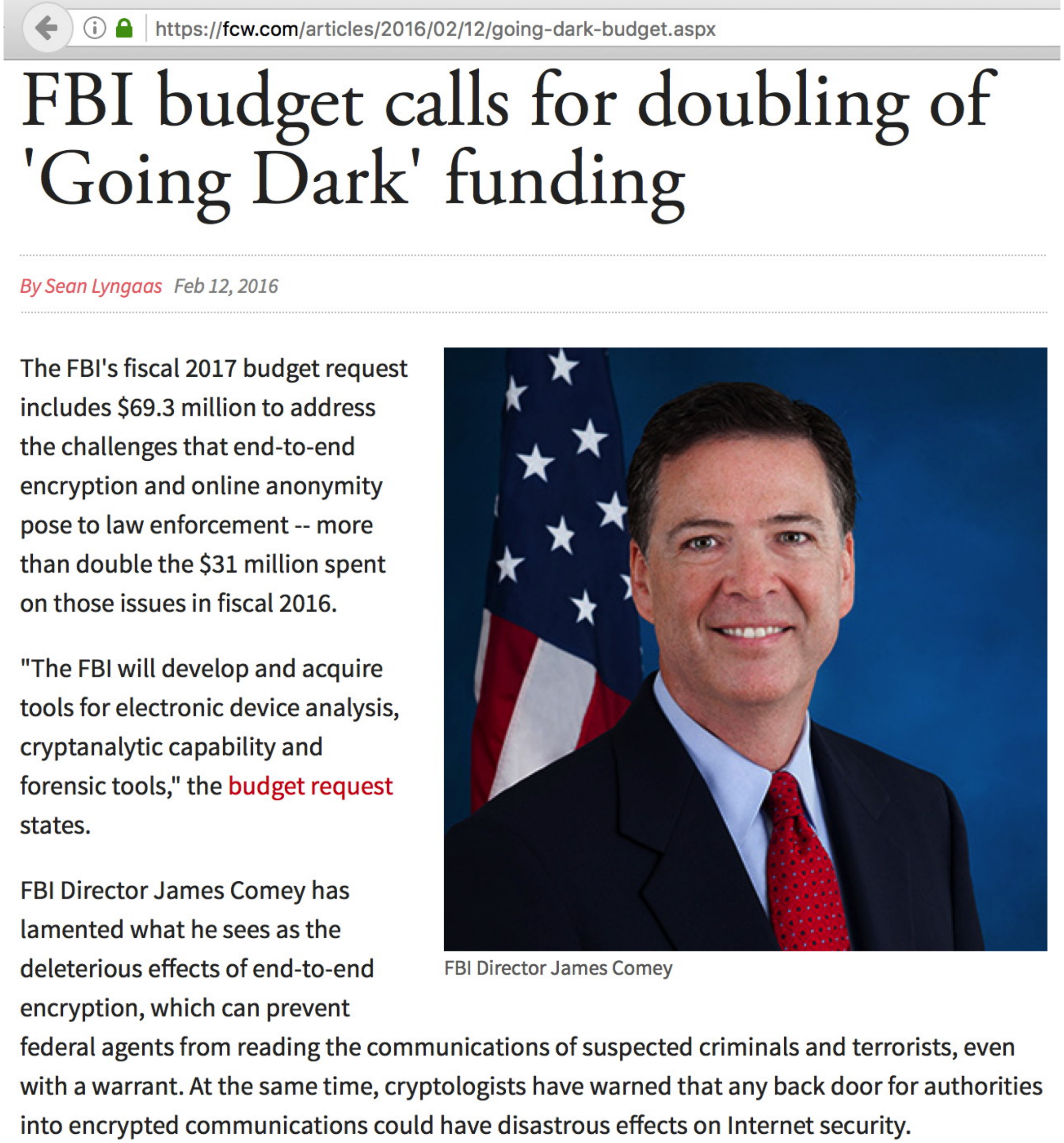
- You can see this play out in the headlines. For example, the FBI is currently actively working to get easier statutory access to records relating to Americans' activities online -- at the same time we see reports that it may be failing to fully adhere to statutory/court-ordered minimization procedures.

- The FBI is also seeking more funding to tackle encryption challenges.

Example: "Secret Text in Senate Bill Would Give FBI Warrantless Access to Email Records"

- As reported at https://theintercept.com/2016/05/26/secret-text-in-senate-bill-would-give-fbi-warrantless-access-to-email-records/ [emphasis added below]

- 'A provision snuck into the still-secret text of the Senate's annual intelligence authorization would **give the FBI the ability to demand individuals' email data and possibly web-surfing history from their service providers without a warrant and in complete secrecy.**
- 'If passed, the change would expand the reach of the FBI's already highly controversial **national security letters.** The FBI is currently allowed to get certain types of information with NSLs -- most commonly, information about the name, address, and call data associated with a phone number or details about a bank account.
- 'Since a 2008 Justice Department legal opinion, the FBI has not been allowed to use NSLs to demand "electronic communication transactional records," such as email subject lines and other metadata, or URLs visited.



https://fcw.com/articles/2016/02/12/going-dark-budget.aspx

FBI budget calls for doubling of 'Going Dark' funding

By Sean Lyngaas Feb 12, 2016

The FBI's fiscal 2017 budget request includes $69.3 million to address the challenges that end-to-end encryption and online anonymity pose to law enforcement -- more than double the $31 million spent on those issues in fiscal 2016.

"The FBI will develop and acquire tools for electronic device analysis, cryptanalytic capability and forensic tools," the budget request states.

FBI Director James Comey

FBI Director James Comey has lamented what he sees as the deleterious effects of end-to-end encryption, which can prevent federal agents from reading the communications of suspected criminals and terrorists, even with a warrant. At the same time, cryptologists have warned that any back door for authorities into encrypted communications could have disastrous effects on Internet security.

But "Court Troubled by Surveillance Excesses at FBI, NSA"

- "Court troubled by surveillance excesses at FBI, NSA", http://www.politico.com/blogs/under-the-radar/2016/04/government-surveillance-fbi-nsa-violations-222162

  > "The court was extremely concerned about NSA's failure to comply with its minimization procedures—and potentially" a provision in federal law, Hogan wrote. The NSA violations appeared to involve preserving surveillance data in its systems beyond the two or five years after which it was supposed to be deleted.

- "Secret spy court scolded NSA, FBI for not deleting data", http://thehill.com/policy/national-security/276904-secret-spy-court-scolded-nsa-fbi-for-not-deleting-data

  > “Perhaps more disturbing and disappointing than the NSA’s failure to purge this information for more than four years, was the government’s failure to convey to the court explicitly during that time that the NSA was continuing to retain this information,” [Judge Hogan] wrote.

- See https://www.dni.gov/files/documents/20151106-702Mem_Opinion_Order_for_Public_Release.pdf

Other Sweeping Cyber Evidence-Related Rulings Are Also Emerging

- **"All your disk image are belong to us, says appeals court",** http://arstechnica.com/tech-policy/2016/05/feds-can-keep-your-hard-drives-indefinitely-and-search-them-too/

  The government can prosecute and imprison people for crimes based on evidence obtained from their computers -- even evidence retained for years that was outside the scope of an original probable-cause search warrant, a US federal appeals court has said in a 100-page opinion paired with a blistering dissent.

- Not clear on the issue? Later in the article, Judge Denny Chin's 40 page dissent is quoted in part:

  "The government did precisely what the Fourth Amendment forbids: it entered Ganias' premises with a warrant to seize certain papers and indiscriminately seized -- and retained -- all papers instead."

"Appeals Court Delivers Devastating Blow to Cellphone-Privacy Advocates"

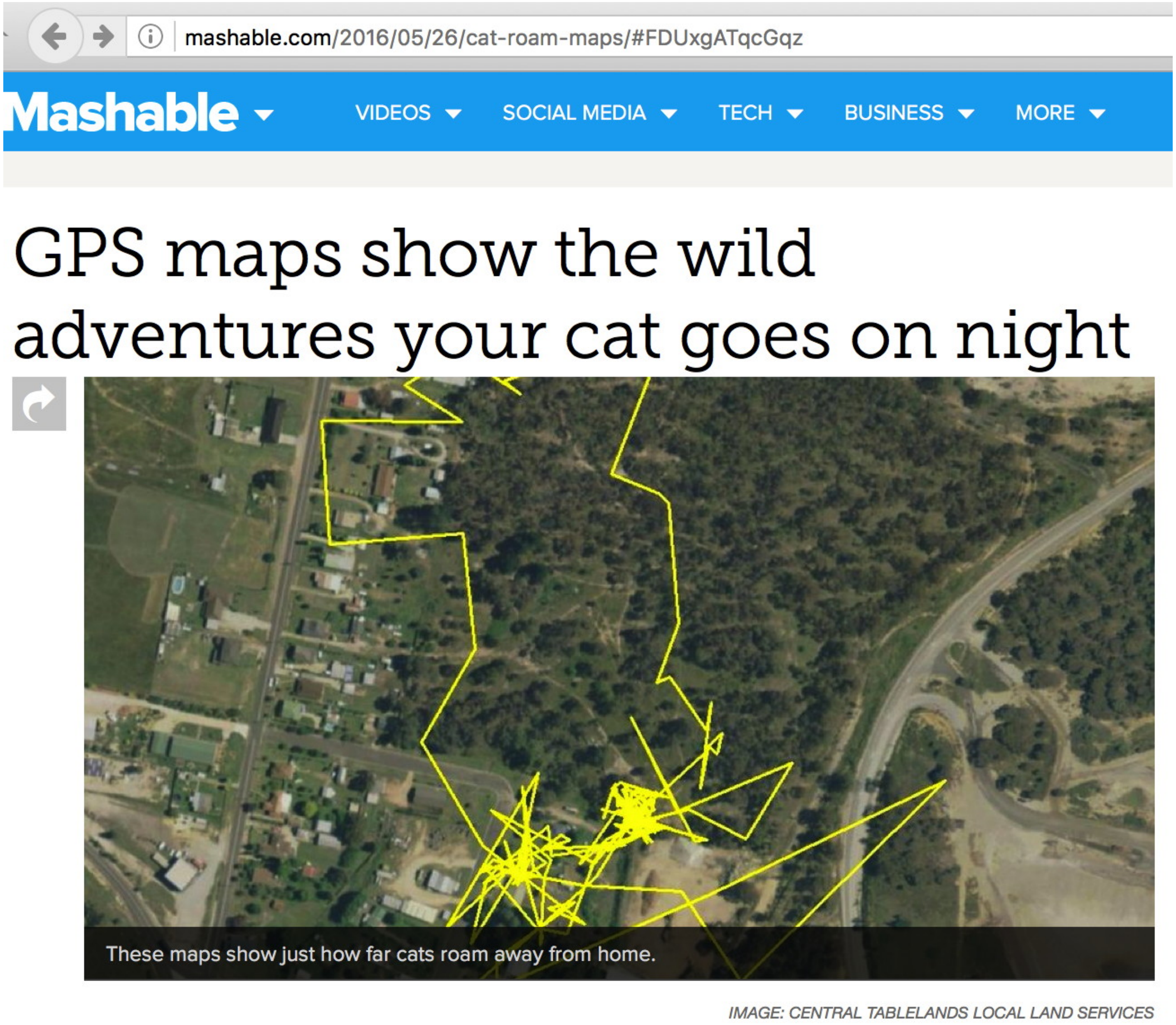
- https://theintercept.com/2016/05/31/appeals-court-delivers-devastating-blow-to-cell-phone-privacy-advocates/

- **Short form: appellate court judges in Richmond found that a warrant is not required for cell phone "location data" due to the "third party" doctrine.**

- Wow. This strips away a huge amount of consumer privacy, assuming you use and carry a cell phone, as virtually everyone does these days.

- The government can potentially track your movements, without a warrant, just like you might track a pet's movements.

Track People (Just Like Tracking Pets), No Warrant



GPS maps show the wild adventures your cat goes on night

These maps show just how far cats roam away from home.

IMAGE: CENTRAL TABLELANDS LOCAL LAND SERVICES

The Use of Clandestine Digital Investigative Techniques Has Caused Some Serious Criminal Cases To Self-Destruct

- **"Judge tosses evidence in FBI Tor hacking child abuse case",** https://nakedsecurity.sophos.com/2016/05/27/judge-tosses-evidence-in-fbi-tor-hacking-child-abuse-case/
- The defense asked for details about how the government intercepted their client's Tor traffic, apparently recognizing that the FBI would be reluctant to disclose their investigative technique **(protection of "sources and methods" tend to trump any individual prosecution).**
- Therefore, asking for that information has the potential to be a bit of a "poison pill" that would potentially kill an entire line of critical evidence.
- In fact, the FBI did decline to supply the requested information, unwilling to "burn" their confidential technology by disclosing it in court.
- **The result? The court proceeded to exclude all evidence resulting from the use of the undisclosed technique, which is really a shame if it means an alleged major offender in a crimes against children case may go unpunished.**
- The problem also appears to go beyond just Michaud's case, see the article.
- **It is risky to try to use confidential collection methods to gather information in criminal investigations.**

III. Other Countries Are Snooping Online, Too. This ***Isn't*** Just a US Thing.

That Means That Even If The US Intelligence Community Gets And Stays "Reigned-In," A Need For Vigilance And Technical Protections Remains

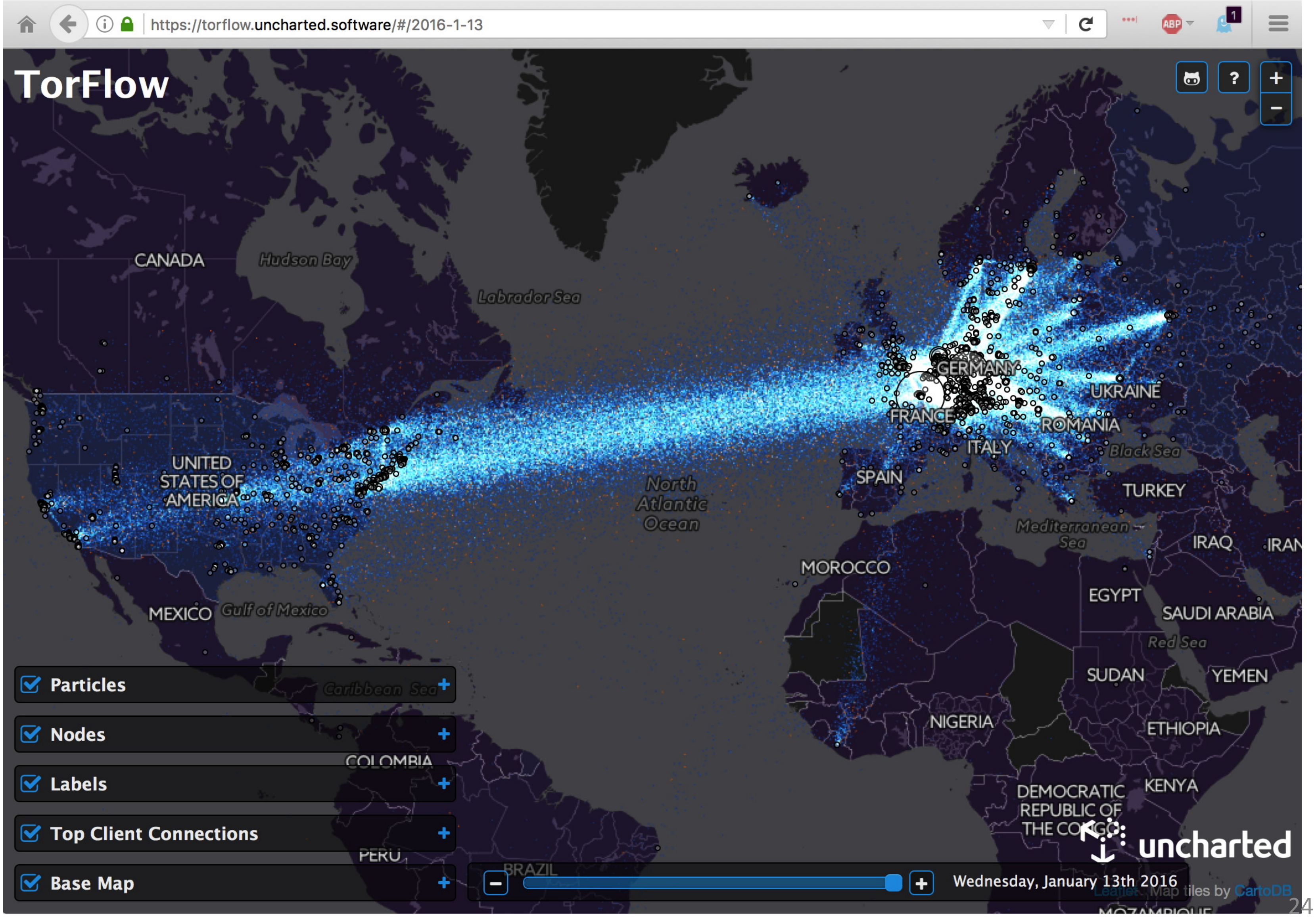
Why Worry About Foreign 'NSA-like' Outfits?

- Online pervasive monitoring takes place both by **western intelligence services** (such as the US's NSA, the UK's GCHQ, Canada's Communications Security Establishment, and other services), as well as by countries not aligned with the west. **Name a major country, it likely has the national equivalent of the US's NSA.** (Excellent bar trivia topic, BTW)

- This is important to "get" if **you travel abroad**, or **simply use the Internet, given that sites may be located anywhere worldwide.**

- You should also know that **online privacy tools (such as Tor)** are largely a **US/European thing**, and hence, if you travel and use Tor in <u>other</u> regions (such as in the Asia-Pacific region, or in the Southern Hemisphere), your traffic may tend to "stand out..."

Tor Traffic Flows: US? Check. Europe? Check. Asia? Southern Hemisphere? Umm, Not So Much…



U.K. Commons Passes Controversial "Snooper's Charter" Bill

- http://www.bloomberg.com/news/articles/2016-06-08/u-k-commons-passes-controversial-snooper-s-charter-bill (8 Jun 2016)

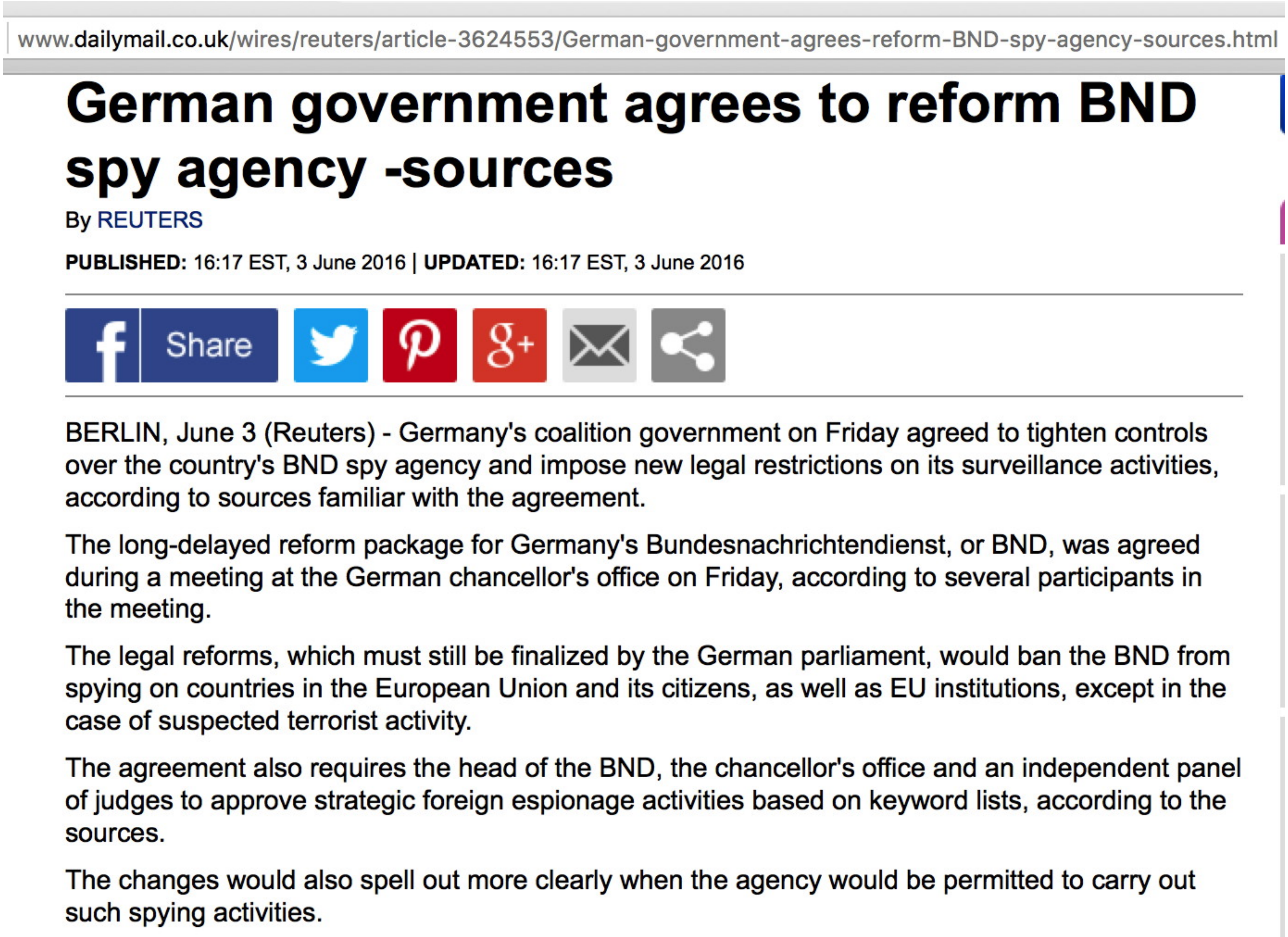
  "The U.K. House of Commons on Tuesday passed a controversial bill giving spy agencies the power to engage in bulk surveillance and computer hacking. * * * The House of Lords will now consider the proposed law, known as the Investigatory Powers Bill. The legislation, which some critics have branded a snooper's charter, will also be analyzed by a panel of legal experts chaired by David Anderson QC, the U.K.'s independent reviewer of terrorism legislation. Anderson will issue a report on the bill -- including an opinion on whether the bulk surveillance powers the government is asking for are justified -- in time for the Lords final vote on the bill sometime in the fall. If it passes, the law will go into effect in January 2017."

France and Online Intelligence Collection

- "**The French government has voted in favor of greater powers of surveillance, giving it intelligence-gathering capabilities on a par with the NSA.** The move came in the wake of the Charlie Hebdo attack which led to the deaths of 12 people and prompted the Je Suis Charlie support campaign.
- "**The new laws allow for NSA-style mass collection of metadata online** as well as setting up the National Commission for Control of Intelligence Techniques (CNCTR) to oversee data collection. It has been criticized by some as being the French equivalent of the Patriot Act and the ruling Socialist Party is accused of prying too far into the private lives of normal people in the name of counter-terrorism."

http://betanews.com/2015/05/06/france-gains-sweeping-nsa-style-surveillance-powers/ (emphasis added)

On The Other Hand: Germany Agrees to Reforms



www.dailymail.co.uk/wires/reuters/article-3624553/German-government-agrees-reform-BND-spy-agency-sources.html

German government agrees to reform BND spy agency -sources

By REUTERS

PUBLISHED: 16:17 EST, 3 June 2016 | **UPDATED:** 16:17 EST, 3 June 2016

BERLIN, June 3 (Reuters) - Germany's coalition government on Friday agreed to tighten controls over the country's BND spy agency and impose new legal restrictions on its surveillance activities, according to sources familiar with the agreement.

The long-delayed reform package for Germany's Bundesnachrichtendienst, or BND, was agreed during a meeting at the German chancellor's office on Friday, according to several participants in the meeting.

The legal reforms, which must still be finalized by the German parliament, would ban the BND from spying on countries in the European Union and its citizens, as well as EU institutions, except in the case of suspected terrorist activity.

The agreement also requires the head of the BND, the chancellor's office and an independent panel of judges to approve strategic foreign espionage activities based on keyword lists, according to the sources.

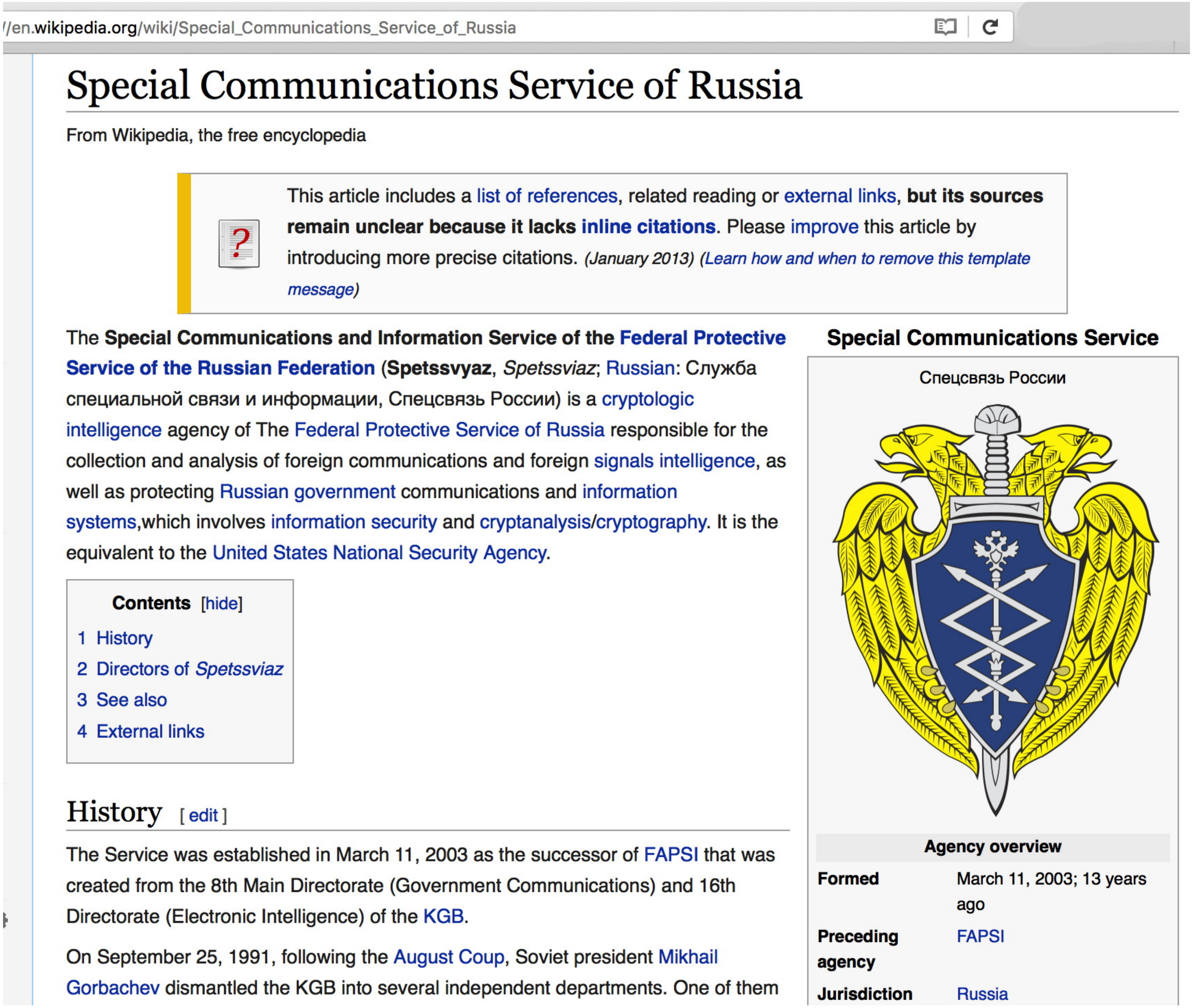
The changes would also spell out more clearly when the agency would be permitted to carry out such spying activities.

What About The Russian Federation? Check Out "SORM"

- "Russian hi-tech spy devices under attack over privacy fears" https://www.yahoo.com/news/russian-hi-tech-spy-devices-under-attack-over-113519708.html

  > "The KGB's post-Soviet successor, the FSB, has long used a sophisticated system called **SORM** to carry out surveillance communications by telephone or on the Internet."

- See https://en.wikipedia.org/wiki/SORM
- See also "Inside the Red Web: Russia's back door onto the internet – extract: In a chapter from their new book, Andrei Soldatov and Irinia Borogan outline how **every ISP has to give access to the state**", https://www.theguardian.com/world/2015/sep/08/red-web-book-russia-internet [emphasis added]



/en.wikipedia.org/wiki/Special_Communications_Service_of_Russia

Special Communications Service of Russia

From Wikipedia, the free encyclopedia

This article includes a list of references, related reading or external links, **but its sources remain unclear because it lacks inline citations**. Please improve this article by introducing more precise citations. *(January 2013) (Learn how and when to remove this template message)*

The **Special Communications and Information Service of the Federal Protective Service of the Russian Federation** (**Spetssvyaz**, *Spetssviaz*; Russian: Служба специальной связи и информации, Спецсвязь России) is a cryptologic intelligence agency of The Federal Protective Service of Russia responsible for the collection and analysis of foreign communications and foreign signals intelligence, as well as protecting Russian government communications and information systems,which involves information security and cryptanalysis/cryptography. It is the equivalent to the United States National Security Agency.

Special Communications Service

Спецсвязь России

Agency overview

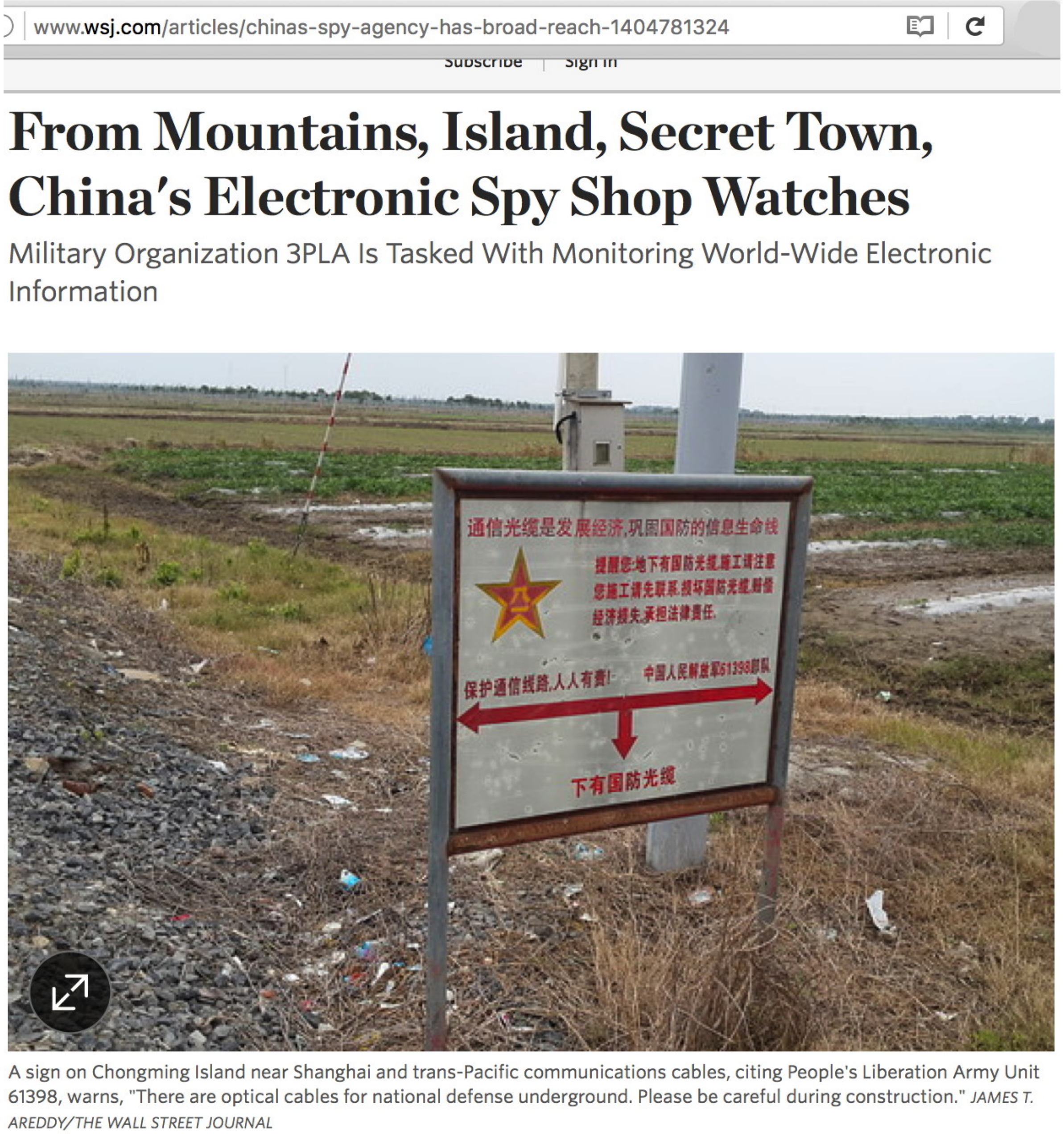
Formed	March 11, 2003; 13 years ago
Preceding agency	FAPSI
Jurisdiction	Russia

History [edit]

The Service was established in March 11, 2003 as the successor of FAPSI that was created from the 8th Main Directorate (Government Communications) and 16th Directorate (Electronic Intelligence) of the KGB.

On September 25, 1991, following the August Coup, Soviet president Mikhail Gorbachev dismantled the KGB into several independent departments. One of them

China? Note China's 3PLA



www.wsj.com/articles/chinas-spy-agency-has-broad-reach-1404781324

Subscribe | Sign In

From Mountains, Island, Secret Town, China's Electronic Spy Shop Watches

Military Organization 3PLA Is Tasked With Monitoring World-Wide Electronic Information

通信光缆是发展经济,巩固国防的信息生命线
提醒您:地下有国防光缆,施工请注意
您施工请先联系,损坏国防光缆,赔偿
经济损失,承担法律责任.
保护通信线路,人人有责!
中国人民解放军61398部队
下有国防光缆

A sign on Chongming Island near Shanghai and trans-Pacific communications cables, citing People's Liberation Army Unit 61398, warns, "There are optical cables for national defense underground. Please be careful during construction." *JAMES T. AREDDY/THE WALL STREET JOURNAL*

SO... Even If The US Totally "Cleans Up" *Its* Act, Many Foreign "NSA-Like" Agencies Will Still Be Going At It

- **This means that we as a community STILL need technical measures to hinder pervasive monitoring and interception of network traffic.**

- Encryption is at or near the top of the list of protective techniques.

- Unfortunately, the "second crypto war" is underway and your ability to use strong encryption as a way to protect your privacy online remains under concentrated attack.

IV. Encryption

There's LOTS Happening Right Now, Including Some Things That Are Good, and Some Things That Are Not So Good

The State of Strong Crypto Today

- Use of strong cryptography is a critical tool in the fight against warrantless pervasive monitoring.

- A lot of good things have been happening in the crypto world.

- Points of concern continue to arise, too.

We've Come FAR, Quite QUICKLY, Post Snowden...

- "The Director of National Intelligence on Monday blamed NSA whistleblower Edward Snowden for advancing the development of user-friendly, widely available strong encryption.
- "**"As a result of the Snowden revelations, the onset of commercial encryption has accelerated by seven years,"** James Clapper said during a breakfast for journalists hosted by the *Christian Science Monitor*. * * *
- "When pressed by *The Intercept* to explain his figure, Clapper said it came from the National Security Agency. "The projected growth maturation and installation of commercially available encryption — **what they had forecasted for seven years ahead, three years ago, was accelerated to now,** because of the revelation of the leaks.""
- See https://theintercept.com/2016/04/25/spy-chief-complains-that-edward-snowden-sped-up-spread-of-encryption-by-7-years/

Google Stats on Encrypting Its Web Properties

- Google has long been a leader in promoting encryption of SMTP, sharing data on its progress in deploying STARTTLS (we'll discuss that elsewhere in this deck)
- **Google is now ALSO sharing data about its progress in encrypting its various web properties.** See https://www.google.com/transparencyreport/https/
- A few select take aways:
  - **80% of all requests to Google's web servers are now encrypted** (this is roughly on-par with Google's STARTTLS success for SMTP)
  - **Web access to Gmail is now 100% encrypted**
  - Looking at the range of crypto penetration for the top 10 countries, Canada is at the bottom with 69%, while Mexico is at top with 88%. The US? 75%
  - **"The vast majority of unencrypted end user traffic originating from a set of surveyed Google services comes from mobile devices. Unfortunately, these devices may no longer be updated and may never support encryption." Mobile devices == 96.6% of all unencrypted user traffic.**

Google's Now Also Tracking <u>3rd Party</u> Web Site Crypto

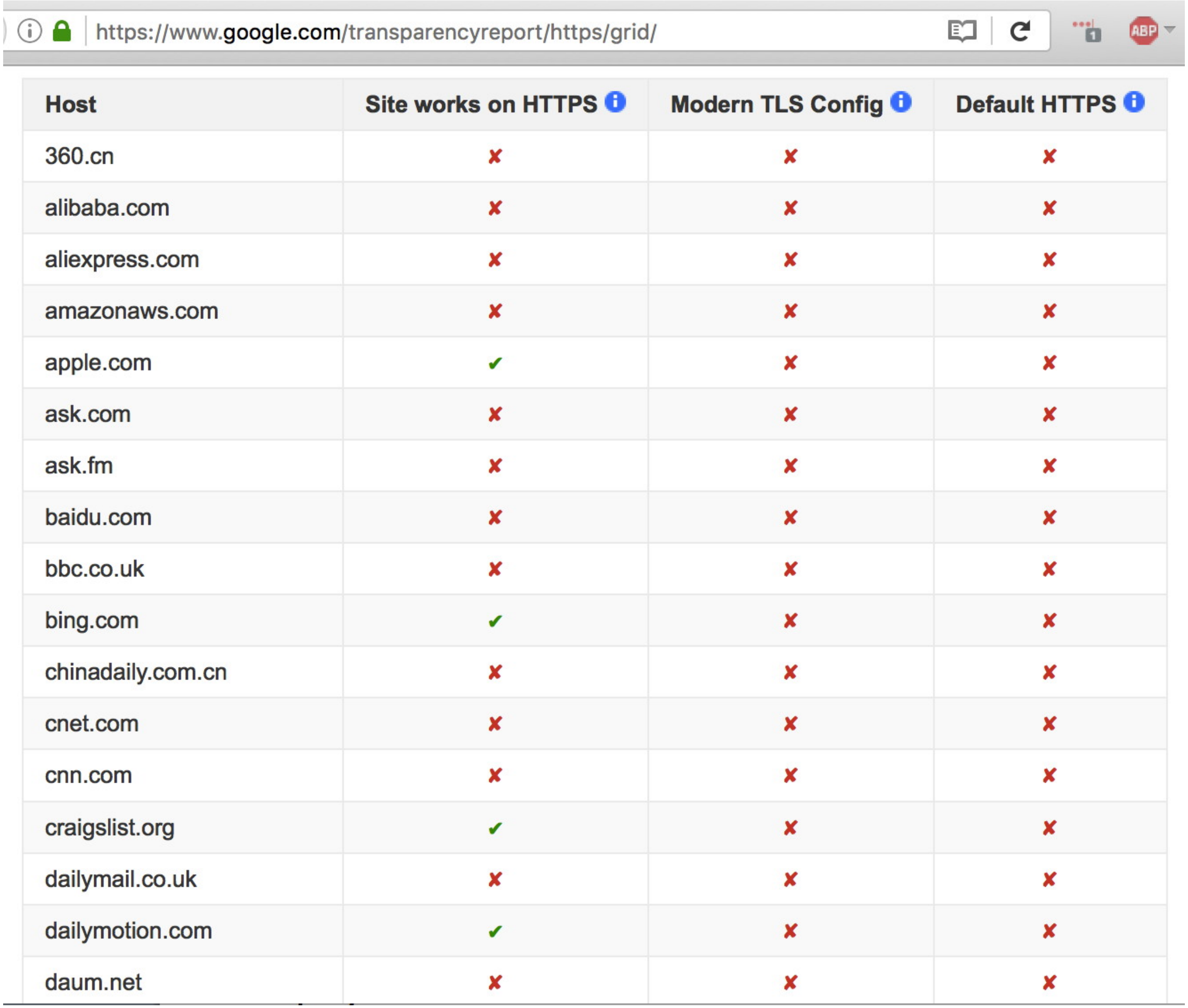
- The same Google transparency report also talks about the crypto status of major 3rd party web sites, considering three areas:

  -- Does the site support https connections?
  -- Does the site use a modern TLS configuration (e.g., TLS 1.2 with an AEAD cipher suites)?
  -- Does the site use https by default (e.g., redirect http requests to an https site)?

- Sadly, **many** major sites are deficient in one or more of these areas (often all three). What about YOUR domain(s)?

  See https://www.google.com/transparencyreport/https/grid/

  Part of their alphabetized list is shown on the next slide...



https://www.google.com/transparencyreport/https/grid/

Host	Site works on HTTPS	Modern TLS Config	Default HTTPS
360.cn	✗	✗	✗
alibaba.com	✗	✗	✗
aliexpress.com	✗	✗	✗
amazonaws.com	✗	✗	✗
apple.com	✓	✗	✗
ask.com	✗	✗	✗
ask.fm	✗	✗	✗
baidu.com	✗	✗	✗
bbc.co.uk	✗	✗	✗
bing.com	✓	✗	✗
chinadaily.com.cn	✗	✗	✗
cnet.com	✗	✗	✗
cnn.com	✗	✗	✗
craigslist.org	✓	✗	✗
dailymail.co.uk	✗	✗	✗
dailymotion.com	✓	✗	✗
daum.net	✗	✗	✗

While We're Speaking of Google: SSLv3/RC4

- SSLv3 and RC4 are cryptographically weak and shouldn't be used. Google and other providers are phasing those protocols out.
- http://www.infoworld.com/article/3071171/security/google-to-shutter-sslv3-rc4-from-smtp-servers-gmail.html wrote:

  "Mark your calendars: Google will disable support for the RC4 stream cipher and the SSLv3 protocol on its SMTP servers and Gmail servers on June 16." ***[Why hey! That's TODAY!]***

  "After the deadline, Google's SMTP servers will no longer exchange mail with servers sending messages via SSLv3 and RC4. Users still using older and insecure mail clients won't be able to send mail using Google's SMTP servers after that date. [article continues]"
- See also https://security.googleblog.com/2015/09/disabling-sslv3-and-rc4.html
- There's a lot more crypto stuff that should be on your radar, too...

Bouncy Castle & JCE non-DH ECC Private Key Leakage

- https://www.cvedetails.com/cve/CVE-2015-7940/ and http://web-in-security.blogspot.ca/2015/09/practical-invalid-curve-attacks.html [emphasis added]

- "Evaluation: We evaluated 8 crypto libraries and their vulnerabilities to invalid curve attacks. We found out that the **Bouncy Castle library** and the **Oracle JCE provider** were vulnerable and **we could extract private keys from the TLS servers running these libraries.** The attacks are quite powerful. For Bouncy Castle, we needed about 3300 real server queries. For Oracle JCE, we needed about 17000 real server queries. We tested with the NIST-256 curve. The high number of requests needed for the Java servers results from a strange behaviour (bug?) in the Java EC computation. You can get more information on the evaluation in our paper.

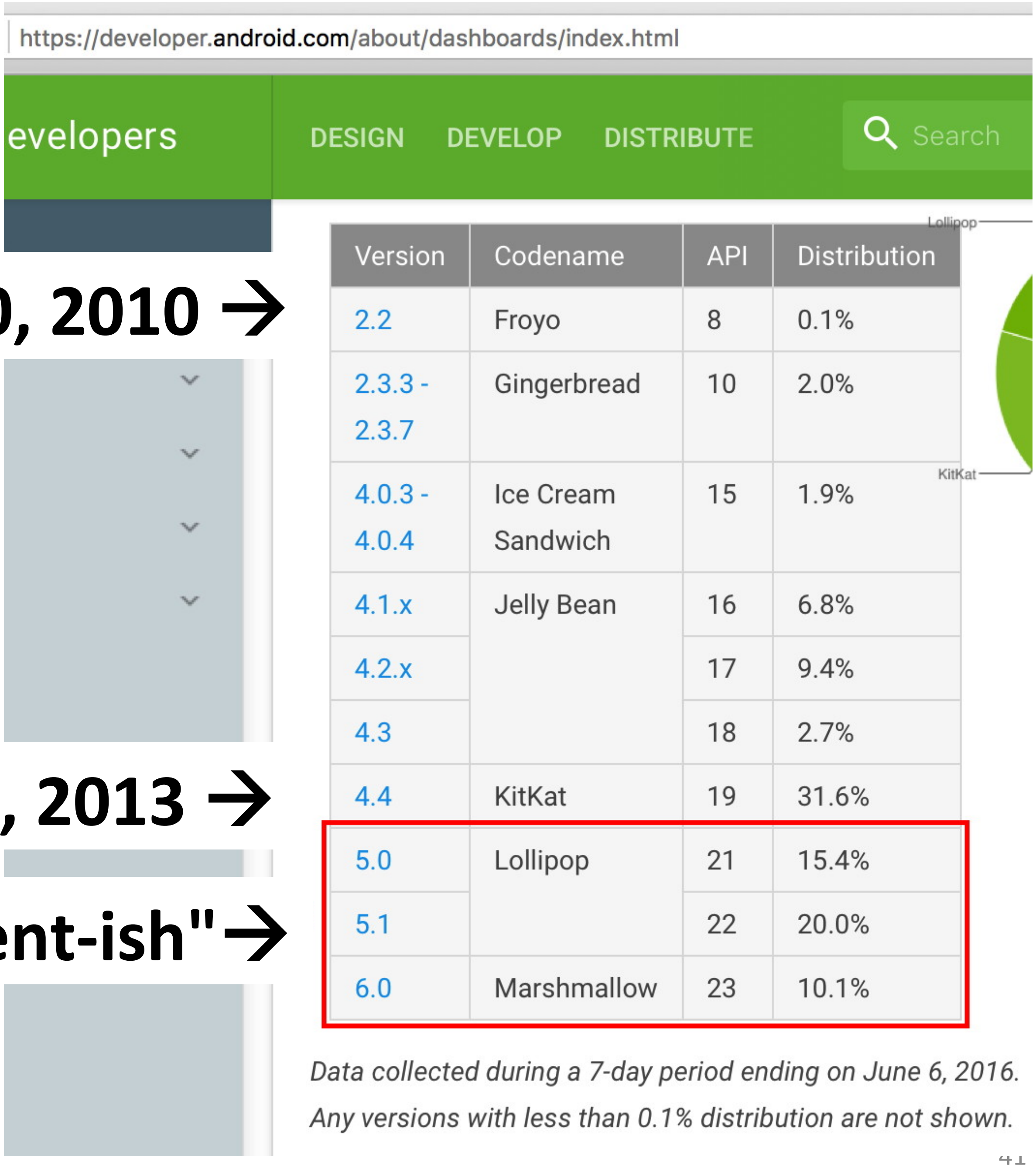
  "If you use these libraries for EC, you better update them and possibly revoke your old EC keys."

Smartphones and Strong Crypto

- **Remember that 96.6% of all the <u>insecure crypto</u> that Google saw on their web properties was associated with smartphones.**

  Many smart phones run non-current versions of the Android operating system, and are unable to support current cryptographic protocols (such as TLS 1.2)

- But let's eyeball what that Android operating system breakdown looks like – what percentage of currently used devices are more or less current, and able to support TLS 1.2 protocols?



https://developer.android.com/about/dashboards/index.html

Version	Codename	API	Distribution
2.2	Froyo	8	0.1%
2.3.3 - 2.3.7	Gingerbread	10	2.0%
4.0.3 - 4.0.4	Ice Cream Sandwich	15	1.9%
4.1.x	Jelly Bean	16	6.8%
4.2.x		17	9.4%
4.3		18	2.7%
4.4	KitKat	19	31.6%
5.0	Lollipop	21	15.4%
5.1		22	20.0%
6.0	Marshmallow	23	10.1%

Data collected during a 7-day period ending on June 6, 2016.
Any versions with less than 0.1% distribution are not shown.

released May 20, 2010 →

released Oct 31, 2013 →

45.5% "current-ish"→

Is It Time For A Concerted Industry Push Around Getting User Smartphones Upgraded?

- Should M3AAWG begin pushing the industry to upgrade out-of-date smartphone operating systems?

- If we assume that many smartphone owners can't/won't upgrade the operating system of existing smartphones, do we need a concerted push to forklift those smartphones and encourage adoption of newer devices?

- But let's not get rat-holed.

  What about other smartphone-related issues?

Smartphone Crypto

- Smartphones are also the focus of much of the discussion around encryption in the media...

- Sometimes the problem was that smartphones frustrated the authorities; other times the news was that it was surprisingly easy for third parties to get at the contents of smartphones or their traffic.

Decryption of Encrypted <u>Blackberry</u> Messages? Sure. Just Use BlackBerry's 'Global Decryption Key'

- **"Exclusive: How Canadian Police Intercept and Read Encrypted BlackBerry Messages"**, https://motherboard.vice.com/read/rcmp-blackberry-project-clemenza-global-encryption-key-canada

> ***BlackBerry (formerly RIM) encrypts all messages sent between consumer phones, known as PIN-to-PIN or BBM messages, using a single "global encryption key" that's loaded onto every handset during manufacturing. With this one key, any and all messages sent between consumer BlackBerry phones can be decrypted and read****. In contrast, Business Enterprise Servers allow corporations to use their own encryption key, which not even BlackBerry can access. * * **
>
> ***"By resorting to the global key," the judge's decision on the Crown's objection to disclosing the key states, "the RCMP was able to decrypt the intercepted messages."*** *It isn't clear how the RCMP obtained the key, and the judge's statement addressing the matter is heavily redacted due to a sealing order.*

Decrypting [At Least One Sort of] iPhone Through Use of A Third Party Vendor's Technology? Yep...

- "The FBI And Cellebrite, The Israeli Company Reportedly Hacking The iPhone, Are Old Friends With $2 Million Worth Of Memories," http://www.ibtimes.com/fbi-cellebrite-israeli-company-reportedly-hacking-iphone-are-old-friends-2-million-2342283

- "For months, the FBI has portrayed its case against Apple Inc. as one of desperation: that it had exhausted every known means to crack the iPhone 5C carried by Syed Farook on Dec. 2 when he and wife, Tashfeen Malik, shot and killed 14 people in San Bernardino, California.

  And yet the "outside vendor" the FBI is reported to be working with to break the encryption on the phone has long relationships with many branches of the U.S. government, including the FBI. [article continues]

Think A Fingerprint Sensor Give Strong Protection Against Compulsory Decryption of A Seized Device?

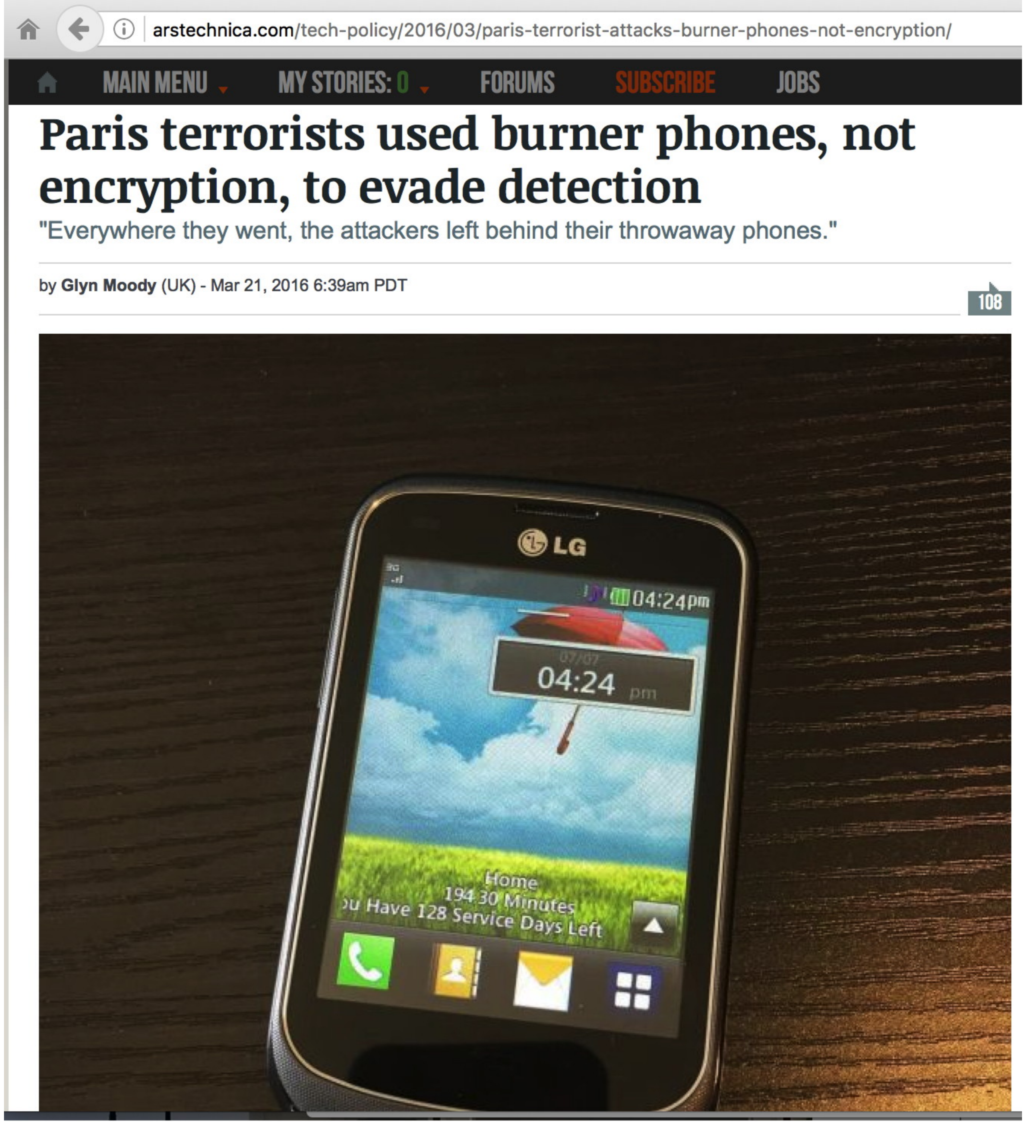
"As the world watched the FBI spar with Apple this winter in an attempt to hack into a San Bernardino shooter's iPhone, federal officials were quietly waging a different encryption battle in a Los Angeles courtroom.

"There, authorities obtained a search warrant compelling the girlfriend of an alleged Armenian gang member to press her finger against an iPhone that had been seized from a Glendale home. The phone contained Apple's fingerprint identification system for unlocking, and prosecutors wanted access to the data inside it.

"It marked a rare time that prosecutors have demanded a person provide a fingerprint to open a computer, but experts expect such cases to become more common as cracking digital security becomes a larger part of law enforcement work."

http://www.latimes.com/local/california/la-me-iphones-fingerprints-20160430-story.html

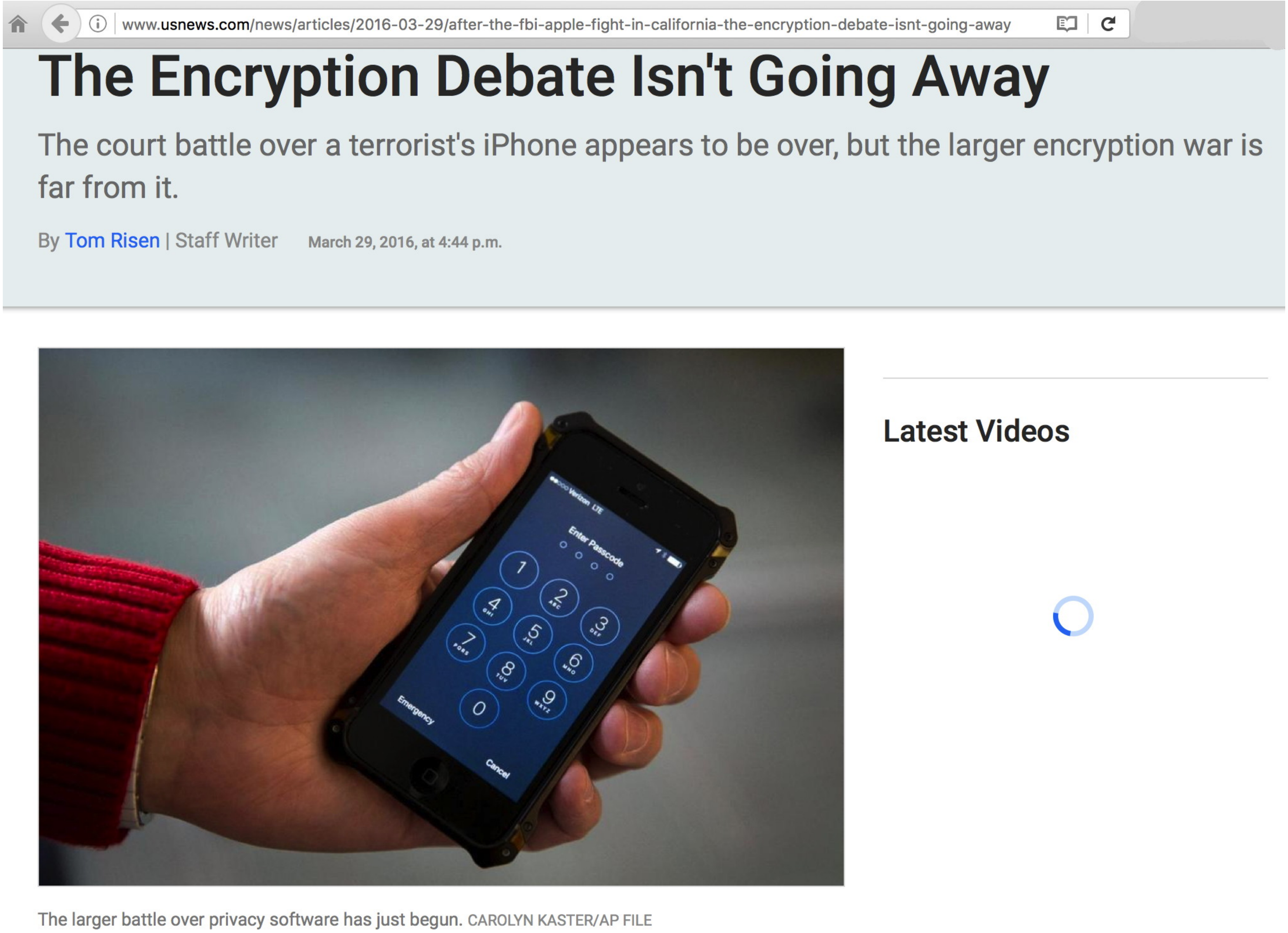
Sometimes, Encryption Was Blamed Even When Encryption Wasn't What Thwarted Detections


arstechnica.com/tech-policy/2016/03/paris-terrorist-attacks-burner-phones-not-encryption/
MAIN MENU
MY STORIES: 0
FORUMS
SUBSCRIBE
JOBS
108
LG
04:24pm
04:24 pm
Home
194 30 Minutes
ɔu Have 128 Service Days Left

Paris terrorists used burner phones, not encryption, to evade detection

"Everywhere they went, the attackers left behind their throwaway phones."

by **Glyn Moody** (UK) - Mar 21, 2016 6:39am PDT



www.usnews.com/news/articles/2016-03-29/after-the-fbi-apple-fight-in-california-the-encryption-debate-isnt-going-away

The Encryption Debate Isn't Going Away

The court battle over a terrorist's iPhone appears to be over, but the larger encryption war is far from it.

By Tom Risen | Staff Writer March 29, 2016, at 4:44 p.m.

Latest Videos

The larger battle over privacy software has just begun. CAROLYN KASTER/AP FILE

CA (and NY) Legislatures: Ban Encrypted Phones?

"Victory: California Smartphone Anti-Encryption Bill Dies in Committee", https://www.eff.org/deeplinks/2016/04/victory-california-smartphone-anti-encryption-bill-dies-committee

"The California Assembly Committee on Privacy and Consumer Protection has scuttled A.B. 1681, the anti-smartphone encryption bill that EFF has been fighting against for the last few months. The bill was unable to get a second in committee, so it died without a formal vote.

"A.B. 1681 was introduced in January of this year, and originally required that every smartphone sold in California have the technical ability to be decrypted and unlocked at the time of sale by the manufacturer or operating system provider. The bill was then amended to penalize companies that couldn't decrypt the contents of a smartphone pursuant to a state court order."

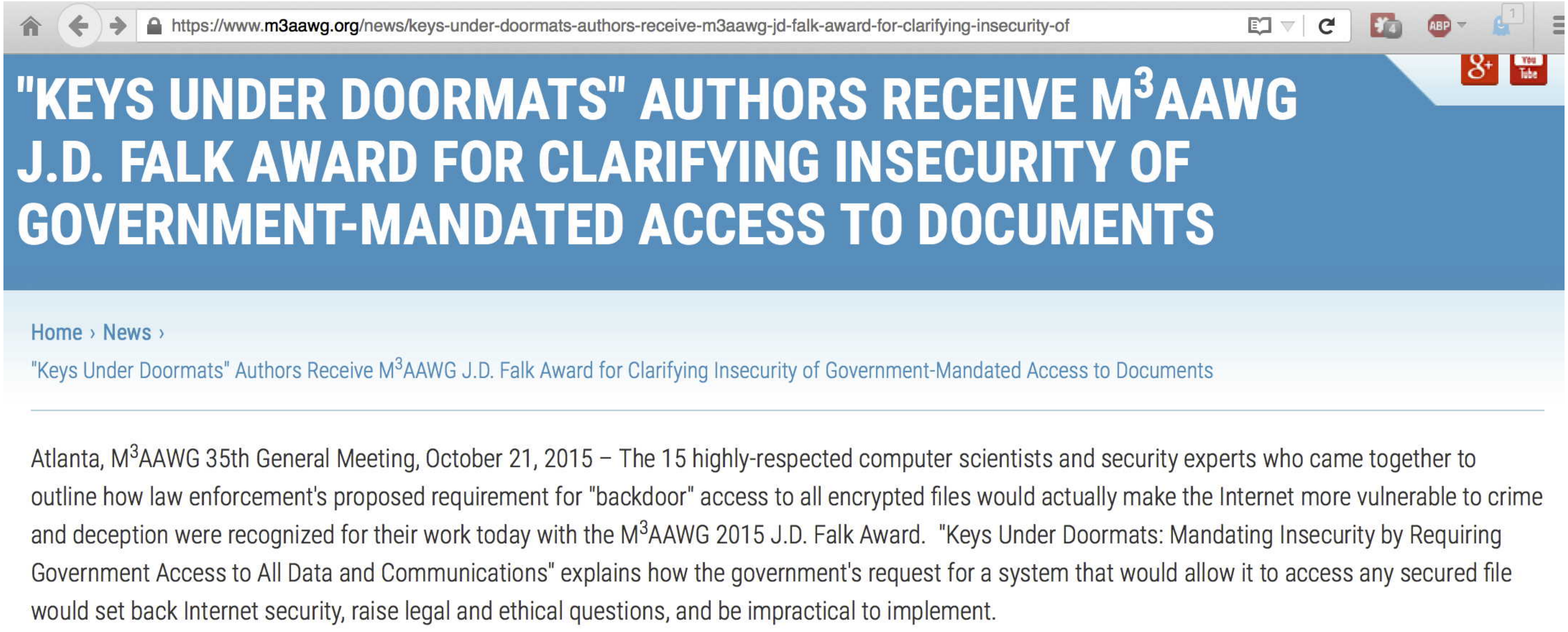
President Obama on Encrypted Smartphones

- **"Government can't let smartphones be 'black boxes,' Obama Says",** http://www.bloomberg.com/politics/articles/2016-03-11/obama-confronts-a-skeptical-silicon-valley-at-south-by-southwest

> President Barack Obama said Friday that smartphones -- like the iPhone the FBI is trying to force Apple Inc. to help it hack -- can't be allowed to be "black boxes," inaccessible to the government. The technology industry, he said, should work with the government instead of leaving the issue to Congress.

- **Mandating insecurity is poor public policy, a point that M3AAWG recognized in awarding the 2015 J.D. Falk award to the landmark "Keys Under the Doormat" paper by 15 leading cryptographers.**

"Keys Under Doormats: Mandating Insecurity By Requiring Government Access To All Data and Communications"



https://www.m3aawg.org/news/keys-under-doormats-authors-receive-m3aawg-jd-falk-award-for-clarifying-insecurity-of

"KEYS UNDER DOORMATS" AUTHORS RECEIVE M^{3}AAWG J.D. FALK AWARD FOR CLARIFYING INSECURITY OF GOVERNMENT-MANDATED ACCESS TO DOCUMENTS

Home › News ›

"Keys Under Doormats" Authors Receive M^{3}AAWG J.D. Falk Award for Clarifying Insecurity of Government-Mandated Access to Documents

Atlanta, M^{3}AAWG 35th General Meeting, October 21, 2015 – The 15 highly-respected computer scientists and security experts who came together to outline how law enforcement's proposed requirement for "backdoor" access to all encrypted files would actually make the Internet more vulnerable to crime and deception were recognized for their work today with the M^{3}AAWG 2015 J.D. Falk Award. "Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications" explains how the government's request for a system that would allow it to access any secured file would set back Internet security, raise legal and ethical questions, and be impractical to implement.

If you haven't read this paper, you should. It's available online at https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf

A Broad Anti-Crypto Draft Bill *Was* Proposed

- "The Senate's Draft Encryption Bill Is 'Ludicrous, Dangerous, Technically Illiterate'", https://www.wired.com/2016/04/senates-draft-encryption-bill-privacy-nightmare/

On Thursday evening, the draft text of a bill called the "Compliance with Court Orders Act of 2016," authored by offices of Senators Diane Feinstein and Richard Burr, was published online by the Hill. ***It's a nine-page piece of legislation that would require people to comply with any authorized court order for data—and if that data is "unintelligible," the legislation would demand that it be rendered "intelligible."*** *In other words, the bill would make illegal the sort of user-controlled encryption that's in every modern iPhone, in all billion devices that run Whatsapp's messaging service, and in dozens of other tech products.* ***"This basically outlaws end-to-end encryption,"*** *says Joseph Lorenzo Hall, chief technologist at the Center for Democracy and Technology.* ***"It's effectively the most anti-crypto bill of all anti-crypto bills."***

But That Bill is Now Believed To Be Kaput

"Now, only months later, much of the support is gone, and **the push for legislation dead**, according to sources in congressional offices, the administration and the tech sector.

"Draft legislation that Senators Richard Burr and Dianne Feinstein, the Republican and Democratic leaders of the Intelligence Committee, had circulated weeks ago likely will not be introduced this year and, even if it were, would stand no chance of advancing, the sources said.

"Key among the problems was the lack of White House support for legislation in spite of a high-profile court showdown between the Justice Department and Apple Inc over the suspect iPhone, according to Congressional and Obama Administration officials and outside observers."

http://www.reuters.com/article/us-usa-encryption-legislation-idUSKCN0YI0EM

<u>Some</u> In Washington *<u>Do</u>* Support Strong Crypto

- **"NSA Chief Stakes Out Pro-Encryption Position, in Contrast to FBI",** https://theintercept.com/2016/01/21/nsa-chief-stakes-out-pro-encryption-position-in-contrast-to-fbi/

'National Security Agency Director Adm. Mike Rogers said Thursday that "encryption is foundational to the future," and arguing about it is a waste of time.

'Speaking to the Atlantic Council, a Washington, D.C., think tank, Rogers stressed that the cybersecurity battles the U.S. is destined to fight call for more widespread use of encryption, not less.' * * *

'A former NSA director, Michael Hayden, said in January that he thinks Comey is on the wrong side of this debate. "I disagree with Jim Comey. I actually think end-to-end encryption is good for America," he said.'

Questions Remain About ECC and NSA's New PQC Crypto Policy: "A Riddle Wrapped In An Enigma"

- "A Riddle Wrapped In An Enigma" http://eprint.iacr.org/2015/1018.pdf

- "In August 2015 the U.S. National Security Agency (NSA) released a major policy statement on the need for post-quantum cryptography (PQC). This announcement will be a great stimulus to the development, standardization, and commercialization of new quantum-safe algorithms. However, certain peculiarities in the wording and timing of the statement have puzzled many people and given rise to much speculation concerning the NSA, elliptic curve cryptography (ECC), and quantum-safe cryptography. Our purpose is to attempt to evaluate some of the theories that have been proposed."

And A New Crypto Focus: RFC7858: Specification for DNS over Transport Layer Security (TLS), May 2016

This document describes the use of Transport Layer Security (TLS) to provide privacy for DNS. Encryption provided by TLS eliminates opportunities for eavesdropping and on-path tampering with DNS queries in the network, such as discussed in RFC 7626. In addition, this document specifies two usage profiles for DNS over TLS and provides advice on performance considerations to minimize overhead from using TCP and TLS with DNS.

This document focuses on securing stub-to-recursive traffic, as per the charter of the DPRIVE Working Group. It does not prevent future applications of the protocol to recursive-to-authoritative traffic.

[https://www.rfc-editor.org/rfc/rfc7858.txt , emphasis added]

V. So What Has M3AAWG Done To-Date?

Meeting Track Sessions, Keynotes, and Training Sessions, Captured on Video...

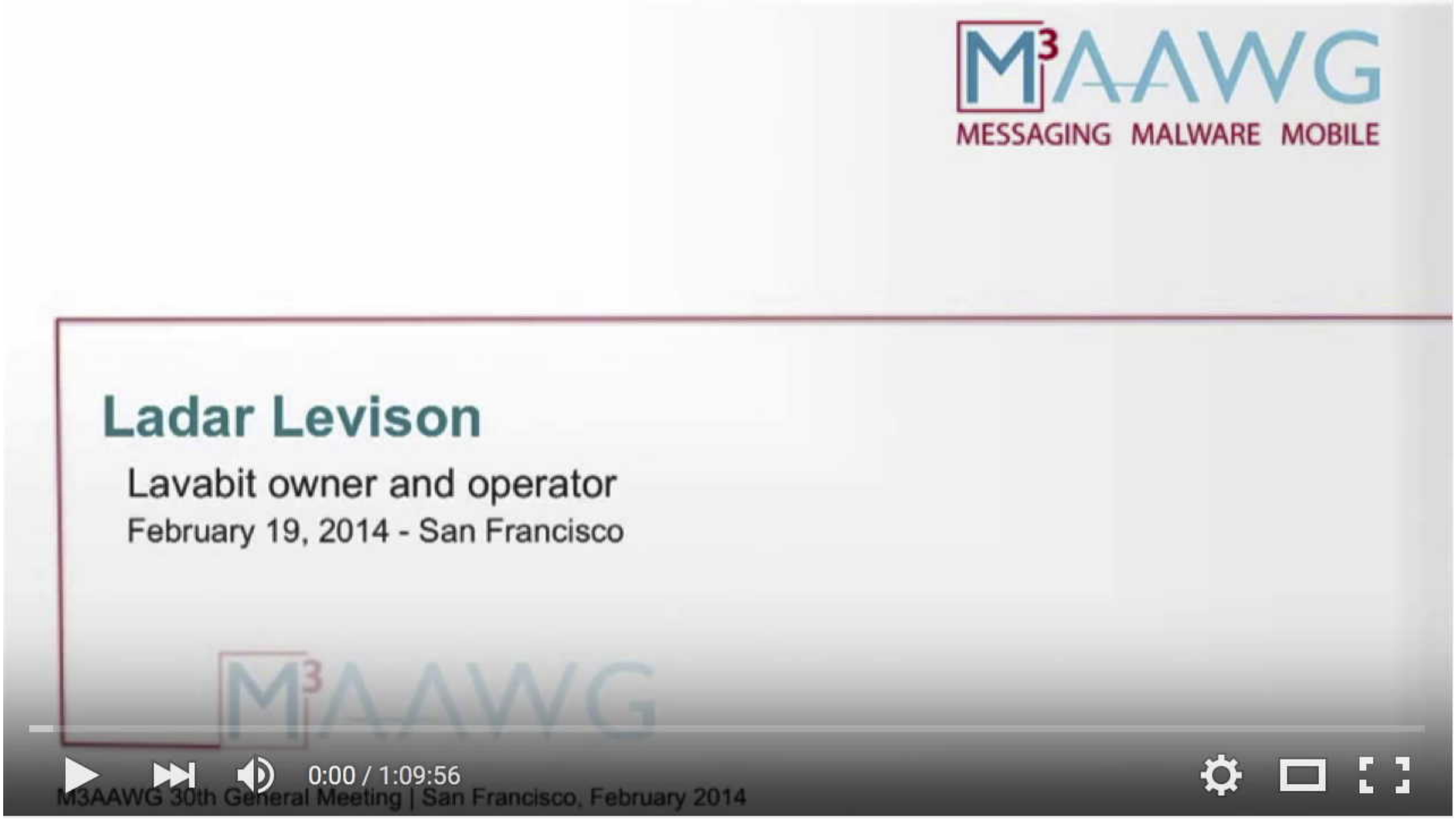
First, Some "Monitoring" Areas That Are Out Of Scope

- **Online tracking for marketing** and related purposes (not saying such tracking is a good thing, because it may not be, just that it's not part of the anti-Pervasive Monitoring SIG's bailiwick)
- Snooping of end-user systems by **criminals hackers** (this is also a problem, just not a focus of the anti-Pervasive Monitoring SIG)
- **Monitoring done with the consent of one party or both parties** to the communication (requirements depend on whether a "single party notification" or "two party notification" state is involved)
- **Monitoring of the Internet activity of minors by parents/schools**
- **Monitoring of employees' Internet activity by their employers**
- **Monitoring of academic institutional networks for research purposes** (particularly if anonymized and done with IRB approval)

M^{3}AAWG Meetings

- M^{3}AAWG meetings include a variety of sessions, including track sessions, invited keynotes, and in-depth training sessions. Many such sessions have recently focused on Anti-Pervasive Monitoring.
- As you'll see in the following slides, multiple Anti-Pervasive Monitoring-related videos are publicly available.
- M3AAWG always tries to bring in speakers with wide-ranging backgrounds so that the community can hear from those with diverse perspectives (do you perhaps have ideas for other speakers for future M3AAWG meetings?)
- Additional M3AAWG videos will continue to be added at https://www.youtube.com/user/MAAWG/videos
- Just to review a few of the videos that are currently out there...

Ladar Levison Keynote: M^{3}AAWG SFO 2/19/14



Ladar Levison

Lavabit owner and operator

February 19, 2014 - San Francisco

M3AAWG 30th General Meeting | San Francisco, February 2014

Watch it at https://www.youtube.com/watch?v=kF-nnyDUOV8

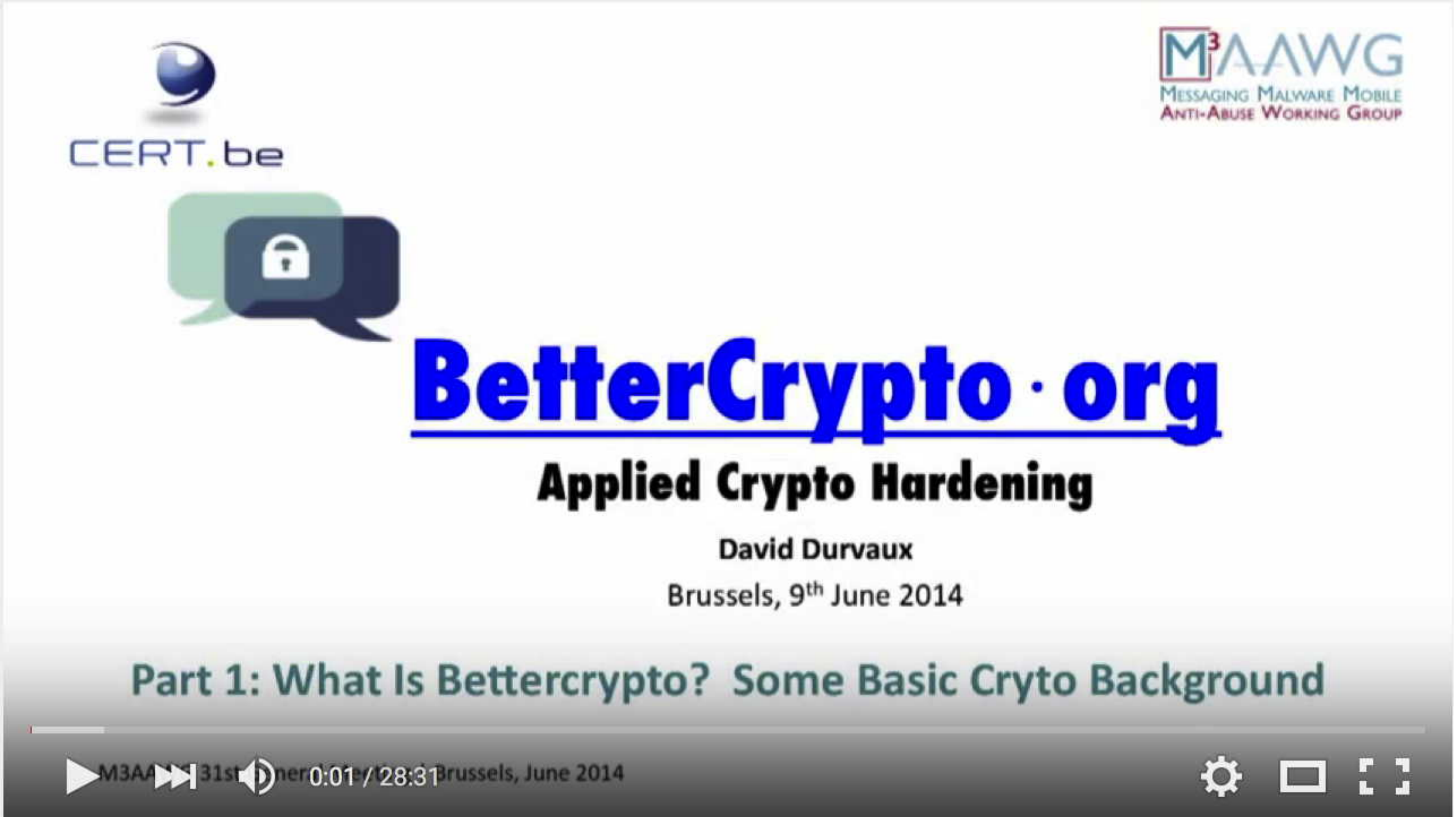
Ladar Levison and Lavabit

- If you're not familiar with Ladar Levison and Lavabit, Lavabit was Edward Snowden's ISP, offering specially encrypted email services.

- After Snowden's revelations began to occur, the government surreptitiously sought to compel Lavabit to release the company's SSL/TLS certificate and associated private key. This would have completely undercut the security of all Lavabit users.

- This keynote talk described what happened during that incident, and makes for a fascinating session to watch. See the Youtube link on the preceding slide.

Training: M^{3}AAWG Brussels, June 9th, 2014


CERT.be
M3AAWG
Messaging Malware Mobile Anti-Abuse Working Group

BetterCrypto·org

Applied Crypto Hardening

David Durvaux

Brussels, 9th June 2014

Part 1: What Is Bettercrypto? Some Basic Cryto Background

M3AA 31st ner Brussels, June 2014
0:01 / 28:31

Part 1: https://www.youtube.com/watch?v=GmhSCH6TfSw
Part 2: https://www.youtube.com/watch?v=WLpipaCyCRg

Brussels Crypto Sessions

- As a practical matter, one of the things service providers need to harden their crypto posture is technical advice about how to best configure their crypto-enabled web servers, mail servers, etc.

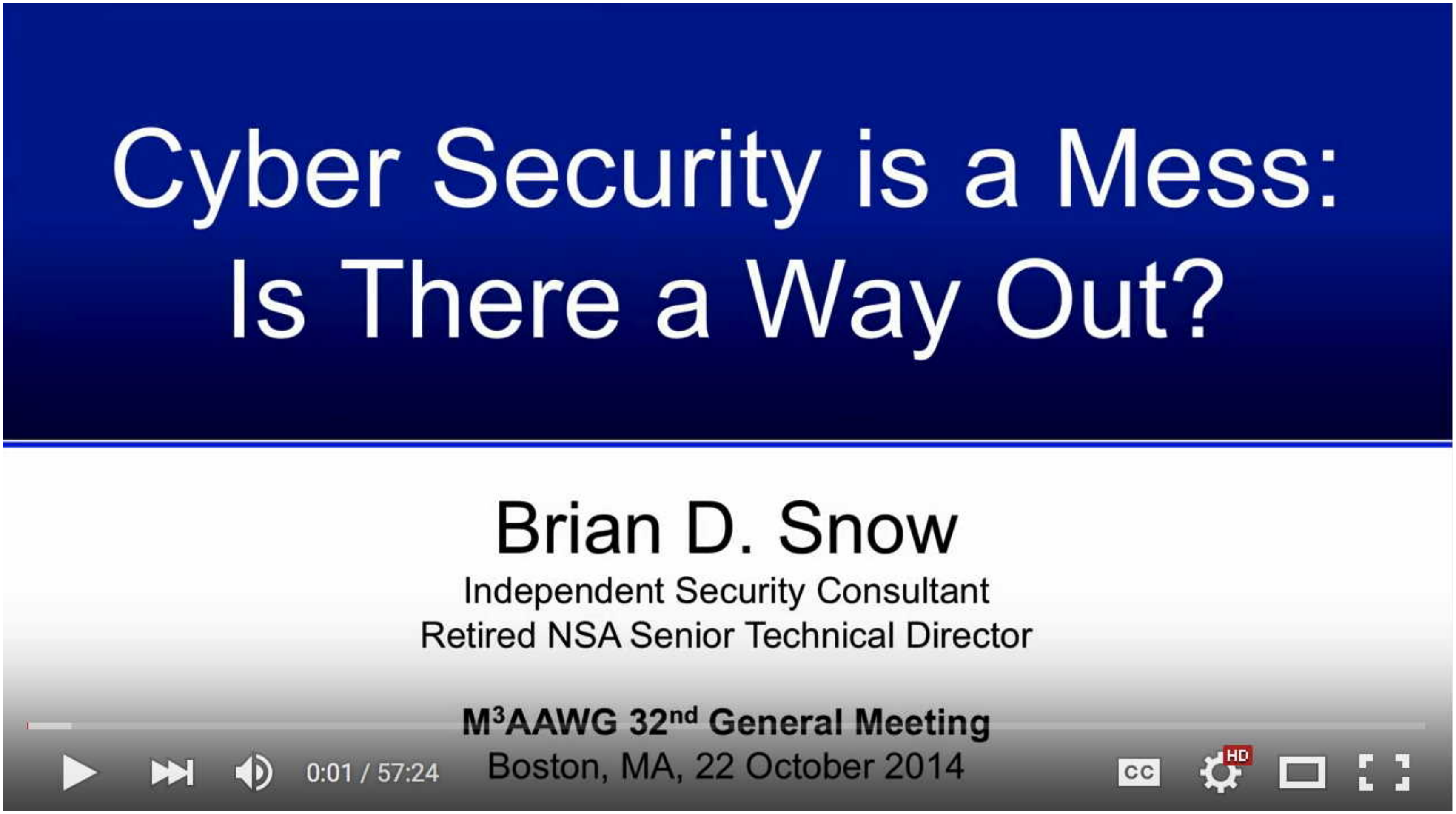
- The Better Crypto Applied Crypto Hardening training was an excellent source of advice for the community, and the Better Crypto handbook remains available online at

  https://bettercrypto.org/static/applied-crypto-hardening.pdf

The Boston, October 2014, Keynotes

- Three pervasive monitoring-related keynote video sessions are available from the Boston M^{3}AAWG meeting.
- One session was by Brian D. Snow, retired NSA Senior Technical Director. As noted at http://synaptic-labs.com/resources/security-bibliography/87-biographies/191-bio-brian-snow.html , "In all of his positions, he insisted that the actions NSA took to provide intelligence for our national and military leaders should not put U.S. persons or their rights at risk."
- A second session was by Dan Geer, a widely well-regarded cyber security expert. Wikipedia states that "Geer is currently the chief information security officer for In-Q-Tel, a not-for-profit venture capital firm that invests in technology to support the Central Intelligence Agency."
- The third session was a joint Q&A for both keynote speakers.

Keynote: M^{3}AAWG Boston, October 22nd, 2014



Cyber Security is a Mess:
Is There a Way Out?

Brian D. Snow
Independent Security Consultant
Retired NSA Senior Technical Director

M^{3}AAWG 32nd General Meeting
Boston, MA, 22 October 2014

Watch it at https://www.youtube.com/watch?v=tM_c7_GOU1Q

Keynote: M^3AAWG Boston, October 22nd, 2014

M^3AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

Shared Risk
and What to Do about It

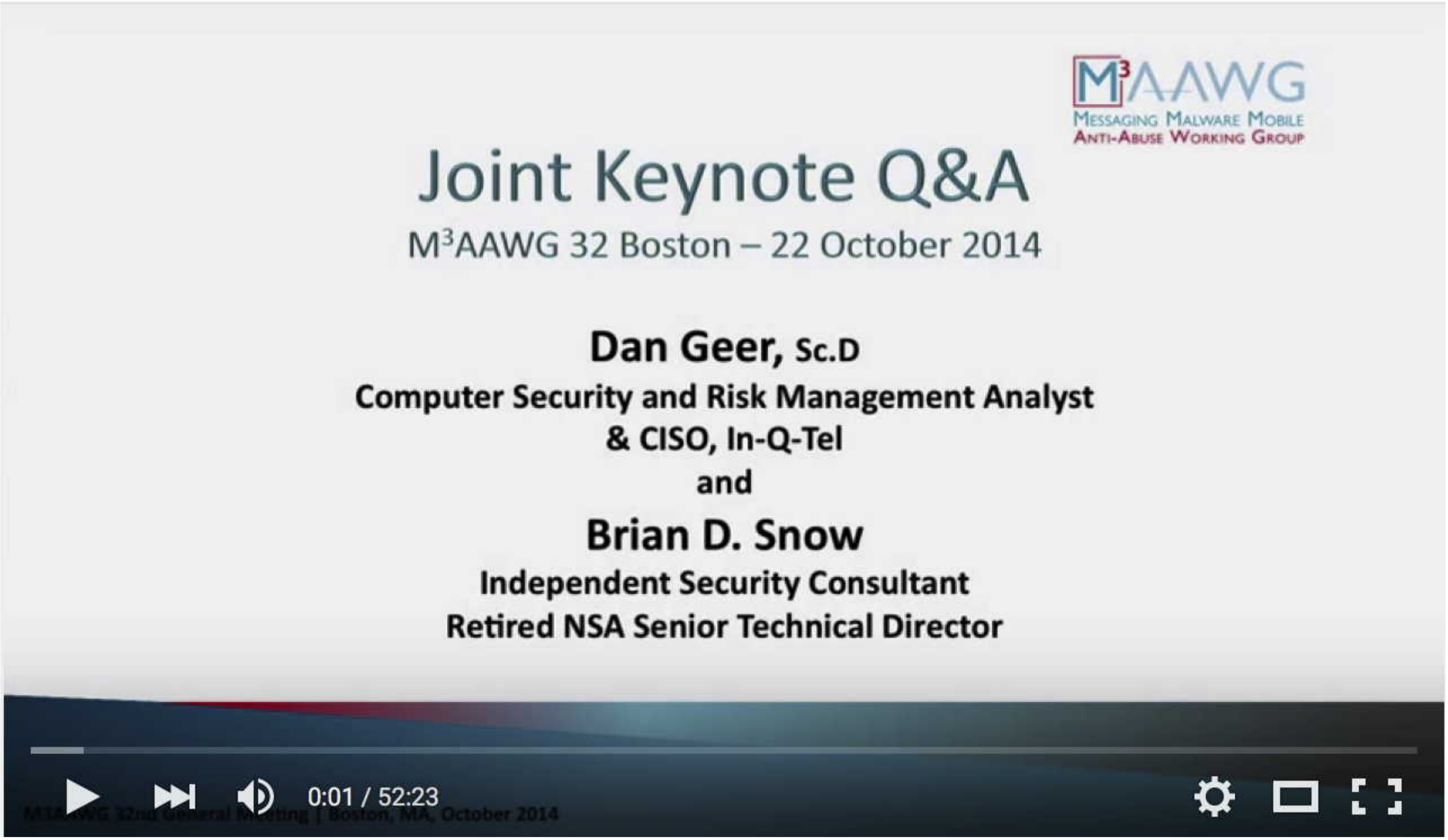
Dan Geer, Sc.D
Computer Security Researcher and Risk Management Analyst,
CISO, In-Q-Tel

October 2014 M^3AAWG 32^{nd} General Meeting

M3AAWG 32nd General Meeting | Boston, MA, October 2014

Watch it at https://www.youtube.com/watch?v=WvW9dVzz_Kg

Keynote Q&A: M^{3}AAWG Boston, October 22nd, 2014



M^{3}AAWG

Messaging Malware Mobile Anti-Abuse Working Group

Joint Keynote Q&A

M^{3}AAWG 32 Boston – 22 October 2014

Dan Geer, Sc.D

Computer Security and Risk Management Analyst

& CISO, In-Q-Tel

and

Brian D. Snow

Independent Security Consultant

Retired NSA Senior Technical Director

M3AAWG 32nd General Meeting | Boston, MA, October 2014

Watch it at https://www.youtube.com/watch?v=vM2pcRtOb6Y

VI. Tackling Passive Monitoring (aka "Network Eavesdropping")

The First Board-Approved M3AAWG Anti-Pervasive Monitoring Recommendation

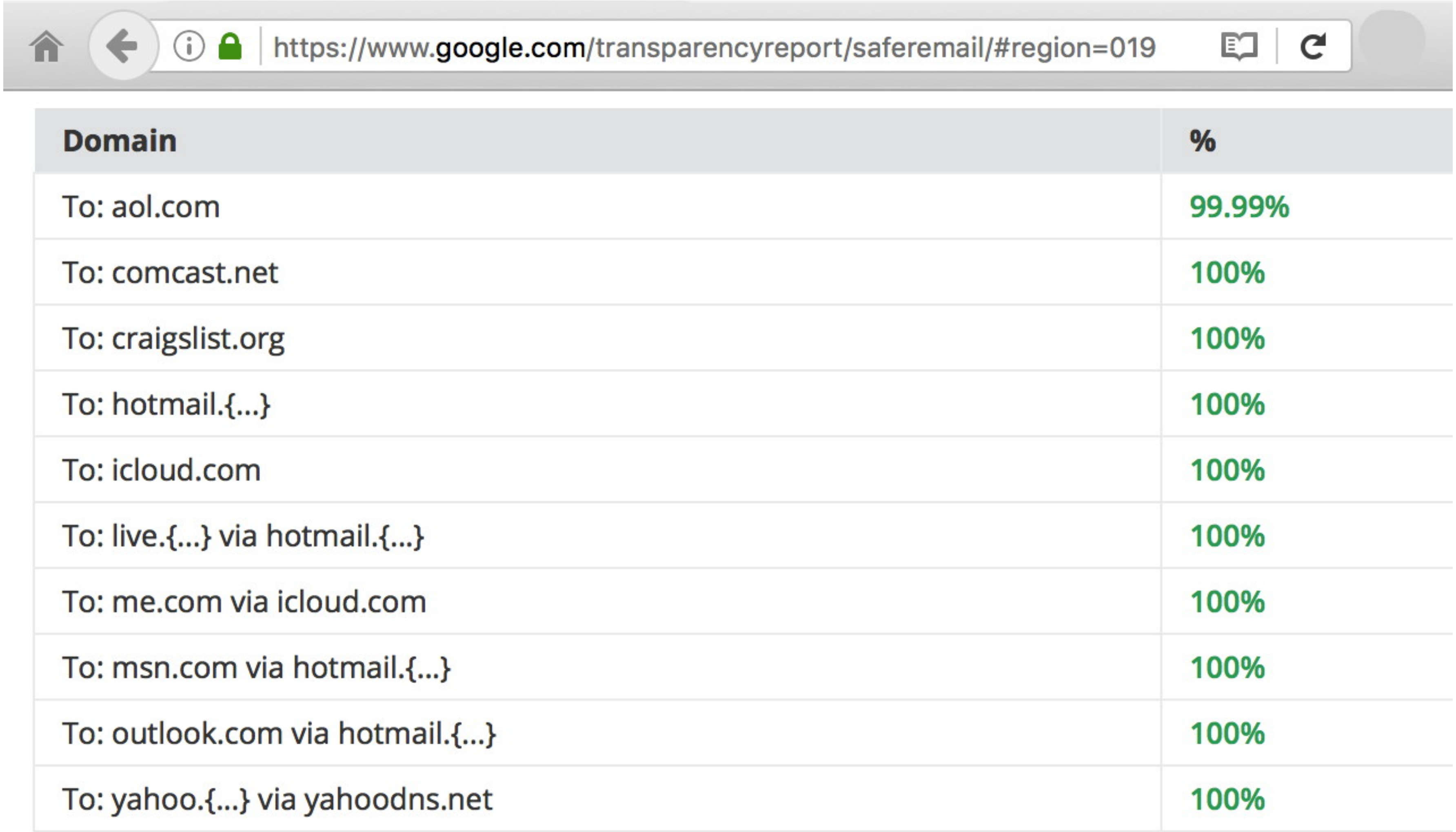
Opportunistic Encryption of Email In Transit

- As you might expect, given that email is a core area of M^{3}AAWG attention, **M^{3}AAWG's first Board-approved anti-pervasive-monitoring recommendation** was around **"TLS for Mail: M^{3}AAWG Initial Recommendations"**

  See https://www.m3aawg.org/sites/default/files/document/M3AAWG_TLS_Initial_Recommendations-2014-12.pdf

- This **M^{3}AAWG Board-approved document** is short (just two pages!) with some pretty basic recommendations:
  - Protect mail flows between providers with opportunistic TLS
  - Protect intracompany network traffic from eavesdropping
  - Protect user passwords from eavesdropping (IMAPS/POPS/SMTP Submit/web email interface)

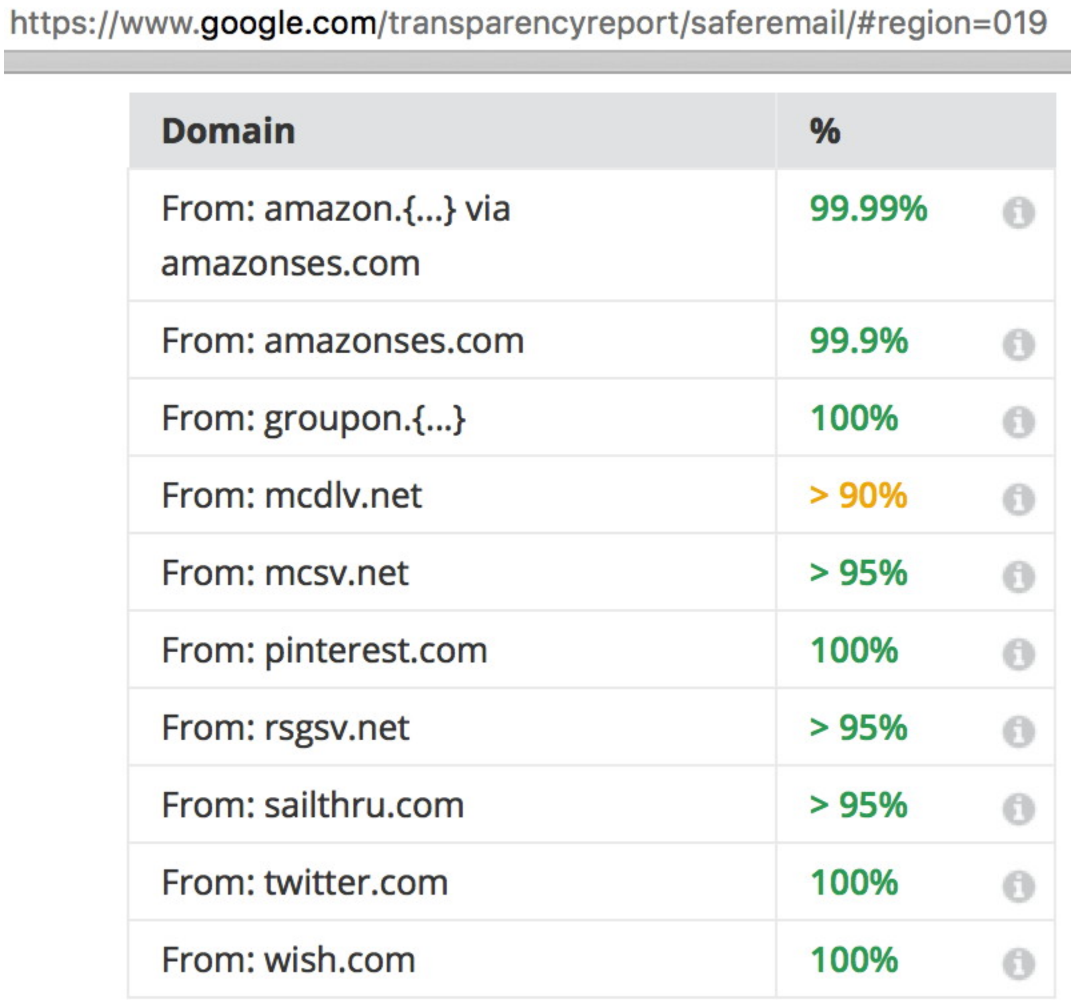
IS Email Getting Encrypted In Transit?
YES! Outbound From Google...



Domain	%
To: aol.com	99.99%
To: comcast.net	100%
To: craigslist.org	100%
To: hotmail.{...}	100%
To: icloud.com	100%
To: live.{...} via hotmail.{...}	100%
To: me.com via icloud.com	100%
To: msn.com via hotmail.{...}	100%
To: outlook.com via hotmail.{...}	100%
To: yahoo.{...} via yahoodns.net	100%

https://www.google.com/transparencyreport/saferemail/#region=019

Inbound To Google...



https://www.google.com/transparencyreport/saferemail/#region=019

Domain	%
From: amazon.{...} via amazonses.com	99.99%
From: amazonses.com	99.9%
From: groupon.{...}	100%
From: mcdlv.net	> 90%
From: mcsv.net	> 95%
From: pinterest.com	100%
From: rsgsv.net	> 95%
From: sailthru.com	> 95%
From: twitter.com	100%
From: wish.com	100%

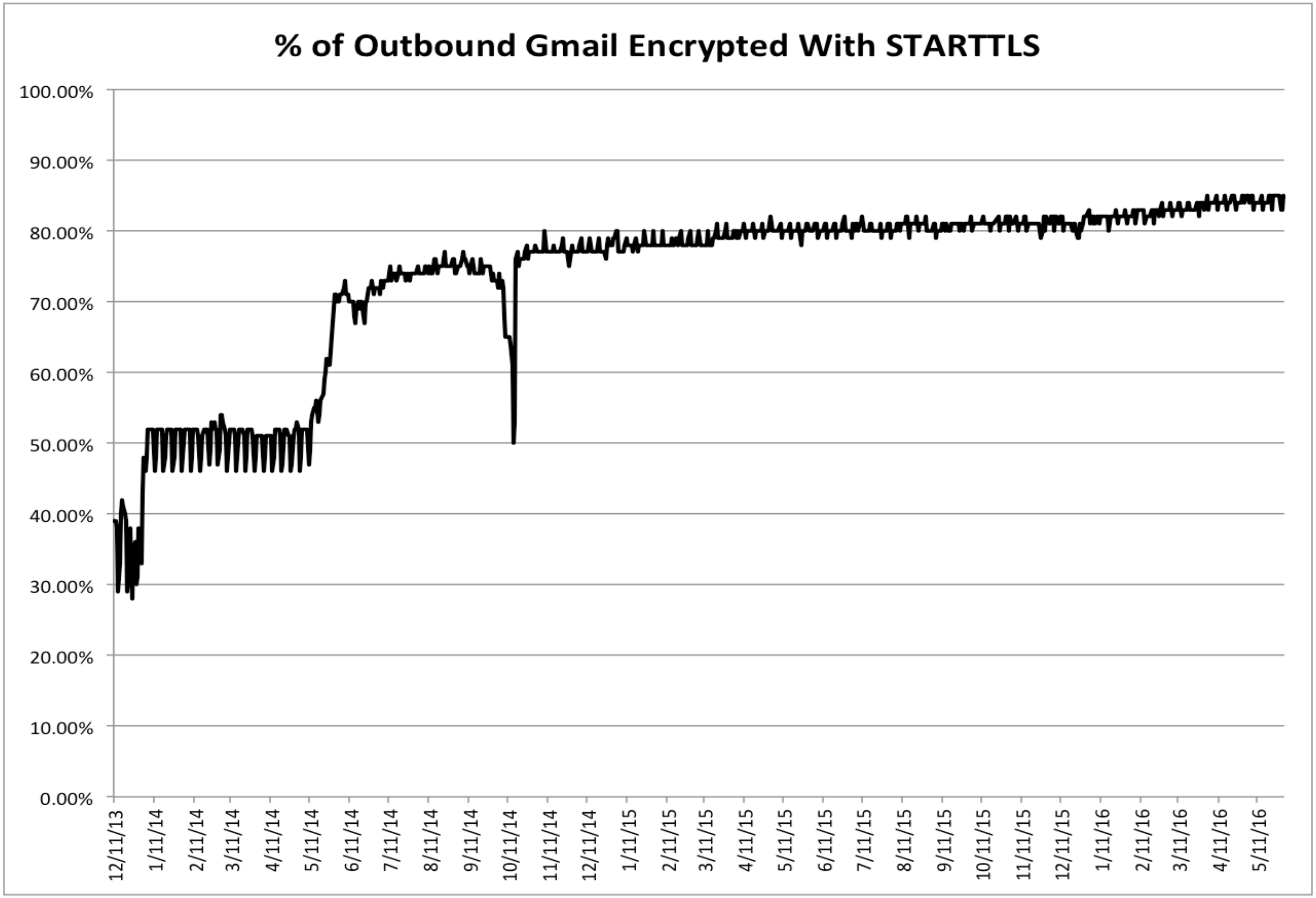
https://www.google.com/transparencyreport/saferemail/#region=019

All Those 100%'s and 99.99%'s? Those Numbers Represent A Bit of a Miracle...

- Few security technologies *ever* successfully deploy at Internet scale.

- **PGP/GPG?** Great, but only used by a tiny subset of all users.
- **IPSec?** Never deployed (except for some *ad hoc* VPN usage)
- **DNSSEC?** Deployment of DNSSEC still trails
- **RPKI?** Another security technology that's had a slow start.

- But ***encryption of email in transit*? THAT's** an example of a security technology that **HAS** deployed at scale. We've gone from 30-40% opportunistic encryption of outbound email from Google a year ago to 85% in just a few years. See the graph on the next slide.



https://www.google.com/transparencyreport/saferemail/google-starttls-percentages.csv

Does This Mean That Gmail Is "Going Dark?" NO!

- "Going dark" is short hand for "LEOs will no longer be able to conduct court-ordered lawful interceptions." That notion forms part of the basis for law enforcement "push back" against encryption (see for example http://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course by FBI Director James B. Comey from 10/16/14).
- The preceding graph is NOT an example of "going dark" even with 85% of outbound Gmail now encrypted in transit. Why? That 85% protection refers to email on the network *in transit*. Law enforcement is still free to obtain a court order for access to the email of a specific user on the ISP's *email servers*.
- So why bother encrypting in transit? ***Answer: It becomes far harder for foreign and domestic intelligence agencies, and any hacker/crackers that may be sitting on the wire, to potentially vacuum up EVERYONE's SMTP traffic indiscriminately.***

VII. Defeating MITM Attacks

The 2nd Board-Approved Recommendation

MITM Attacks

- Opportunistic SSL/TLS (as described in the initial M^{3}AAWG recommendations) protects against passive monitoring, but does nothing to address an active "man in the middle" attack.
- There are many ways that an attacker can MITM a conversation. **The SIG's 2nd Board-approved document,** on MITM (see https://www.m3aawg.org/sites/default/files/M3AAWG-Man-in-the-Middle-Recommendations2015-07.pdf) mentions:
  - ARP spoofing
  - Rogue DHCP servers
  - Use of Web Cache Control Protocol (WCCP)
  - Web Proxy Autodiscovery Protocol (WPAD)
  - Spoofed WiFi wireless access points ("evil twin" access points)
  - DNS poisoning
  - BGP route injection
  - Physical (inline) network traffic interception devices

Our Assessment of the Risks of MITM Attacks

- If an adversary can successfully execute a MITM attack against unencrypted/unsigned network traffic, the adversary will be able to:
  - eavesdrop upon the traffic,
  - modify the traffic, and
  - impersonate parties to the communication.

- **If the traffic is encrypted in transport, but endpoints are NOT cryptographically protected against MITM attacks, an adversary can execute the same attacks against encrypted traffic as it can against unencrypted traffic.**

- It is therefore extremely important that cryptographically "protected" transmissions be made robust to MITM attacks.

The Basic Problem With Opportunistic Encryption

- Opportunistic encryption "does the best it can" to protect email from eavesdropping. However, that may **not** be **good enough.**
- **To understand why this is true, think about what typically happen if opportunistic encryption is deemed to NOT be "good enough:" in that case, MTA-to-MTA transmissions normally fall back to sending email traffic in plain text, e.g., totally unencrypted.**
- In that sort of scenario, your "choice" may devolve to (a) tolerating "best effort crypto" (including crypto that's *totally* vulnerable to MITM attacks), (b) living with "no crypto at all," or (c) not transferring the message. None of those choices is very good. For example, even if "best effort" crypto is thought to be better than "no crypto at all," a MITM attacker with a self-signed cert could easily impersonate a real server.

What We Need: A Rigorous Alternative

- Mail servers identify themselves using a globally trustworthy certificate (e.g., the server is using a commercially-procured certificate that chains to a globally-trusted root; **the server is NOT using a self-signed certificate**)
- The name of the server correspond to one of the domain names for which the certificate was issued (**the server and certificate "match"**)
- Checking Online Certificate Status Protocol (OCSP) and/or a Certificate Revocation List (CRL), **the certificate can be seen to not have been revoked.**
- **The certificate is not being used before it is first valid, nor after it has expired.**
- The certificate is **signed using a (now-industry-standard) SHA-2 signature.**

The Rigorous Alternative (continued)

- The certificate covers a **strong (2048 or 4096 bit) RSA key pair.**
- The originating and receiving mail server support the most recent version of the TLS protocol (**TLS 1.2** at the time this document was drafted)
- The servers mutually agree upon using a cipher suite that supports **forward secrecy** for the purpose of key exchange (normally Ephemeral Diffie Hellman (EDH) or Elliptic Curve Diffie Hellman Ephemeral (ECDHE)
- A strong symmetric cipher is negotiated (ideally **AES-128 or AES-256**).
- **If ANY of the preceding conditions are not satisfied between the sending MTA and the receiving MTA, the sending server cannot be sure that it can safely transfer the message.**

What If A Message CAN'T Be Securely Conveyed?

- Options hypothetically include:
  - The message can be **rejected outright,** and returned to the sender for his or her processing (assuming the sending host and the receiving host reach an agreement that they CANNOT securely exchange a message *while a connection is still established*); messages that cannot be securely delivered must NOT be subsequently bounced to apparent message body senders (due to spoofed apparent senders).
  - Alternatively, the message can be **temporarily queued, and retried one or more times thereafter,** thereby helping to address transient non-deliverability issues.
  - After that, **the message must be summarily dropped.** (This presumes that the sender has an application-level delivery confirmation mechanism that will detect silent non-deliveries if/when they occur)

Yes, We Know

- This is really a brutal way of doing business, much like DNSSEC (it's either cryptographically "right," or it just doesn't happen).
- We also know that if we support plain text SMTP traffic as well as encrypted SMTP traffic, there's a risk of STARTTLS stripping
- Yes, the rigorous approach relies on the commercial certificate authority infrastructure, with all of its admitted shortcomings (the alternative, DANE, is lightly supported by available software)
- It mandates OCSP or CRL checking, which is another area where many rightfully don't feel all warm and fuzzy (see for example: https://www.imperialviolet.org/2014/04/19/revchecking.html); and yes, there is an increased risk of denial of service attacks.
- There may be some scenarios where it is difficult to talk about "matching" certificate names to machines (e.g., consider an MX server that is meant to answer for hundreds if not thousands of unique domains)

VIII. Forward Secrecy

Solution to Capturing-and-Then-Eventually-Decrypting Intercepted Encrypted Traffic

The Third Board-Approved Recommendation

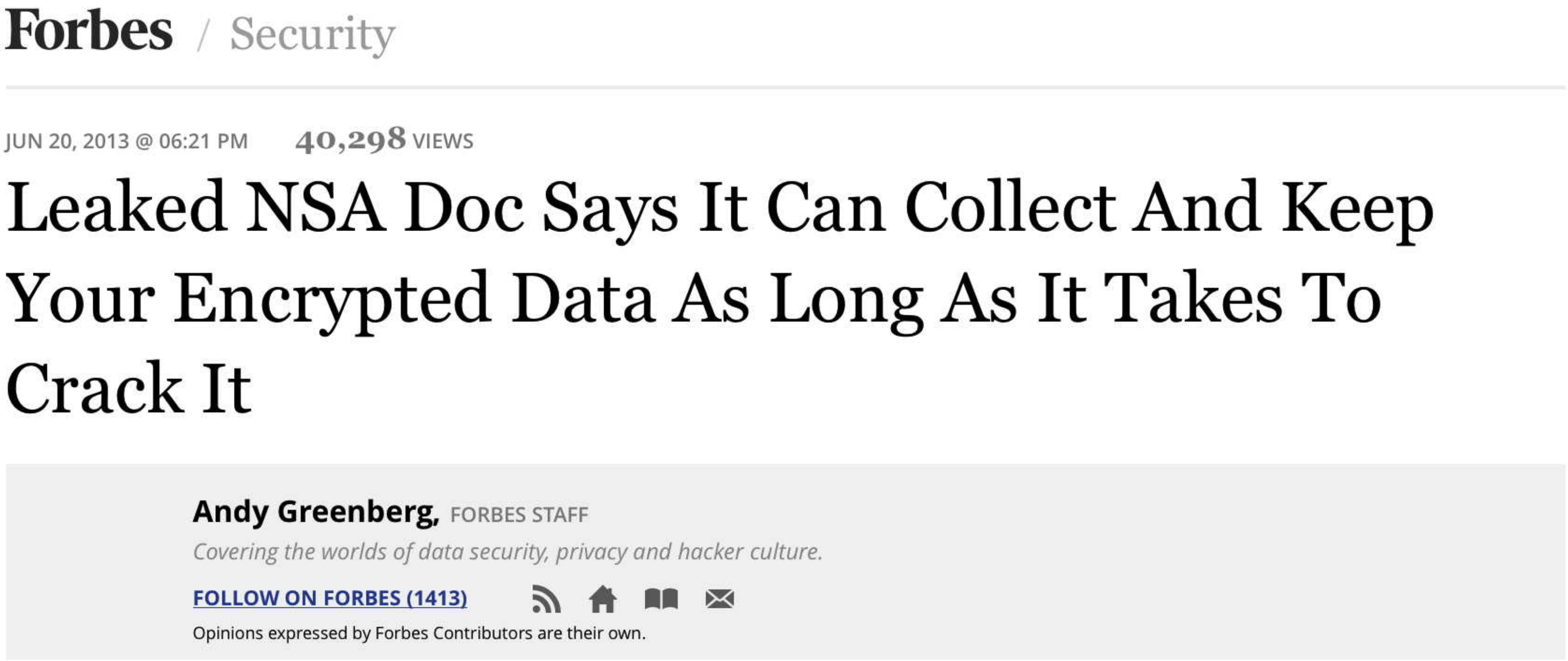
The Non-Forward Secrecy Risk Model

- The **third board-approved recommendation** was around Forward Secrecy, see http://www.m3aawg.org/sites/default/files/m3aawg-forward-secrecy-recommendations-2016-01.pdf

- Asymmetric crypto (relatively time consuming/expensive) is normally used to bootstrap agreement about a shared symmetric key. That approach generally works fine, with one exception:
  - An adversary intercepts & retains some or all of your TLS-encrypted traffic
  - The adversary ALSO manages to obtain a copy of your private key.

- If that happens, and you've NOT been using a cipher suite that has forward secrecy, then your adversary has everything they need to retrospectively decrypt ALL the traffic they may have squirreled away associated with that key.

Is Encrypted Traffic Being Retained? Yes...



Forbes / Security

JUN 20, 2013 @ 06:21 PM 40,298 VIEWS

Leaked NSA Doc Says It Can Collect And Keep Your Encrypted Data As Long As It Takes To Crack It

Andy Greenberg, FORBES STAFF

Covering the worlds of data security, privacy and hacker culture.

FOLLOW ON FORBES (1413)

Opinions expressed by Forbes Contributors are their own.

Forbes, June 20th, 2013

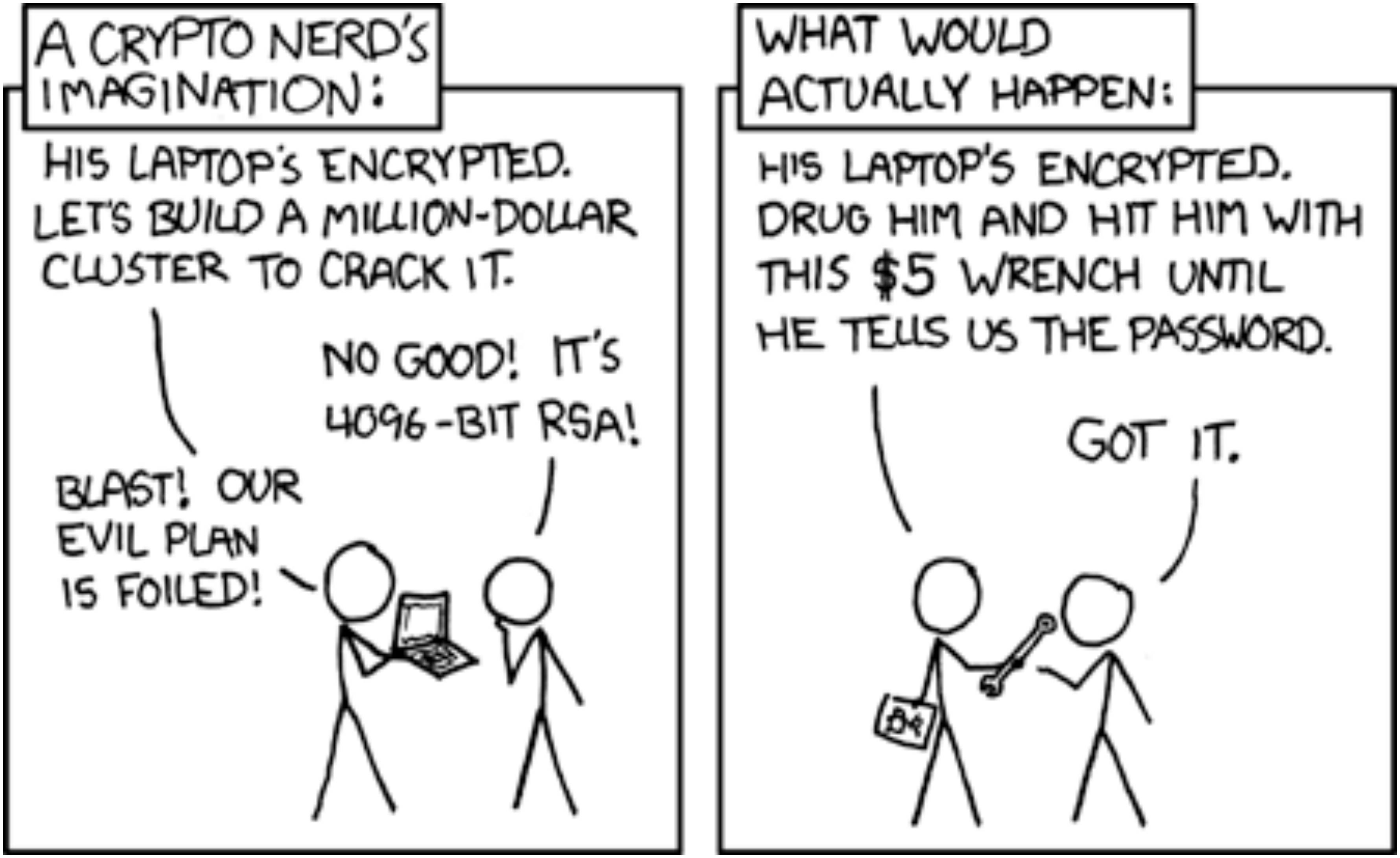
Are Private Keys Really At Risk of Disclosure?

- Since many sites just store their private key in a regular file (rather than storing their keys in a hardware security module (HSM) where the key can be *used* but not *extracted*), anyone who can arrange to access to the keys stored in a regular file would then be able to decrypt any associated encrypted traffic.

- Strategies for getting access to that key might include:

  - Subornation of a system administrator or other privileged user (bribery, extortion, torture, etc.),
  - A court order compelling disclosure (*ala* Lavabit)
  - Access to a poorly-secured copy of that file (e.g., perhaps access to an unencrypted backup stored at a third party site, or the system gets hacked/cracked by a cyber intruder who's after that critical file's contents).

$5 Wrenches As A Solution To Getting Private Keys


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.
$4

Source: https://xkcd.com/538/

The Solution: Forward Secrecy

- Fortunately there is a solution to this problem, and that's ephemeral key exchange.

- If sites uses a key exchange mechanism that offers forward secrecy, such as Diffie Hellman Ephemeral (DHE) or Elliptic Curve Diffie Hellman Ephemeral (ECDHE), **a new public/private key pair is created for each connection and then discarded immediately after use.**

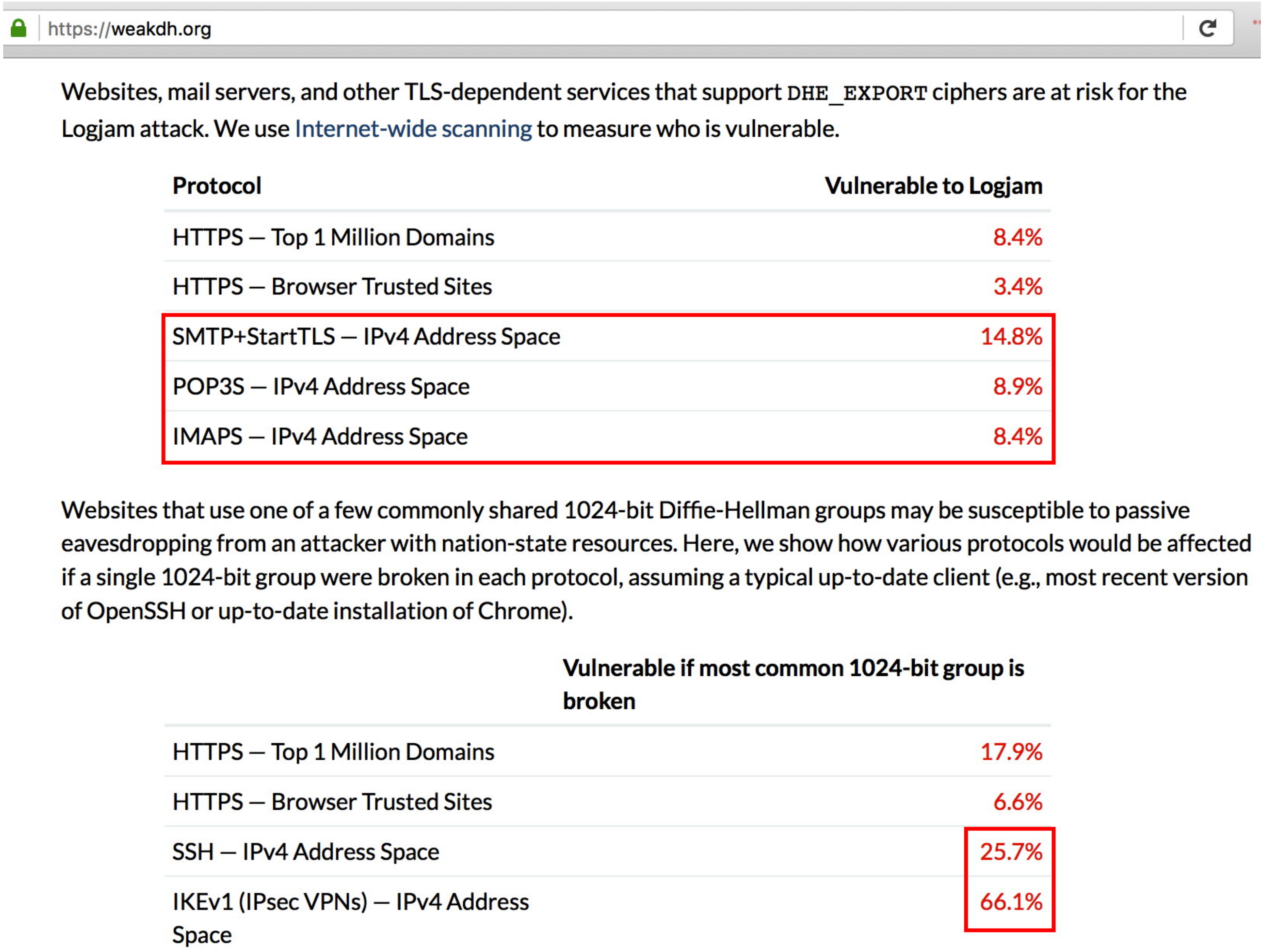
- With that approach, even if traffic does get captured and the security of the RSA private key is compromised, those adverse events won't result in an adversary being able to do retrospective decryption. Critical information needed for retrospective decryption will simply never have gotten saved in the first place.

Diffie-Hellman Parameters

- **In using ephemeral key exchange mechanisms, some care must be taken to ensure that long/strong Diffie-Hellman parameters get used.** At least in some circumstances, the default Diffie-Hellman parameters may only be 1024 bits long. Fortunately, current versions of popular cryptographic libraries such as OpenSSL now allow DH parameters all the way up to 4096 bits.

- Please note the recent article "Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice," https://weakdh.org/imperfect-forward-secrecy-ccs15.pdf

  See also the stats on the following slide from the weakdh.org site...



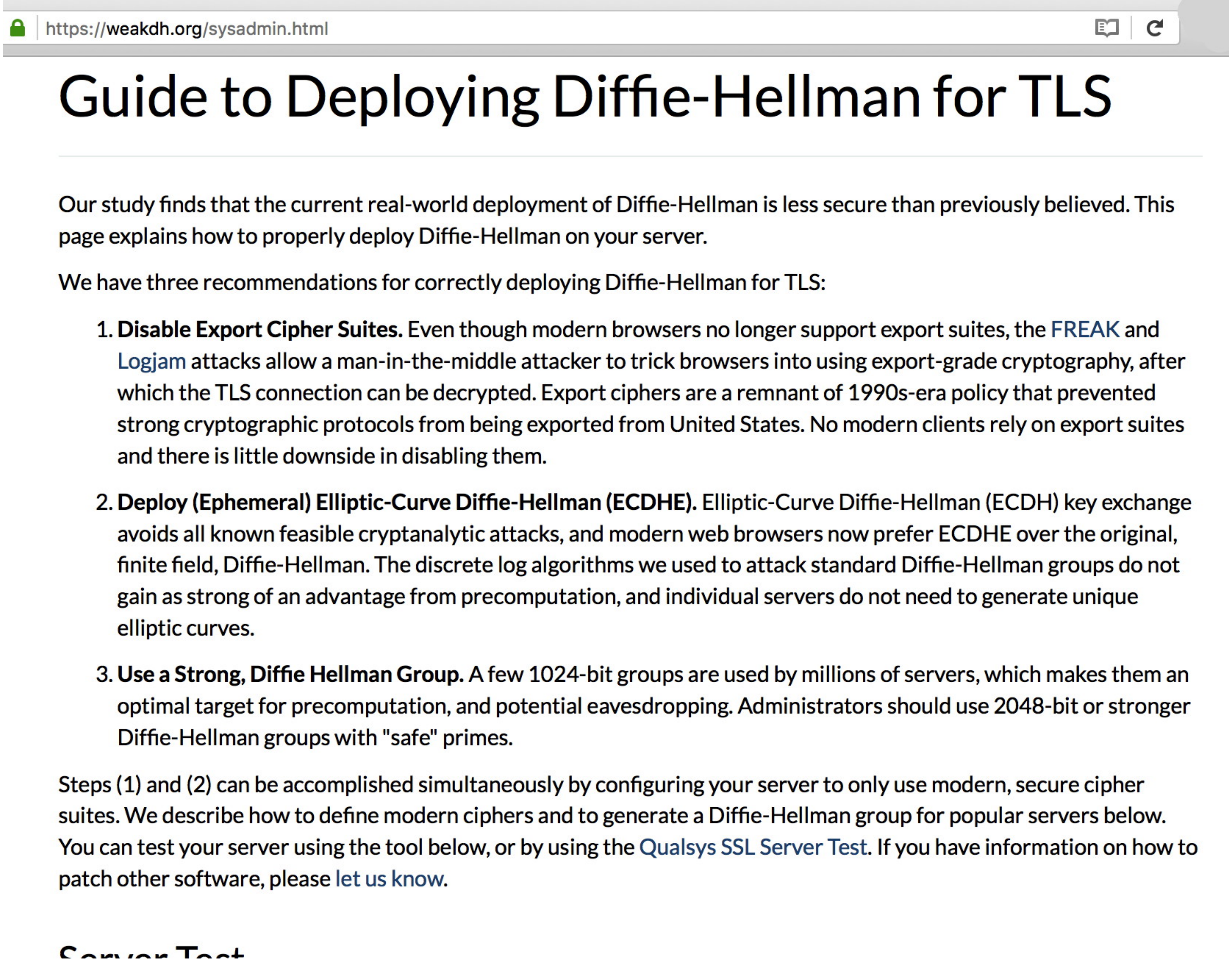
https://weakdh.org

Websites, mail servers, and other TLS-dependent services that support `DHE_EXPORT` ciphers are at risk for the Logjam attack. We use Internet-wide scanning to measure who is vulnerable.

Protocol	Vulnerable to Logjam
HTTPS — Top 1 Million Domains	8.4%
HTTPS — Browser Trusted Sites	3.4%
SMTP+StartTLS — IPv4 Address Space	14.8%
POP3S — IPv4 Address Space	8.9%
IMAPS — IPv4 Address Space	8.4%

Websites that use one of a few commonly shared 1024-bit Diffie-Hellman groups may be susceptible to passive eavesdropping from an attacker with nation-state resources. Here, we show how various protocols would be affected if a single 1024-bit group were broken in each protocol, assuming a typical up-to-date client (e.g., most recent version of OpenSSH or up-to-date installation of Chrome).

	Vulnerable if most common 1024-bit group is broken
HTTPS — Top 1 Million Domains	17.9%
HTTPS — Browser Trusted Sites	6.6%
SSH — IPv4 Address Space	25.7%
IKEv1 (IPsec VPNs) — IPv4 Address Space	66.1%



Guide to Deploying Diffie-Hellman for TLS

Our study finds that the current real-world deployment of Diffie-Hellman is less secure than previously believed. This page explains how to properly deploy Diffie-Hellman on your server.

We have three recommendations for correctly deploying Diffie-Hellman for TLS:

1. **Disable Export Cipher Suites.** Even though modern browsers no longer support export suites, the FREAK and Logjam attacks allow a man-in-the-middle attacker to trick browsers into using export-grade cryptography, after which the TLS connection can be decrypted. Export ciphers are a remnant of 1990s-era policy that prevented strong cryptographic protocols from being exported from United States. No modern clients rely on export suites and there is little downside in disabling them.
2. **Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE).** Elliptic-Curve Diffie-Hellman (ECDH) key exchange avoids all known feasible cryptanalytic attacks, and modern web browsers now prefer ECDHE over the original, finite field, Diffie-Hellman. The discrete log algorithms we used to attack standard Diffie-Hellman groups do not gain as strong of an advantage from precomputation, and individual servers do not need to generate unique elliptic curves.
3. **Use a Strong, Diffie Hellman Group.** A few 1024-bit groups are used by millions of servers, which makes them an optimal target for precomputation, and potential eavesdropping. Administrators should use 2048-bit or stronger Diffie-Hellman groups with "safe" primes.

Steps (1) and (2) can be accomplished simultaneously by configuring your server to only use modern, secure cipher suites. We describe how to define modern ciphers and to generate a Diffie-Hellman group for popular servers below. You can test your server using the tool below, or by using the Qualsys SSL Server Test. If you have information on how to patch other software, please let us know.

Server Test

IX. Traffic Analysis and "Metadata"

The Fourth Board-Approved Document

The Traffic Analysis Problem

- Even if an adversary can't see the contents of your message, **simply knowing the sender and the receiver, when a communication was sent, how large the communication was, etc., can still yield important information to a trained analyst.**

- Traffic analysis the fundamental reason why metadata gets collected. **Traffic analysis can be exceptionally powerful.**

- **If you'd like to learn more about traffic analysis, I did a talk on traffic analysis for M^{3}AAWG last year, see:**

  ***The Enduring Challenge of Traffic Analysis*, June 11th, 2015, https://www.stsauver.com/joe/dublin-traffic-analysis/dublin-traffic-analysis.pdf (108 slides)**

Our 4th Board Approved Recommendation

- I'm also very pleased to report that just this week M3AAWG was able to publicly post the 4th Board-approved anti-pervasive monitoring document. This 4th document summarizes the traffic analysis/metadata problem, and considerations pertaining to managing that issue.

- Please see "M3AAWG Introduction to Traffic Analysis," https://www.m3aawg.org/sites/default/files/ m3aawg_traffic_analysis_2016-06.pdf

TCP Host Identification, Even When NAT'd

- In the Dublin presentation mentioned at the start of this section, I discussed how broadband providers can limit some traffic analysis exposures through the use of non-1:1 NAT/PAT.

- Not surprisingly, there have been proposals in the IETF that would undercut the protection that NAT potentially provides as a defense against traffic analysis, see https://tools.ietf.org/id/draft-williams-exp-tcp-host-id-opt-08.txt

- There are many reasons why a site might be interested in tackling what they may perceive as the "NAT problem," but if this proposed approach is used in a way inconsistent with the draft RFC's recommendations, it could impact user protections against pervasive monitoring.

TCP Host Identification (continued)

- Note, however, http://www.ietf.org/mail-archive/web/ietf-announce/current/msg15033.html (emphasis added below):

  The IESG has completed a review of draft-williams-exp-tcp-host-id-opt-07 consistent with RFC5742. The IESG recommends that 'Experimental Option for TCP Host Identification' <draft-williams-exp-tcp-host-id-opt-07.txt> NOT be published as an Experimental RFC.

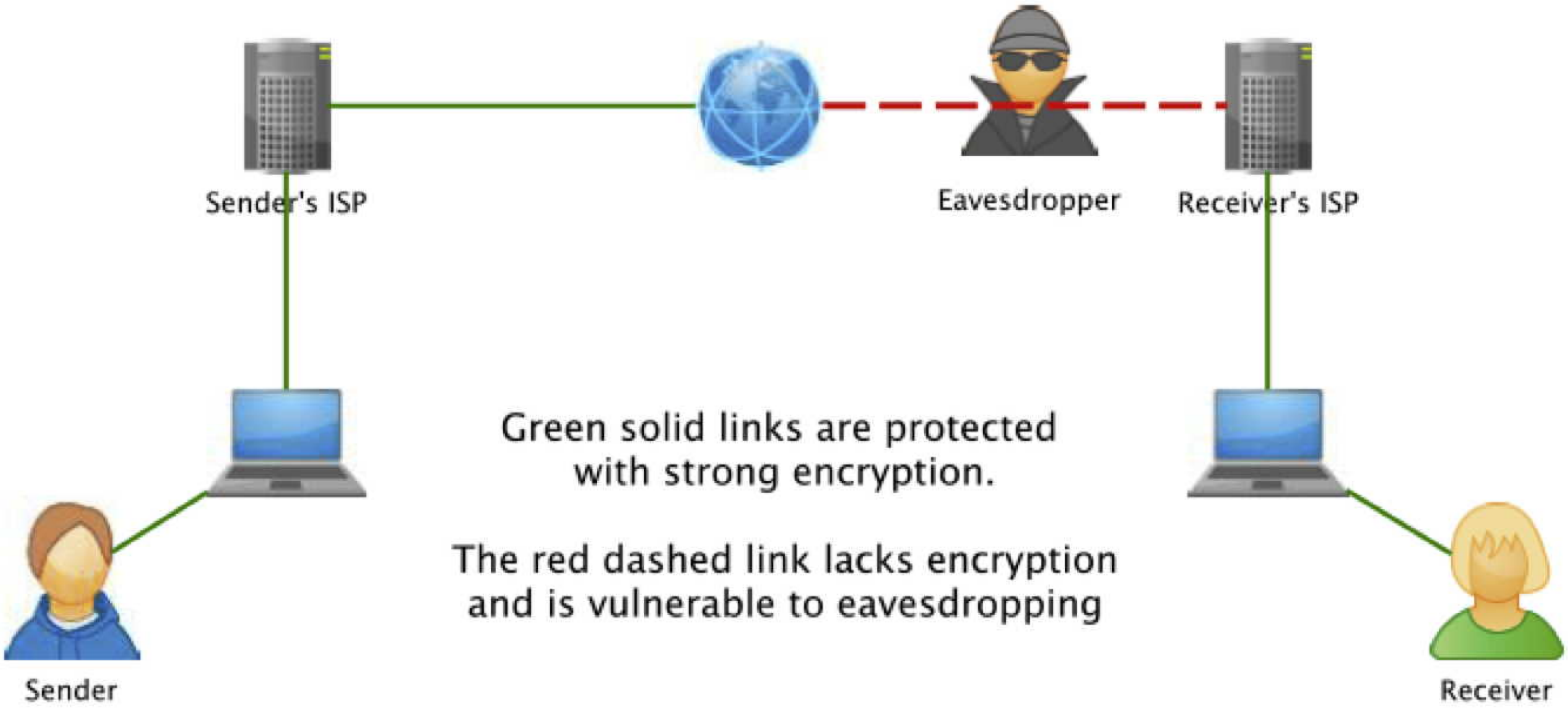
  *The IESG has concluded that **this document violates IETF procedures about pervasive monitoring (RFC 7258) and should therefore not be published without IETF review and IESG approval**. [post continues]*

X. Other Anti-Pervasive Monitoring Work Areas:

End-To-End Encryption

__Introduction:__ A typical message will routinely pass through many systems and networks on its way from sender to recipient. If that message is NOT protected by *end-to-end encryption*, the privacy of that message depends on the protection the message receives from EACH individual system or network through which it passes. If any ONE of those systems or networks is untrustworthy, the message may no longer be confidential.

IF EVEN ONE LINK OR SYSTEM IS INSECURE, CONFIDENTIALITY CAN BE LOST



Green solid links are protected with strong encryption.

The red dashed link lacks encryption and is vulnerable to eavesdropping

End-to-End Crypto Is Relatively Little Used

- Has use of end-to-end crypto made the Internet "go dark?" No.
- Usage statistics are scarce, however end-to-end cryptography (e.g., encryption with PGP/GPG or S/MIME) is probably used for no more than 1/100th of 1% of all messages currently traversing the Internet. That is, if we assume a daily traffic volume of 300 billion email messages a day, 1/100th of that 1% would be just 30 million end-to-end encrypted messages a day (even that estimate is likely wildly optimistic)
- At that level of market penetration, end-to-end encryption isn't a particularly significant technology relative to opportunistic encryption (given that opportunistic encryption is currently protecting over 85% of all outbound traffic at Google, albeit not end-to-end), and traffic analytic approaches handle E2E encrypted messages or unencrypted messages alike.

Nonetheless, M3AAWG Has Done Training For Both S/MIME and PGP/GPG

- *Client Certs and S/MIME Signing and Encryption: An Introduction* Feb 20, 2012, M^{3}AAWG 24, San Francisco https://www.stsauver.com/joe/maawg24/maawg24.pdf

- *Pretty Good Privacy (PGP) & GNU Privacy Guard (GPG): Just Enough Training To Make You Dangerous*, June 8, 2015, M^{3}AAWG 34, Dublin, Ireland https://www.stsauver.com/joe/pgp-tutorial/pgp-tutorial.pdf

- Additional trainings and a broader selection of software integrations may help uptake of PGP/GPG and S/MIME by average Internet user populations.

XI. "The Potential Role of DANE TLSA in Securing MTA-to-MTA Flows"

DANE TLSA

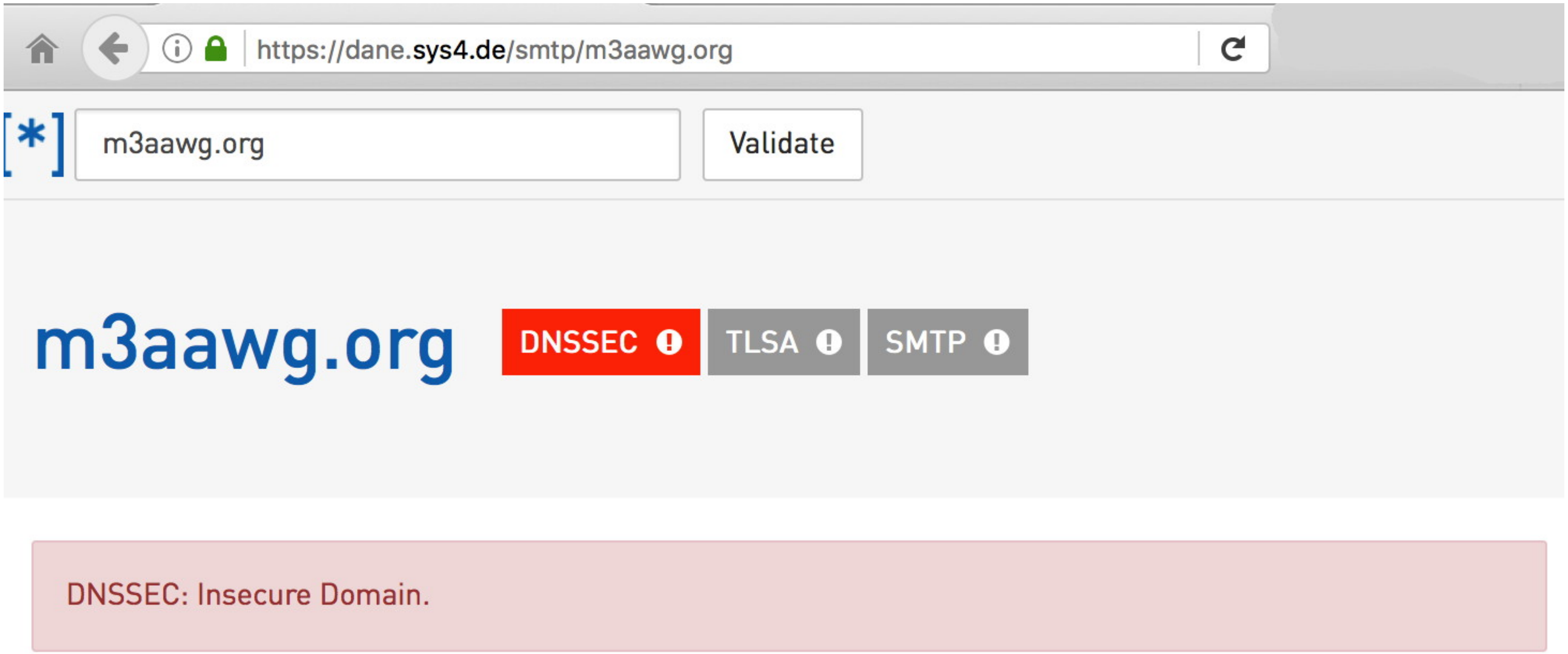
- DANE TLSA has the potential to deter 3rd parties from using improperly-obtained globally-trusted certificates, however it depends on sites having:
  - DNSSEC
  - An MTA which supports DANE

- Deployment of DANE TLSA has been slow to date. You can check sites of interest using the tester that's available at:

  https://dane.sys4.de/

  Example of a site that **does** do DANE: ietf.org
  Example of a site that does DNSSEC, but **not** DANE: icann.org
  Example of sites that do neither: [lots of those, sadly!]

A Sample Report



https://dane.sys4.de/smtp/m3aawg.org

m3aawg.org

DNSSEC: Insecure Domain.

Suggestion (in the spirit of eating one's dog's own food):

M3AAWG should sign its own zone, and validate the DNSSEC signatures of others. M3AAWG should also do DANE.

XII. Authentication, Anonymity, And Identity Management (AT LAST!)

What Is Identity Management?

- The Identity Mgmt SIG's first document (now in final editing) was around **password management**
- **Passwords are part of Identity Management, but there's a whole lot more, too.** See "Identity Management--Background Concepts, Goals and Jargon," https://www.stsauver.com/joe/maawg-id-mgmt/ (dating from M3AAWG Austria when Snowden's leaks hit)
- Just to mention a few areas touched by Identity Management:
  – The **user provisioning process** (cradle-to-grave): identity proofing, initial credential creation and distribution, etc., all the way to account deletion
  – **Levels of assurance** (LOA) and **multifactor authentication**
  – **Federated auth, attribute management, and privacy-preserving auth**
  – Working to **recover from account compromises**
  – **Device-based authentication** (for IOT devices, cable modems, etc.)
- See also: http://csrc.nist.gov/projects/iden_ac.html and http://www.nist.gov/nstic/

Why Is Identity Management Important?

- Users and companies alike rely on identity management to **protect access to services** (e.g., email msgs. / other private info).
- Identities allow the Internet to hold users (and their providers) **accountable for online abuse, such as spam and phishing.**
- Identity management is one of those infrastructural bits that can either enable Internet businesses to thrive, or (if done badly) can **tie companies up in knots** as they struggle to manage accounts.
- **Users are the "denominator"** for how many the Internet's most influential organizations get valued. For example, the recent $26.2 billion dollar offer by Microsoft for LinkedIn was calculated at **"$220 for each of LinkedIn's monthly active users"** by the NY Times. [See http://www.nytimes.com/2016/06/14/business/dealbook/for-microsoft-linkedin-deal-could-be-a-26-2-billion-time-machine.html]
- Online identities turn out to **also be critical to pervasive monitoring.**

Identity Management And Pervasive Monitoring

- **Pervasive monitoring fundamentally seeks to understand who's doing what online.** (Note particularly the **"who"** in that sentence)
- Defending against pervasive monitoring might include:
  -- securing the contents of communications with **encryption**
  -- limiting **traffic analysis** attacks by technically controlling access to usable metadata (info about "who's talking to whom," as gathered from network flow data or pen registers/trap and trace devices, etc.)
  -- procedural measures, such as requiring a **court order for subscriber registration or billing information**
- Some might assume that ID Management may be at odds with M3AAWG's anti-Pervasive Monitoring Work – but it's not.
- The two can actually COMPLIMENT each other.

"Who" (Identity Mgmt) And "What" (Traffic Inspection) May Represent "Compensating Controls"

- Some vendors are now offering "transparent outbound email filtering" solutions that inspect traffic to help detect spam, phishing, malware, etc. (This may even include MITM'ing TLS-protected traffic, proof that we're not doing strict TLS certificate checking for SMTP connections very well)
- **Along the way, I happened to think that this is a bit like the millimeter wave scanners passengers go through at the airport. If you're known ("well identified") to TSA (e.g., the "Precheck" program) you won't have to go through "inspection" (the millimeter wave scanners).**
- Because many ISP or hosting provider might not know and trust parties emitting email, the ISP/hosting provider necessarily shifts from focusing on WHO is emitting email to WHAT sort of email they're emitting.
- **Is it time to consider something like "TSA Precheck" for senders?** That is, if I know and trust a sender, can providers become comfortable with allowing those senders to skip transparent outbound email filtering?

Folks Don't Always Need To Know Who You Are

- Identity management **SHOULD NOT** mean "whenever someone's on, they should always be identified."

- **Contrast two perspectives...**

"China Is Requiring People to Register Real Names for Some Internet Services"

"BEIJING—China announced sweeping new regulations **requiring users of an array of Internet services to register with their real names** and avoid spreading content that challenges national interests.

"[...] **Chinese Internet companies face significant added operational costs associated with identifying users, verifying their information and tracking their activities, analysts said.** With regulators offering few details about implementation, it is possible companies will again try to resist, though analysts said **the government was not likely to give up on real-name registration.**"

See http://www.wsj.com/articles/china-to-enforce-real-name-registration-for-internet-users-1423033973 (Feb 4th, 2015)

"National Strategy For Trusted Identities In Cyberspace"

"Just as there is a need for methods to reliably authenticate individuals, there are many Internet transactions for which ***identification and authentication is not needed, or the information needed is limited. It is vital to maintain the capacity for anonymity and pseudonymity in Internet transactions in order to enhance individuals' privacy and otherwise support civil liberties****. Nonetheless, individuals and businesses need to be able to check each other's identity for certain types of sensitive transactions, such as online banking or accessing electronic health records."*

https://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf [emphasis added]

Consequences If Privacy and Identity Are Handled Poorly: People Will Opt Out

Nearly one in **two Internet** ***users say privacy and security concerns have now stopped them from doing basic things online — such as posting to social networks, expressing opinions in forums or even buying things from websites, according to a new government survey released Friday.*** *[e.g., May 13, 2016]*

This chilling effect, pulled out of a survey of ***41,000 U.S. households*** *who use the Internet, show the insecurity of the Web is beginning to have consequences that stretch beyond the direct fall-out of an individual losing personal data in breach. The research suggests some consumers are reaching a tipping point where they feel they can no longer trust using the Internet for everyday activities.* * * *

The new NTIA data suggests a significant number of Americans have embraced at least one strategy: Opting out of online activities."

That trend could have major consequences for banks, online retailers, and the broader Internet economy.

"Why a staggering number of Americans have stopped using the Internet the way they used to," https://www.washingtonpost.com/news/the-switch/wp/2016/05/13/new-government-data-shows-a-staggering-number-of-americans-have-stopped-basic-online-activities/ [emphasis added]

If Identities Cannot Be Protected, People May Also See Serious Personal Consequences

A Chinese reporter who was sentenced to prison in 2005 […] Shi Tao had been released on 23 August [2013], 15 months before the end of his sentence […]

Shi was arrested in 2004 and sentenced to prison the following year on charges of disclosing state secrets. He had sent details of a government memo about restrictions on news coverage of the Tiananmen Square massacre anniversary to a human rights forum in the United States […]

[The email provider] based in Sunnyvale, California, [had] said it was obligated to comply with Chinese government demands for information. […]

See http://tinyurl.com/ztwwvj2

Degrees of Online Identification

- Many sites may not need to know "everything."
- For example, if I'm a faculty member simply interested in accessing an online academic database that my institution has licensed, all that needs to be established is that I am a faculty member from an authorized institution. My full name, email address, faculty ID number, and so forth, don't need to be shared with the database vendor.
- **Federated authentication,** one of the topics that the M3AAWG Identity Management SIG will be working on this year, allows the user and the relying party to agree on the release of just a **subset of attributes.**
- By limiting the attributes that are shared to only the bare minimum that's necessary, opportunities for user attributable pervasive monitoring are reduced.

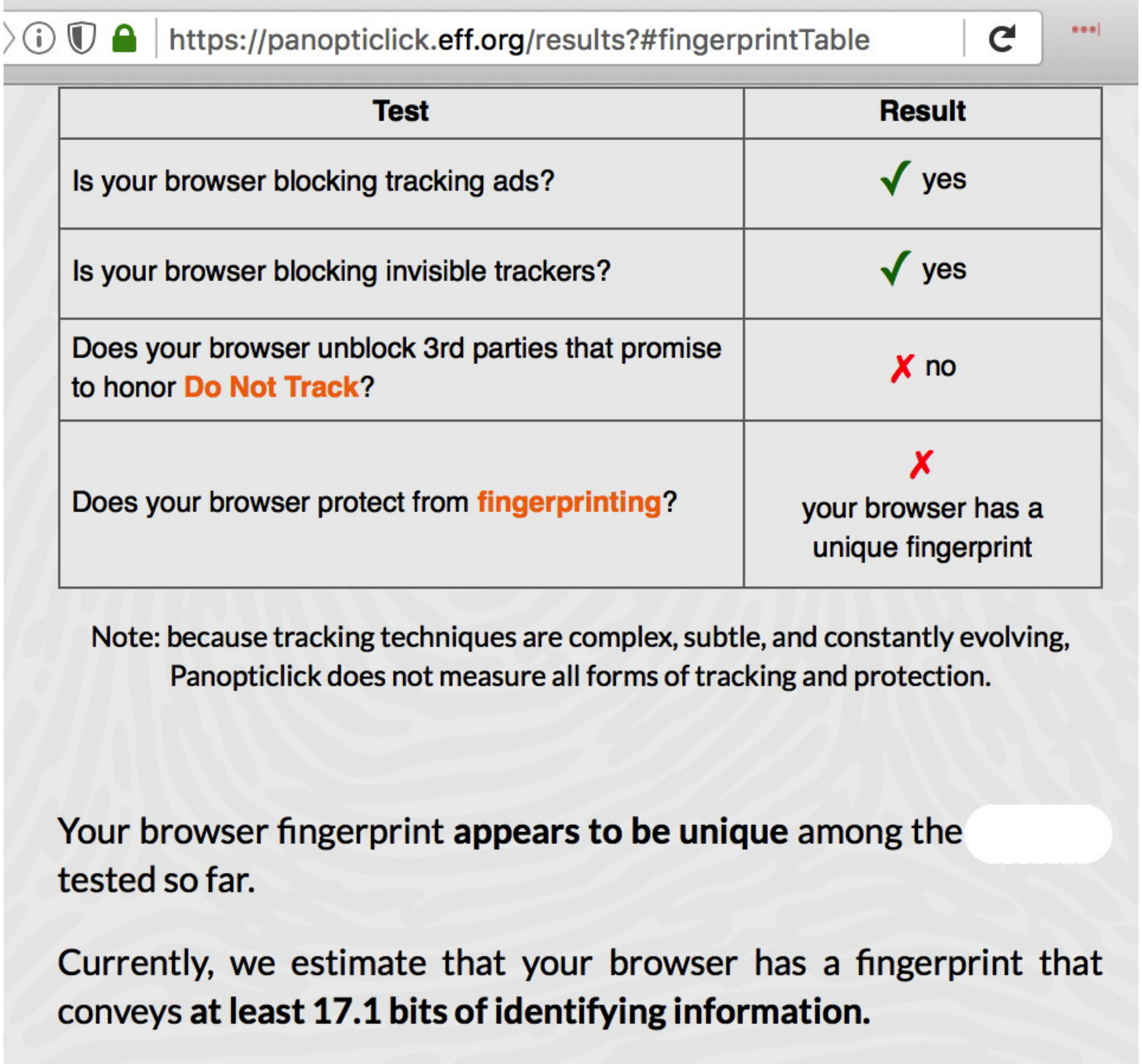
Another Example: "Differential Privacy"

- Differential privacy is an identity management topic that hit the mainstream media this week courtesy of Apple's WWDC. (See https://www.wired.com/2016/06/apples-differential-privacy-collecting-data/):

  > *Differential privacy, translated from Apple-speak, is the statistical science of trying to learn as much as possible about a group while learning as little as possible about any individual in it. With differential privacy, Apple can collect and store its users' data in a format that lets it glean useful notions about what people do, say, like and want. But it can't extract anything about a single, specific one of those people that might represent a privacy violation. And neither, in theory, could hackers or intelligence agencies.*

- Many devices DO currently leak personally identifying information…

Does Your System/Browser Identify You?



https://panopticlick.eff.org/results?#fingerprintTable

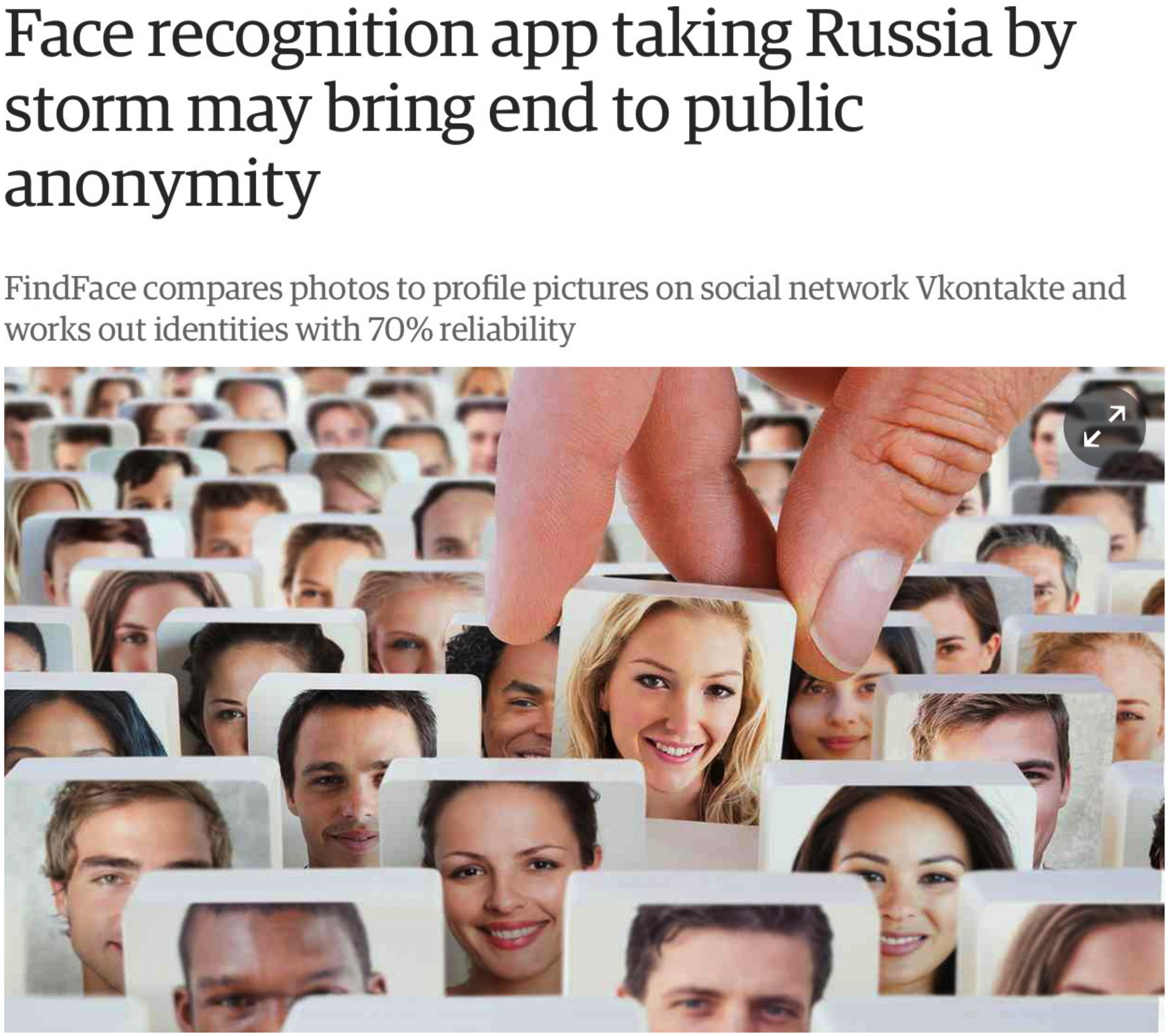
Test	Result
Is your browser blocking tracking ads?	✓ yes
Is your browser blocking invisible trackers?	✓ yes
Does your browser unblock 3rd parties that promise to honor Do Not Track?	✗ no
Does your browser protect from fingerprinting?	✗ your browser has a unique fingerprint

Note: because tracking techniques are complex, subtle, and constantly evolving, Panopticlick does not measure all forms of tracking and protection.

Your browser fingerprint **appears to be unique** among the tested so far.

Currently, we estimate that your browser has a fingerprint that conveys **at least 17.1 bits of identifying information.**

Loss of Anonymity May Be "Inescapable" In Some Cases



Face recognition app taking Russia by storm may bring end to public anonymity

FindFace compares photos to profile pictures on social network Vkontakte and works out identities with 70% reliability

https://www.theguardian.com/technology/2016/may/17/findface-face-recognition-app-end-public-anonymity-vkontakte

XIII. Conclusion

Conclusion

- You've now had a bit of a "whirlwind tour" of some of M^{3}AAWG's work against Pervasive Monitoring and how it interacts with the work of M^{3}AAWG's Identity Management SIG.
- You now know why we're STILL working, and working hard, in this particular area: pervasive monitoring has NOT been conclusively "dealt with" as a concern.
- You've learned that there are M^{3}AAWG videos you can watch, if you'd like to learn more, plus pointers to some M^{3}AAWG-approved recommendations and crypto training materials.
- You've also learned about M^{3}AAWG Identity Management SIG's work. Perhaps this is work you'd like to become involved with, too?
- Thanks for the chance to talk!
- **If we still have time, are there any questions?**