

The Enduring Challenges of Traffic Analysis

M3AAWG 34

11:00-12:00, Thursday, June 11, 2015

Dublin, Ireland

Joe St Sauver, Ph.D. (stsauver@fsi.io)

M3AAWG Senior Technical Advisor

Distributed System Scientist

Farsight Security, Inc.

<https://www.stsauver.com/joe/dublin-traffic-analysis/>

Disclaimer: all opinions expressed are the author's.

I. Introduction

TODAY'S "ASK"

- **I'm here to ask for your HELP**
- **Law-abiding users of the Internet need technical solutions that will let them effectively avoid pervasive metadata collection and traffic analysis, regardless of who may be targeting them. (Yes, I know this is hard)**
- At the same time, ISPs and criminal LEOs need to be able to continue to use traffic analytic techniques for appropriate uses:
 - these techniques are needed by providers for appropriate self-defense and for anti-abuse purposes, and
 - by LEOs for narrowly-targeted and court-approved lawful intercepts needed to combat abusive online criminal activity.

Tensions Between Those Two Main Objectives

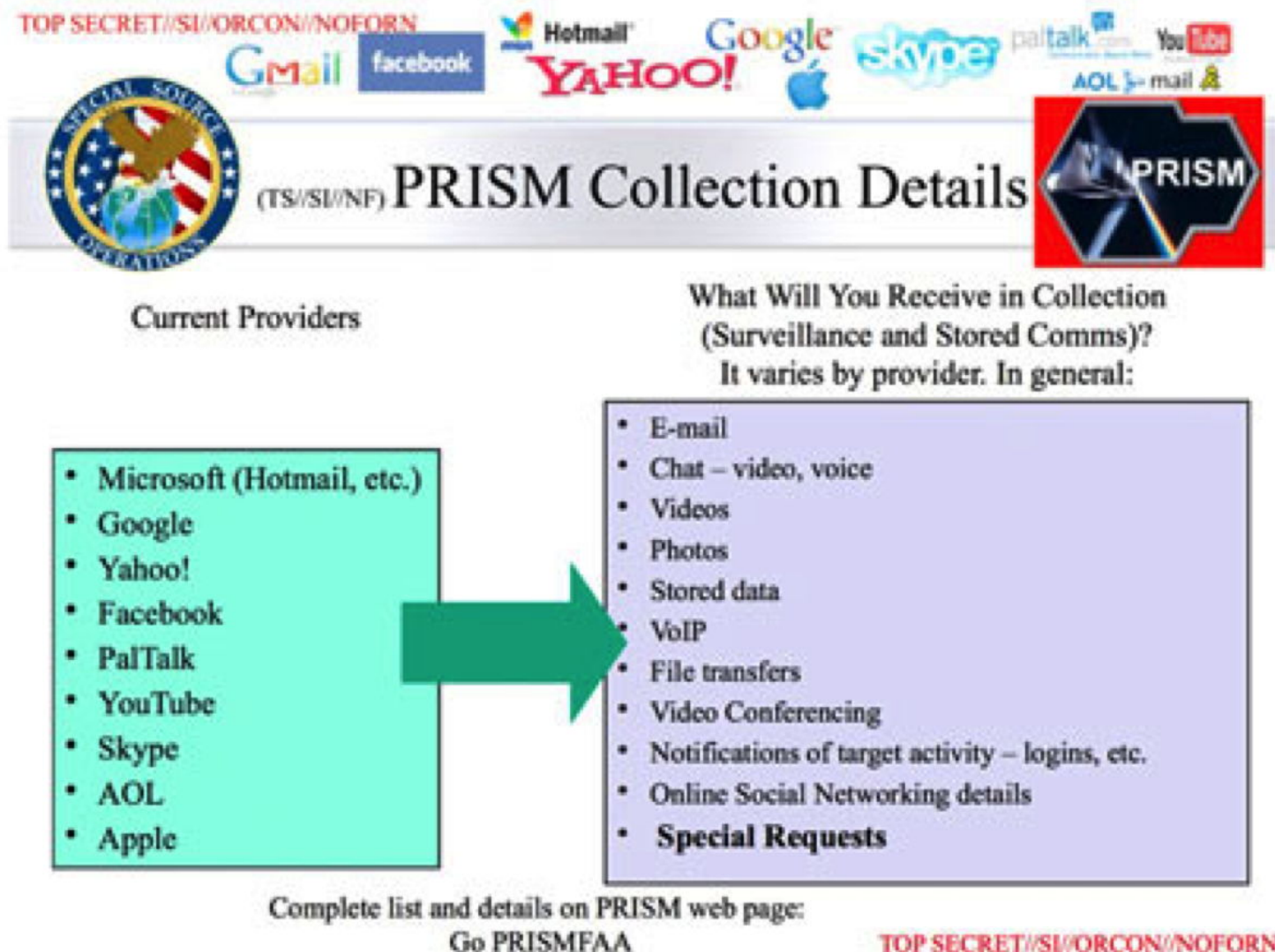
- Let me be very candid that I unquestionably get that there is definite tension between those two objectives:
 - on the one hand, I want help making routine Internet traffic robust *against* traffic analysis for pervasive monitoring (hard, in and of itself);
 - on the other hand, I also want the community to work on being better able to *continue* to perform, or even to *better* perform, carefully targeted traffic analyses (also hard, in and of itself)
- Asking for BOTH of those things together? REALLY hard.
- This is, in many ways, directly parallel to what we see in the cryptographic world.

II. "Sneaking Up On Traffic Analysis"
By Starting With The "Easy" Issue First:
Countering Eavesdropping With Encryption

Detering Eavesdropping Through Use of Encryption

- For a long time, most email traffic (and most web traffic) on the Internet has been **unencrypted** and vulnerable to **eavesdropping**.
- **Email end-to-end privacy tools** (such as S/MIME and GNU PrivacyGuard) have long been widely available, but generally have been "**too tricky**" for most "mere mortals" to routinely use (but we did do a PGP training here for M3AAWG this Monday)
- SSL/TLS is another cryptographic tool, but for a long time it was pretty badly technically flawed, and normally it was something that was only used to protect credit card numbers & login information and for a few other very limited use cases.
- ***Bottom line:* most Internet traffic content was broadly vulnerable to passive network monitoring.**
- Many of us *suspected* that monitoring of unencrypted Internet traffic was taking place, but few knew for sure until June 2013.

Snowden and The PRISM Program Disclosures, Now Two Years Ago...



Users Suddenly KNEW That The NSA Was Listening; Providers Took Steps to Harden Their Services

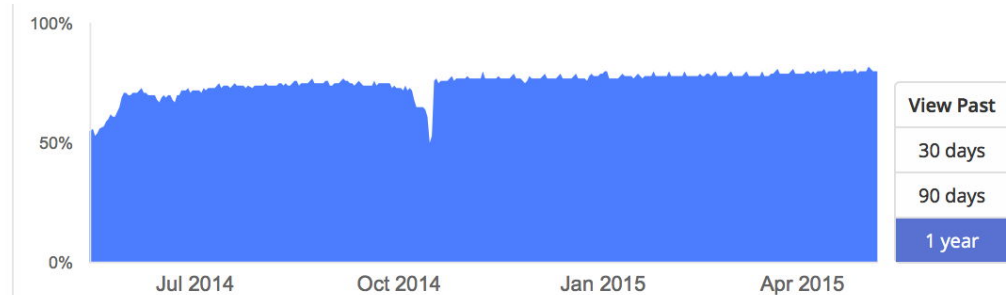
- Once users knew that the contents of their communications were being monitored, they wanted protection from **eavesdropping**.
- **Encryption** became an exceptionally "hot" topic and great progress was made in finding and fixing flaws, and in expanding cryptographic protections, particularly for email.
- A prime example of this can be seen in Google's "Gmail Email Transparency Report" shown on the next slide.
- **Virtually all outbound email from Gmail to top destinations worldwide is now encrypted in transit.**

How much email was encrypted in transit?

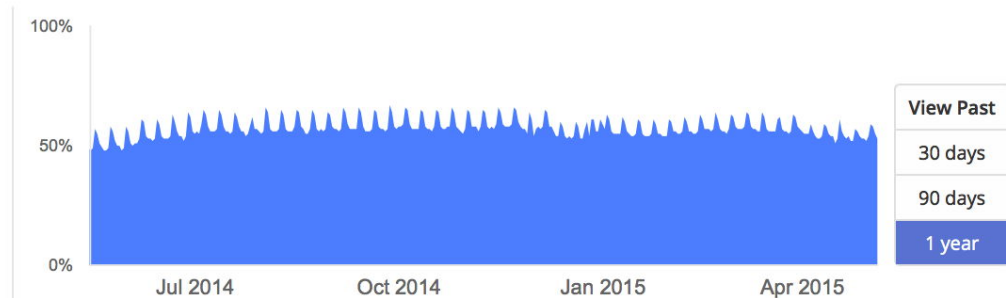
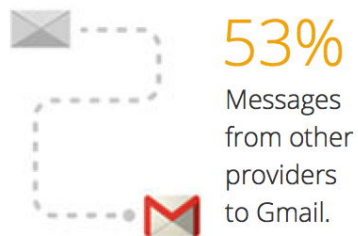


Generally speaking, use of encryption in transit increases over time, as more providers enable and maintain their support. Factors such as varying volumes of email may explain other fluctuations.

Outbound



Inbound





Who supports encryption in transit

Below is the percentage of email encrypted for the top domains in terms of volume of email to and from Gmail, in alphabetical order.

Select Region World ⓘ

Top domains by region, inbound

Domain	%	
From: amazon.{...} via amazonses.com	99.9%	ⓘ
From: amazonses.com	99.9%	ⓘ
From: constantcontact.com	> 95%	ⓘ
From: facebookmail.com via facebook.com	99.99%	ⓘ
From: linkedin.com	99%	ⓘ
From: mcdlv.net	0%	ⓘ
From: mcsv.net	0%	ⓘ
From: sailthru.com	> 95%	ⓘ
From: twitter.com	99.99%	ⓘ
From: yahoo.{...}	99%	ⓘ

These are both Mailchimp domain names

Top domains by region, outbound

Domain	%	
To: aol.com	99.99%	ⓘ
To: comcast.net	100%	ⓘ
To: craigslist.org	100%	ⓘ
To: hotmail.{...}	100%	ⓘ
To: live.{...} via hotmail.{...}	100%	ⓘ
To: mail.ru	99.99%	ⓘ
To: msn.com via hotmail.{...}	100%	ⓘ
To: orange.fr	100%	ⓘ
To: outlook.com via hotmail.{...}	100%	ⓘ
To: yahoo.{...} via yahoodns.net	100%	ⓘ

Tuesday, May 5, 2015

Who supports encryption in transit



Below is the percentage of email encrypted for the top domains in terms of volume of email to and from Gmail, in alphabetical order.

Select Region

Europe



Top domains by region, inbound

Domain	%	
From: adsender.us	0%	
From: contactlab.it	0%	
From: ebay.{...} via emarsys.net	99.99%	
From: emarsys.net	99.9%	
From: emsmtp.com	100%	
From: getresponse.com	< 1%	
From: github.com via github.net	100%	
From: privalia.com	< 1%	
From: twoomail.com via netlogmail.com	0%	
From: venteprivee.com	0%	

Top domains by region, outbound

Domain	%	
To: free.fr	< 50%	
To: gmx.de via gmx.net	100%	
To: libero.it	100%	
To: mail.ru	99.99%	
To: orange.fr	100%	
To: seznam.cz	< 1%	
To: wanadoo.fr via orange.fr	100%	
To: web.de	100%	
To: wp.pl	100%	
To: yandex.ru	100%	

Tuesday, May 5, 2015

All Those 100%'s and 99.9%'s?

Those Numbers Represent A Bit of a Miracle...

- Few security technologies have *ever* successfully deployed 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, too...
- **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 fully 80% in just a year. That's AWESOME.

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

- *"Going dark" is "short hand" for "law enforcement agencies will no longer be able to conduct court-ordered lawful interceptions."* It is 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 October 16th, 2014).
- You might think the preceding data are an example of "going dark," what with 80% of outbound Gmail now encrypted in transit. It isn't. That 80% 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*.
- **Q:** So why bother encrypting in transit? **A:** 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 on a wholesale basis.

Perfect Example of "Threading The Needle"?

- This is, perhaps, a perfect example of "threading the needle" or balancing apparently conflicting objectives:
 - widespread use of encryption during transit deters indiscriminant "dragnet" surveillance efforts on the network
 - legitimate carefully-targeted and court-authorized access has been preserved (at least as long as users don't choose to use end-to-end encryption, such as PGP/GPG). That is, law enforcement can still get access with appropriate paperwork for mail stored on email providers' mail servers, if they have probable cause.
- **Oh, and average users don't need to become crypto experts to get reasonable protection.**

More Cryptographic Work Remains To Be Done

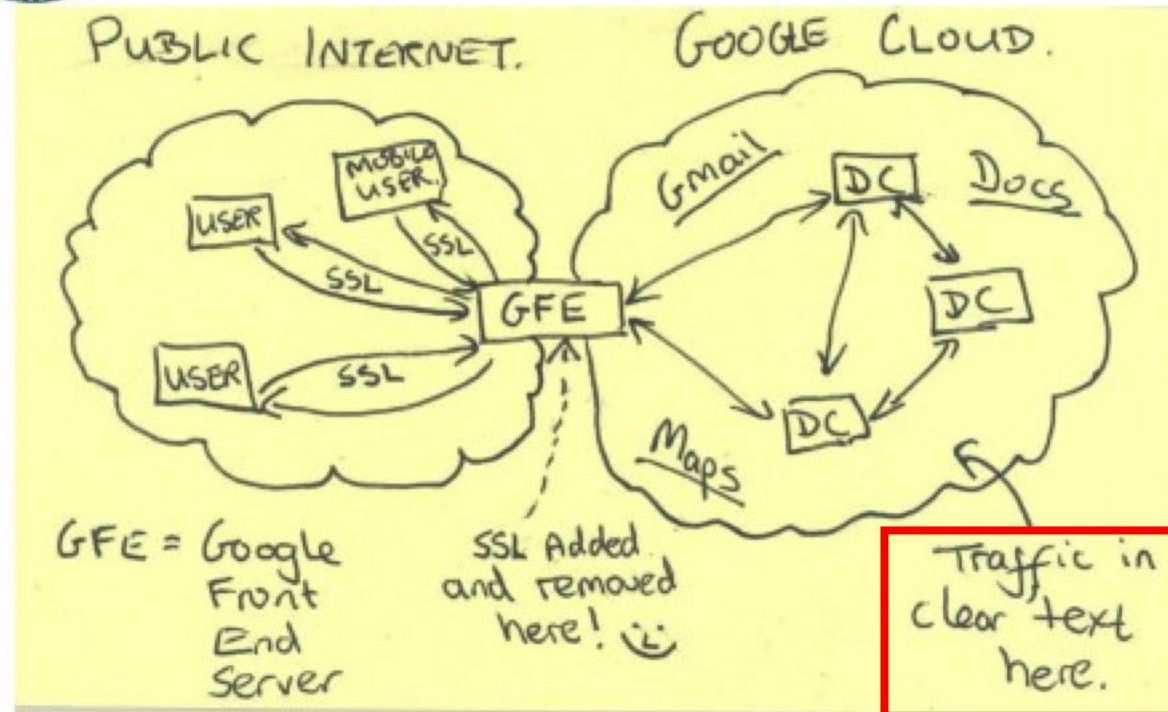
- At least **20% of all email outbound remains unencrypted** in transit even from Gmail. We need to keep whittling away at that.
- The protection of email with STARTTLS is still imperfect. We need to keep working on helping sites move to **stronger crypto** deployments. We need to **find and patch flaws in OpenSSL, GNUTLS and other crypto implementations** (nice example? The "Frankencerts" paper from Univ of Texas, see https://www.cs.utexas.edu/~shmat/shmat_oak14.pdf)
- We need **stronger keys** (AES 128→256, RSA 2048→4096 bit)
- We need to deploy **elliptic curve** cryptography using cryptographically **safe curves!** [see <http://safecurves.cr.yp.to/>]
- We need to work on deployment of **Layer 1/2/3 crypto**.
- And we need **end-to-end (not just hop-by-hop) crypto usage**.
- We should also look at **hardening ssh**, too.

Remember This Revelation About "MUSCULAR"?

TOP SECRET//SI//NOFORN



Current Efforts - Google



TOP SECRET//SI//NOFORN

(Red box added by JES)

Layer 1/2/3 Crypto

- Most security architectures endeavor to deploy **security in depth**. Deploying overlapping layers of protection means that even if there's a flaw or compromise in one layer, redundant protection at other layers still delivers protection.
- Much of the focus to-date has been at the application layer, particularly on **SSL/TLS**.
- The time has come to remember that crypto can also be done at other layers, too. Some might assume that this means doing **IPsec in tunnel mode at layer three**, and you could certainly try that, but it would be painful if possible at all, particularly at **major-provider-and-carrier-relevant speeds (10Gbps or 100Gbps)**.
- My suggestion is that providers should probably be looking at pervasively enabling encryption in **optical transport systems at layer one**, AND in Ethernet switching infrastructures at **layer two (IEEE 802.1AE, aka "MACsec" or "LinkSec")**, instead.

L1/L2/L3 Crypto Protection Is Getting Deployed

- "Google encrypts data amid backlash against NSA spying,"
9/6/2013, http://www.washingtonpost.com/business/technology/google-encrypts-data-amid-backlash-against-nsa-spying/2013/09/06/9acc3c20-1722-11e3-a2ec-b47e45e6f8ef_story.html
"Google is racing to encrypt the torrents of information that flow among its data centers around the world in a bid to thwart snooping by the NSA and the intelligence agencies of foreign governments, company officials said Friday."
- <http://www.zdnet.com/article/microsoft-to-encrypt-network-traffic-amid-nsa-datacenter-link-tapping-claims/>
- <http://www.zdnet.com/article/yahoo-bolsters-encryption-after-nsa-datacenter-link-tapping/>
- Pointer to a document discussing some L1/L2/L3 crypto options:
<https://www.stsauver.com/joe/protecting-high-speed-links.docx>

Time To Renew Efforts on End-to-End Crypto, Too

- In the case of email, this might mean things like S/MIME and GNU PrivacyGuard, but I'd actually suggest that the community NOT focus on email for end-to-end crypto, at least not at first.
- **I think the "low hanging fruit" for end-to-end crypto is in the area of voice and instant messaging on smartphones/tablets.**
- I'm sure you've seen some of the voice and IM crypto options that have hit the market over the last few years (including solutions from <https://silentcircle.com/> and <https://whispersystems.org/>), but there are literally dozens of other options to also consider, including products from companies located *outside* the U.S. (such as <https://www.seecrypt.com/en/>). See more products at: <https://www.stsauver.com/joe/non-email-crypto.docx>
- The biggest challenge we face in encouraging adoption of encrypted voice and IM is the **lack of interoperability**: most solutions are proprietary and can't talk to other vendors' products.

Hardening ssh

- A final example of an area where additional cryptographic work is required is ssh. People have spent lots of time and effort hardening SSL/TLS, but ssh has largely been overlooked.
- ssh is used at many sites for mission-critical purposes, including access to core routers and essential servers, but ssh is often not configured to be as operationally strong as it can be.
- Fortunately, people are beginning to work on improving this, too.

See for example the recommendations in "Secure Secure Shell"
<https://stribika.github.io/2015/01/04/secure-secure-shell.html>

III. Metadata

Bringing This Talk Back Around to Metadata and Traffic Analysis

- As discussed in the preceding section of this talk, we've made *huge strides* when it comes to deploying encryption to deter pervasive eavesdropping on traffic content at Internet scale.
- Unfortunately, the Internet has made virtually **NO PROGRESS** when it comes to dealing with its metadata exposures, and when it comes to dealing with traffic analysis attacks.
- In fact, most people don't even understand what metadata is, or what traffic analysis is, or why they're major issues worthy of our attention. As long as people don't understand metadata and traffic analysis, the challenges they pose will never get addressed.

The *"It's Only Metadata"* Myth

- Quoting John Naughton of the Open University from July 2013:

Over the past two weeks, I have lost count of the number of officials and government ministers who, when challenged about internet surveillance by GCHQ and the NSA, try to reassure their citizens by saying that the spooks are "only" collecting metadata, not "content".

"The NSA/GCHQ metadata reassurances are breathtakingly cynical," www.theguardian.com/technology/2013/jul/07/nsa-gchq-metadata-reassurances

- **Let me be clear: metadata can convey a LOT of information.**

What Is Metadata: It's "Data About Data"

- Most every photo taken by a smart phone has metadata by default:
 - *what camera/smartphone was used?* (brand, model number, etc)
 - *when was the photo taken?* (date and time)
 - *where was the photo taken?* (cameras include GPS receivers)
 - *how was the camera configured?* (shutter speed, aperture, etc.)This data is routinely helpful to photographers.

- **It can *also* be key to criminal investigations.** An example:
<http://www.smh.com.au/technology/technology-news/hacking-cases-body-of-evidence-20120411-1wsbh.html> (a taunting photo supplied by a computer intruder contained GPS metadata, metadata which allowed identification and arrest of that intruder)
- **Or for military operations:** "American airstrike obliterates ISIS stronghold after 'moron' reveals its location in a SELFIE,"
<http://www.mirror.co.uk/news/technology-science/technology/american-airstrike-obliterates-isis-stronghold-5821711>

Metadata Isn't Just a "Photographic Thing"

- Metadata is something that exists for **most digital objects**, including:
 - Network traffic flows
 - Email messages
 - Telephone calls
 - etc.

What Metadata Is Normally Available For Network Flow-based Traffic Analyses?

- "Source" and "destination" IP addresses and corresponding port numbers
- Traffic start and stop times and traffic volume in octets
- Other technical traffic characteristics not related to message content (for example, packet type, TCP flags, ASNs, etc.)
- We may have this information for each traffic flow, or just for some sampled subset of flows (perhaps 1 in 100, or 1 in 1000 flows, etc.)

Do Network Traffic Sources/Destinations Map Closely To Individuals? *Sometimes...*

- For example, a static IP address may be persistently used by just one person. The identity of that user can often be determined by issuing paperwork to the party responsible for that IP range, or through use of other techniques.
- Other static IPs may be for servers shared by many users, as is the case on low-cost shared web servers.
- Addresses may be multiplexed across multiple users, either:
 - shared at the same time (e.g., NAT/PAT)
 - or serially shared (DHCP-assigned dynamic addresses).Those cases are harder to directly attribute -- typically only the operator of the firewall doing the NAT/PAT translation, or the operator of the relevant DHCP server, can translate IP address+time stamp+port info to a definitive customer identity.
- *Hold onto this thought, you'll see this information again later.*

What Metadata is Available for Email?

- Metadata for email normally includes most (but **not all**) of the information in the email message "headers"
- Stuff that IS normally considered metadata includes the contents of the "From:", "To:", "CC:", and "Date:", headers, and the multiple "Received:" headers showing the message's routing info, among other headers.
- It normally does **NOT** include the contents of the email message's "**Subject: header**" (even though that too is a header), because it contains "information concerning the substance, purport, or meaning of that communication" (see, e.g., 18 U.S.C. 2510(8))
- Excellent discussion of the "Subject:" header in "The Content/Envelope Distinction in Internet Law," http://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID2478285_code705039.pdf?abstractid=1123304&mirid=1

Bulk Email Metadata HAS Been Collected

www.theguardian.com/world/2013/jun/27/nsa-data-mining-authorized-obama

NSA

Glenn
Greenwald on
security and
liberty

NSA collected US email records in bulk for more than two years under Obama

- Secret program launched by Bush continued 'until 2011'
- Fisa court renewed collection order every 90 days
- [Current NSA programs still mine US internet metadata](#)

**Glenn Greenwald
and Spencer
Ackerman**

Thursday 27 June 2013
11.20 EDT

 Comments
1,276



 The internet metadata collection program was halted in 2011 for 'operational and resource reasons'.
Photograph: Pablo Martinez Monsivais/AP Pablo Martinez Monsivais /AP

Telephony Metadata

- Metadata isn't limited to just Internet traffic or email. Metadata also exists in a telephony environment, too. In the telephony space, metadata is defined in the United States to be:

"comprehensive communications routing information, including but not limited to session identifying information (e.g., originating and terminating telephone number, International Mobile Subscriber Identity (IMSI) number, International Mobile station Equipment Identity (IMEI) number, etc.), trunk identifier, telephone calling card numbers, and time and duration of call.

Telephony metadata does not include the substantive content of any communication, as defined by 18 U.S.C. § 2510(8), or the name, address, or financial information of a subscriber or customer." (See for example <https://www.eff.org/files/2013/11/06/mooredeclexh.pdf>)

Telephony Metadata Has Been, And *Was Being*, Collected

- "Consistent with prior declassification decisions and in light of the significant and continuing public interest in the telephony metadata collection program, DNI James R. Clapper declassified the fact that the government filed an application with the FISC to reauthorize the existing program until **June 1, 2015**, and that the FISC issued an order approving the government's application. The Government sought renewal of this authority to and including **June 1, 2015** in order to align the expiration date of the requested order for this program with the June 1, 2015 sunset of Section 215 of the PATRIOT Act." [emphasis added]

<http://www.dni.gov/index.php/newsroom/press-releases/210-press-releases-2015/1176-joint-statement-by-the-department-of-justice-and-the-office-of-the-director-of-national-intelligence-on-the-declassification-of-renewal-of-collection-under-section-215-of-the-usa-patriot-act>

Why Not Collect "Full Traffic Contents?"

- There can be many reasons why "traffic content" isn't available to an analyst.
- Sometimes traffic may be protected with *strong encryption*. As a result, there may be no technical ability to access things like the body of email messages, or actual telephone conversations.
- Other times, there may be policy/administrative constraints that preclude access to traffic contents. For example, a US court may not have authorized a "Title III" "full contents" lawful intercept.
- Or perhaps storage is the binding constraint. Given fast links and a finite storage archive, there may be a trade off between:
 - a relatively brief archive of "full content" traffic vs.
 - a far longer window of summarized flow-level traffic.
- Sometimes "less" [detail] really does mean "more" [longer data retention window]

The UK's TEMPORA Program: 3 Days Full Contents; A Month of Metadata

TEMPORA are GCHQ's large-scale, Deep Dive deployments on Special Source access ([SSE](#)). Deep Dive XKeyscores work by promoting loose categories of traffic (e.g., all web, email, social, chat, EA, VPN, VoIP...) from the bearers feeding the system and block all the high-volume, low value traffic (e.g., P2P downloads). This usually equates to ~30% of the traffic on the bearer. We keep the full sessions for 3 working days and the metadata for 30 days for you to query, using all the functionality that Keyscore offers to slice and dice the data. The aim is to put the best 7.5% of our access into TEMPORA's, comprising a mix of Deep Dive Keyscores and promotion of data based on IP subnet or technology type from across the entire MVR. At the moment, users are able to access 46x10Gs of data via existing Internet Buffers.. This is a lot of data! Not only that, but the long-running [TINT](#) program and our initial 3-month operational trial of the CPC Internet Buffer (the first operational Internet Buffer to be deployed) show that every area of ops can get real benefit from this capability, especially for target discovery and target development. Internet Buffers are different from TINT in that the latter is purely an experimental, research environment whereas Internet Buffers can be used operationally for [EPR](#), [Effects](#), enabling [CNE](#) etc.

<https://www.aclu.org/files/natsec/nsa/20140722/Report%20on%20the%20NSA%27s%20access%20to%20TEMPORA.pdf>

Domestic Bulk Metadata Collection Has Been Going On For A Long Time – And Was Revealed – Long BEFORE Snowden Blew The Whistle in June 2013

- While everyone may assume that domestic bulk metadata first became a public issue with Edward Snowden's disclosure in June 2013, that's a misperception. Credit for raising the metadata issue should actually go to *USA Today*. On **May 10th, 2006** it published:

"NSA has massive database of Americans' phone calls,"

http://usatoday30.usatoday.com/news/washington/2006-05-10-nsa_x.htm

- That was **SEVEN YEARS** before Snowden's revelations.
- That was **FIVE YEARS** after bulk domestic collection of metadata began, shortly after the attacks of 9/11 occurred.
- See the description from a *New Yorker* article on the next slide...

The Vice-President's lawyer, David Addington, drafted language authorizing the N.S.A. to collect four streams of data without the FISA court's permission: the content of Internet and phone communications, and Internet and phone metadata. The White House secretly argued that Bush was allowed to circumvent the FISA law governing domestic surveillance thanks to the extraordinary power granted by Congress's resolution, on September 14th, declaring war against Al Qaeda. On October 4th, Bush signed the surveillance authorization. It became known inside the government as the P.S.P., the President's Surveillance Program. Tenet authorized an initial twenty-five million dollars to fund it. Hayden stored the document in his office safe.

Over the weekend of October 6, 2001, the three major telephone companies—A. T. & T., Verizon, and BellSouth, which for decades have had classified relationships with the N.S.A.—began providing wiretap recordings of N.S.A. targets. The content of e-mails followed shortly afterward. By November, a couple of weeks after the secret computer servers were delivered, phone and Internet metadata from the three phone companies began flowing to the N.S.A. servers over classified lines or on compact disks. Twenty N.S.A.

"Pen Register" & "Trap and Trace" Orders

- Traffic analytic approaches are, in fact, **strongly associated with telephony**. LEOs have used telephony "pen registers" and "trap and trace" techniques for a long time as part of their criminal investigations.
- A "pen register" records the *outgoing* calls made from a phone (in the old days of rotary pulse dialing, this meant literally tracing out the pulses made by the phone dial as it clicked around).
- "Trap and trace devices," on the other hand, focus on capturing the origin of *incoming* calls received by a phone.
- Normally BOTH pen register AND trap and trace data is collected, not just one OR the other.
- Even as investigations have moved away from telephony and toward Internet TCP/IP data, those old (and now unquestionably antiquated) terms have "stuck" (even if they're a mouthful).

The Other Side of the Coin:

Title III ("Full Content") Intercepts

- Pen registers and trap and trace devices do NOT provide access to message contents (normally you can't even use a pen register/trap and trace order get access to URLs, see http://www.justice.gov/usao/eousa/foia_reading_room/usam/title9/7mcrm.htm#9-7.500)
- **Title III intercepts**, on the other hand, provide the "**whole communication.**" For example, in a telephony context, you'd get to hear the whole conversation. In an Internet context, you'd get the contents of an email message, not just header information.
- Because of the invasiveness of a full content intercept, requests for full content intercepts were historically given strict scrutiny, and were hard to obtain. Onesie-twosie pen registers/trap and trace orders, however, were relatively easily obtained, in part because there was little judicial appreciation for their true power.

IV. Traffic Analysis

"You can observe a lot by just watching."

Yogi Bera

Metadata Drives Traffic Analysis

- So far we've been talking about metadata. That's the "what."
- Now let's talk about the "how," aka traffic analysis.

Traffic Sources and Destinations

Can Sometimes Be More Than Enough

- For example, if you observe an employee who works at a sensitive defense industrial site attempting to surreptitiously communicate with a representative of a foreign intelligence service, the exact details of what's being said are (to a first approximation) irrelevant.
- The simple fact that any such conversation is being held or attempted should be more than enough to send up a red flag (unless undertaking that communication was directed and approved at senior levels, etc.)

Ru-Roh, Scooby...



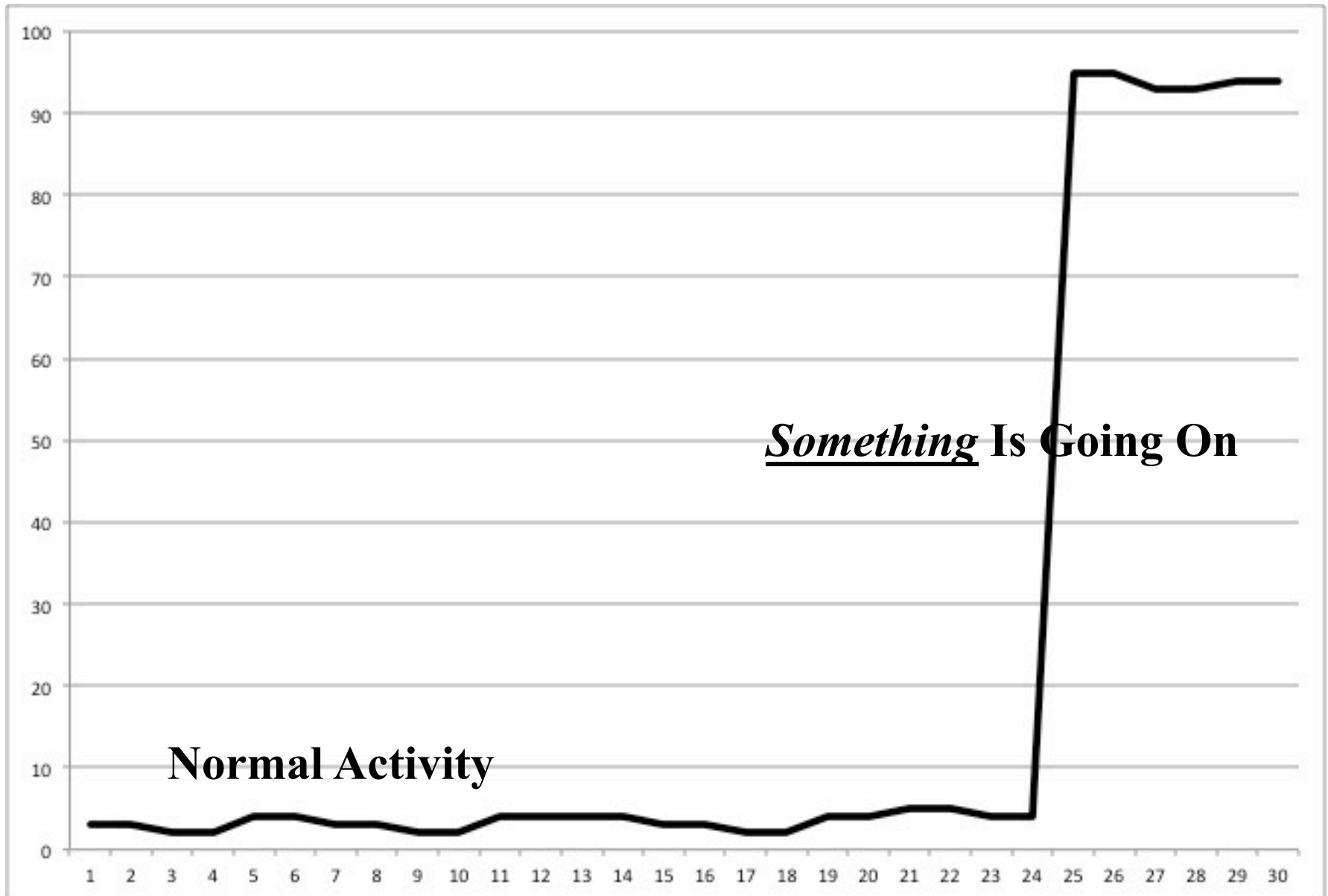
**US Government
Employee In
Sensitive Role**



**Representative
of A Foreign
Intelligence
Service**

Changes In Traffic Patterns Can Also Be Key

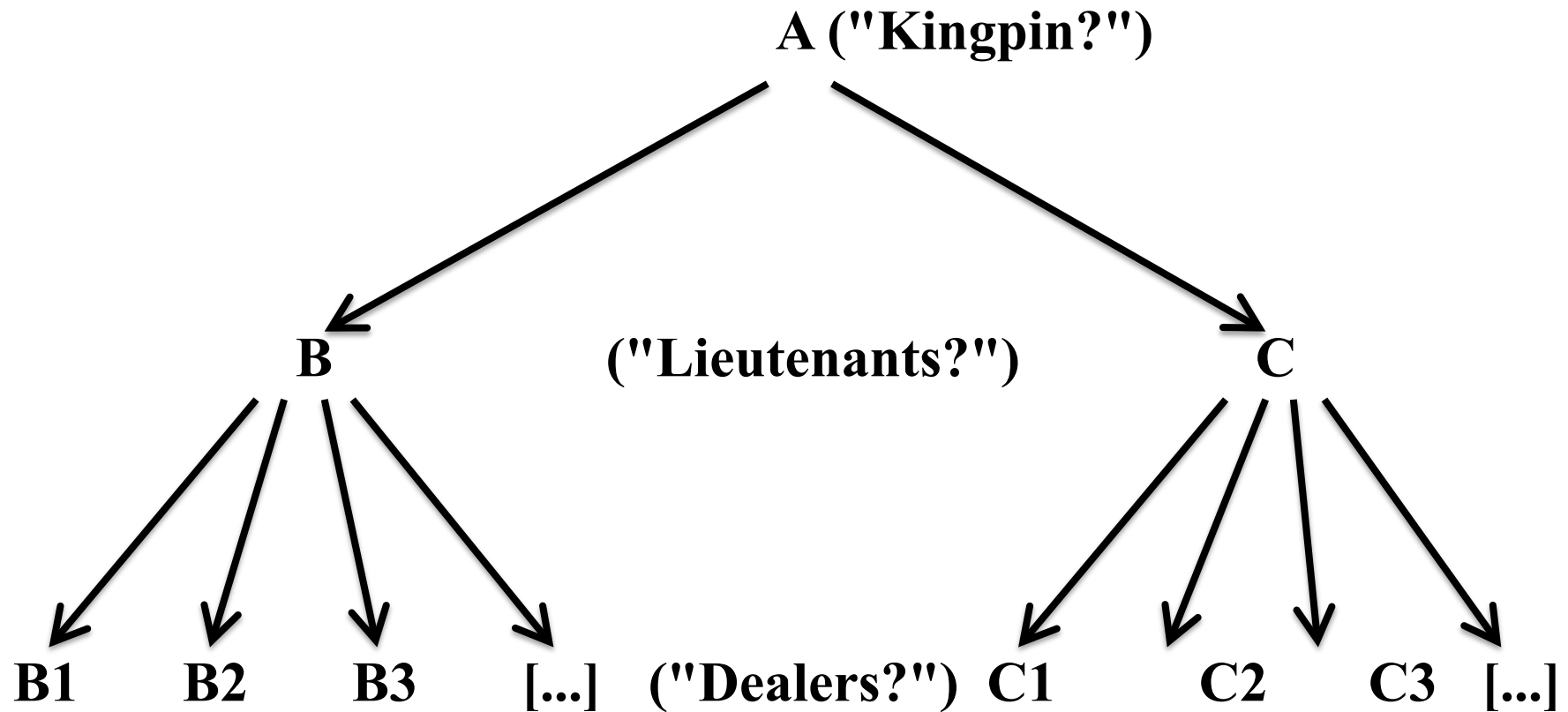
- Assume we're monitoring traffic levels between a foreign military headquarters and its "bases." Because that traffic's encrypted, we don't know what's being said, but over time, we've come to know what normal traffic looks like, e.g., we've got a "traffic baseline."
- Suddenly, out of the blue, traffic from HQ to those bases begins to run 10X or even a 100X normal levels. Something is happening. (This is an example of the "elevated level of chatter" you'll sometimes hear mentioned by the news media.)
- Alerted to this reality, monitoring authorities might decide to task other assets (such as satellite imagery or human intelligence sources) in an effort to figure out exactly what's going on. For example, is the foreign power preparing to launch an attack?
- A sudden drop in traffic can be equally concerning: is this "radio silence" prior to an attack? Was our monitoring detected and somehow circumvented?



Traffic Sequencing Can Also Be Quite Revealing

- As another example, assume encrypted communications between parties A, B, and C are being monitored.
- Two messages (each roughly of the same size, and in close proximity, time-wise) are seen. One is sent from A to B, and another sent from A to C.
- Shortly after those two messages are sent, B is observed sending a message of roughly the same size to ten additional recipients (B1-B10). C does likewise for another dozen recipients (C1-C12).
- From those observations, we might hypothesize a hierarchical communication or command-and-control structure: A directs B and C. B commands B1-B10. C commands C1-C12.
- Being able to infer these sort of relationships can be crucial if you know that some of B1-B10 and C1-C12 are known drug dealers, and B and C are suspected drug distributors. Is A the "king pin?"

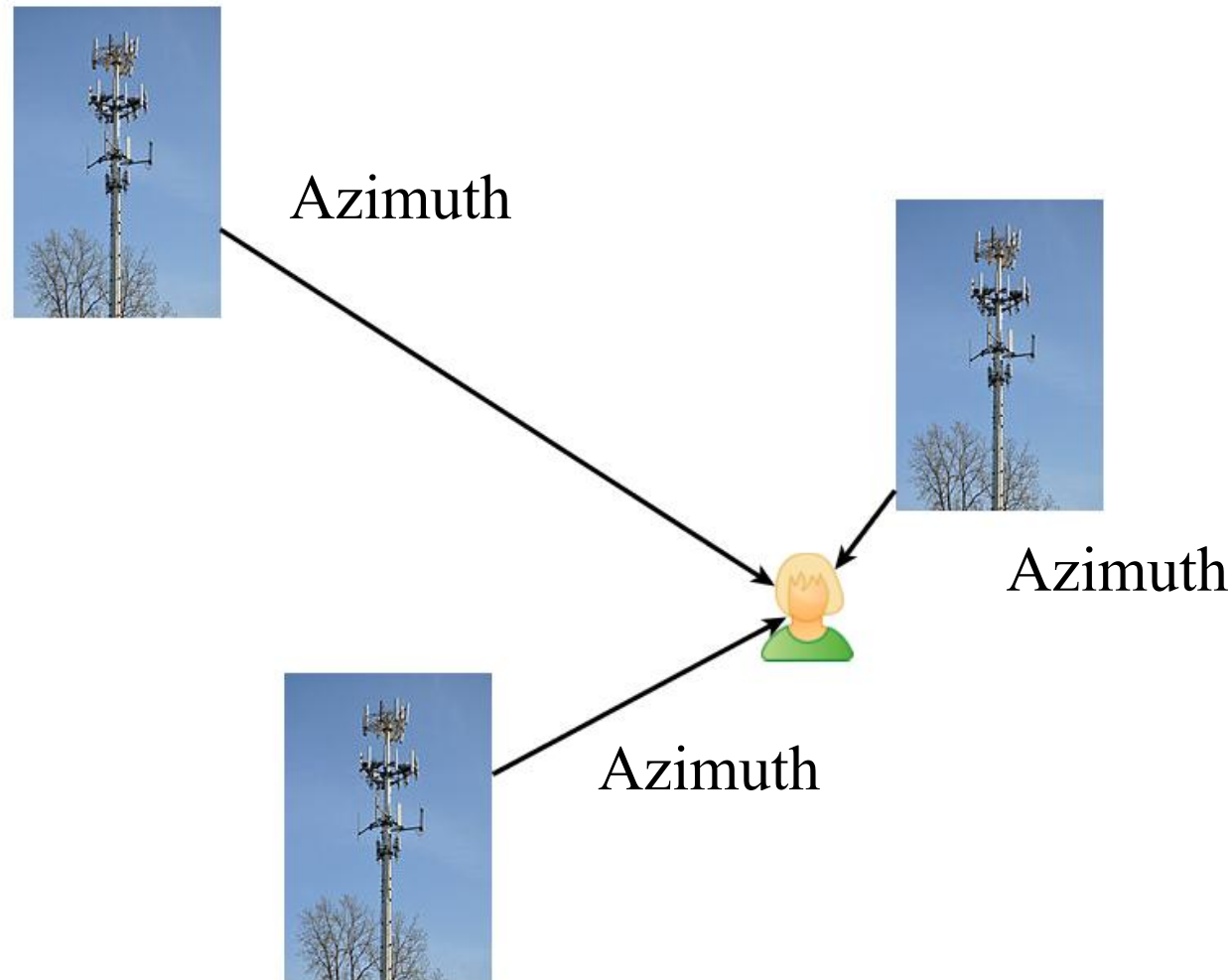
Communication/Control Structure Inference Example



Geolocation of Specific Traffic Sources

- As a final example, assume that a kidnapper contacts the parents of a kidnapped child from his cell phone.
- The kidnapper may not know that the location of cell phones can be determined via GPS, or at least by "cell phone tower triangulation" (measuring the angle ("azimuth") from two or more cell towers to the phone)
- GPS location information, or cell phone tower triangulation data, would allow law enforcement officers to see where the kidnapper is located or may be going, thereby perhaps also finding where a kidnapped child is being held.
- Geolocation can also be important for "E911" emergency calls (including finding a person who has called 911 after suffering a heart attack, stroke or some other life-threatening emergency)

Geolocation Triangulation: Two or More Bearings -- The Cell Phone's Located At the Point of Intersection



Raw cell tower image credit: Joe Ravi [CC BY-SA 3.0] via Wikimedia Commons
http://commons.wikimedia.org/wiki/File:Cell_Phone_Tower.jpg

Appropriate Gov't Uses Cases For Traffic Analysis

- The preceding examples are four examples of appropriate governmental uses for traffic analytic approaches:
 - Counterintelligence surveillance of a sensitive government employee (where there's never any expectation of privacy)
 - Monitoring of a foreign military power for the purpose of detecting an attack and ensuring an appropriate national defensive response
 - Criminal law enforcement investigation of an illegal drug ring
 - Recovery of a kidnapping victim/arrest of a kidnapper (or emergency services response to a medical emergency)

ISPs May ALSO Legitimately Do Traffic Analysis

The following are some (but not necessarily all) examples of appropriate ISP traffic analysis:

- For **routine network operations** (as necessary to run the network, detect faults and equipment failures, plan for required expansion, negotiate peering, perform usage-based billing, etc.)
- To **protect service provider assets and services** (e.g., for intrusion detection, DDoS mitigation, fraud prevention, etc.)
- Other uses as **contractually agreed to** between provider and customer. Examples: delivery of value-added security monitoring services as an extra-cost service at the customer's request, or for research (after appropriate anonymization), etc.

A Few Examples of Some Inappropriate Targets For Governmental Surveillance

- Surveillance targeting peaceful political or religious dissidents, or law-abiding members of an opposition political party
- Surveillance of communications between professionals and clients that are protected by privilege, e.g.:
 - attorney/client privilege
 - clergyman/penitent privilege
 - health care provider/patient privilege
 - journalists/confidential source privilege, etc.
- Surveillance of judges and legislators during the lawful discharge of their duties, especially if those men and women are in an oversight role relating to defense, law enforcement, or intelligence programs and activities [ask Senator Feinstein!]
- **Bulk pervasive monitoring of law-abiding citizens is our primary concern today**

Some Problems With Bulk Pervasive Monitoring

- The collection is **INDISCRIMINANT and UNTARGETED** (data is collected about effectively EVERYONE in dragnet fashion), no individualized suspicion required)
- The collection is **ONGOING**
- The collection is NOT justified by **PROBABLE CAUSE**
- No data **MINIMIZATION** takes place.
- **DATA RETENTION** is perpetual.
- Oversight is **PRO FORMA** at BEST
- **THIS IS ORWELLIAN:** 'In the society that [George] Orwell describes, **every citizen is under constant surveillance by the authorities** [...] The people are constantly reminded of this by the phrase "Big Brother is watching you" [http://en.wikipedia.org/wiki/Big_Brother_%28Nineteen_Eighty-Four%29]

By Contrast, Appropriate Federal Government Uses In Criminal Investigation Situations

In broad terms (and not necessarily covering every corner case)...

- Limited to specific statutorily-designated serious crimes (e.g., kidnapping, racketeering, murder-for-hire, etc.)
- Based on probable cause
- Narrowly targeted and of limited duration
- All collections are carefully minimized
- Last resort (all less-intrusive alternatives have been exhausted)
- Reviewed and approved at a senior level within the law enforcement agency requesting the lawful intercept
- Authorized and carefully supervised by an appropriate court
- Under seal only as long as necessary (NOT effectively "forever")
- Usage annually reported (see <http://www.uscourts.gov/Statistics/WiretapReports/wiretap-report-2013.aspx>)

Appropriate Use In National Security Cases

- I suggest a simple rule:

National security surveillance activity should be subject to the **same terms and conditions** as the criminal use case from the preceding slide.

- Extraordinary national security measures for a limited period of time during an emergency are one thing; turning extraordinarily intrusive measures into "routine practice" for 13 years (!) is something else entirely.
- Let's consider this in the U.S. case...

What Is A "US Person?"

- That definition is more inclusive than you might think.
- “United States person” means a citizen of the United States, **an alien lawfully admitted for permanent residence** (as defined in section 1101 (a)(20) of title 8), **an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence**, or **a corporation which is incorporated in the United States**, but does not include a corporation or an association which is a foreign power, as defined in subsection (a) (1), (2), or (3) of this section."

50 U.S.C. 1801(i) [emphasis added]

Why "U.S. Persons Matter" #1: FISA

- 50 U.S. Code § 1842 - **Pen registers and trap and trace devices for foreign intelligence and international terrorism investigations**

"Notwithstanding any other provision of law, the Attorney General or a designated attorney for the Government may make an application for an order or an extension of an order authorizing or approving the installation and use of a **pen register or trap and trace device** for any investigation to obtain foreign intelligence information **not concerning a United States person or to protect against international terrorism or clandestine intelligence activities**, provided that **such investigation of a United States person** is not conducted solely upon the basis of activities protected by the first amendment to the Constitution which is being conducted by the Federal Bureau of Investigation under such guidelines as the Attorney General approves pursuant to Executive Order No. 12333, or a successor order."
[emphasis added]

Why "U.S. Persons Matter" #2: The USA PATRIOT Act

"Section 215" "Business Records" Provisions

- **50 U.S. Code § 1861 - Access to certain business records for foreign intelligence and international terrorism investigations**
- (a)(1) Subject to paragraph (3), the Director of the Federal Bureau of Investigation or a designee of the Director (whose rank shall be no lower than Assistant Special Agent in Charge) may make an application for an order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information **not concerning a United States person** or **to protect against international terrorism or clandestine intelligence activities**, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution.

Aside: Why Are Telephony Metadata Suddenly "Business Records" Instead Of Pen Register/Trap and Trace Data?

- Is telephony metadata simultaneously BOTH a "business record" AND "pen register/trap and trace" data simultaneously?
- Is 50 U.S. Code § 1842 (FISA Pen Register/Trap and Trace provision) subsumed by the (presumably more-encompassing) Section 215 business records provision?
- Or is this just a case where because detailed call records are routinely collected as part of delivering cellular service, a pen register/trap and trace action isn't required because the data already exists, albeit for completely unrelated reasons?

Examples of Domestic Bulk Metadata Collection

- Domestic bulk metadata collection efforts have included:
 - collecting all telephone call details records,¹
 - collecting Internet traffic flow data,²
 - collecting all postal mail addressing information,³
 - a database of vehicle license plates seen with geolocation data,⁴
 - and pervasive facial recognition and geolocation tracking.⁵
- **WHAT ABOUT ABROAD? We are in Ireland, for example...**

[1] "NSA collecting phone records of millions of Verizon customers daily,"

<http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order>

[2] "A Story of Surveillance," <http://www.washingtonpost.com/wp-dyn/content/article/2007/11/07/AR2007110700006.html> [the Mark Klein AT&T NSA SFO wireroom

incident]

[3] "Postal Service Confirms Photographing All U.S. Mail," <http://www.nytimes.com/2013/08/03/us/postal-service-confirms-photographing-all-us-mail.html>

[4] <https://www.eff.org/deeplinks/2014/02/national-license-plate-recognition-database-what-it-and-why-its-bad-idea>

[5] <http://money.cnn.com/2014/09/16/technology/security/fbi-facial-recognition/>

What Does The EU Say, In General?

- **"(21) Measures should be taken to prevent unauthorised access to communications in order to protect the confidentiality of communications, including both the contents and any data related to such communications, by means of public communications networks and publicly available electronic communications services. [...]"**

"Directive on privacy and electronic communications,"

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML> [emphasis added]

- Sounds pretty good, right?

Well, there's a "small" exception you should be aware of...

The Big (Attempted) "Carve-Out"

- "This Directive **shall not apply to** activities which fall outside the scope of the Treaty establishing the European Community, such as those covered by Titles V and VI of the Treaty on European Union, and in any case to **activities concerning public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law.**"

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML> at Article 15 [emphasis added]

- Hmmm... Nonetheless...

Relevant CJEU Finding

- "Mass metadata storage law 'invalid' invasion of privacy"
<http://www.wired.co.uk/news/archive/2014-04/08/eu-data-retention-directive>

"The European Court of Justice (CJEU) has declared that an EU directive which requires telecoms companies to store the communications data of EU citizens for up to two years is invalid and represents an invasion of privacy.

"According to the court, the Data Retention Directive represents "a wide-ranging and particularly serious interference" with the fundamental rights to respect for private life and to the protection of personal data, and goes beyond what is deemed strictly necessary." [...]

"The case was taken to the CJEU after **Ireland's** High Court and Austria's Constitutional Court asked it to examine whether the law was in line with the Charter of Fundamental Rights of the EU. The move followed a dispute in **Ireland** between a company called **Digital Rights Ireland** and the **Irish** authorities regarding the legalities of retaining this data."

And Yet, Just This May...

www.nytimes.com/2015/05/06/world/europe/french-legislators-approve-sweeping-intelligence-bill.html



EUROPE

Lawmakers in France Move to Vastly Expand Surveillance

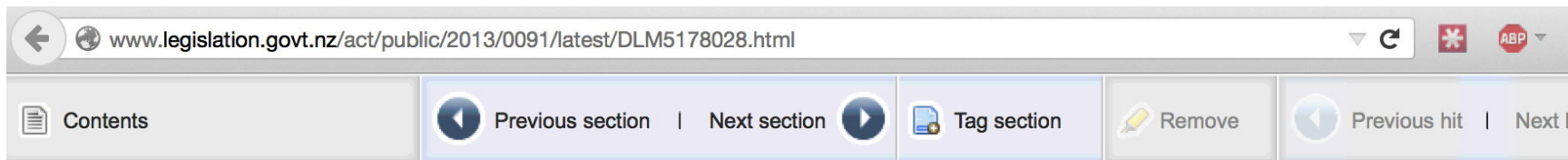
Lawmakers in France Move to Vastly Expand Surveillance

By ALISSA J. RUBIN MAY 5, 2015



The lower house of the French parliament held a vote on Tuesday to adopt new surveillance rules.
Ian Langsdon/European Pressphoto Agency

What About Outside of the EU? For Example, What About NZ? Uh Oh: TICS



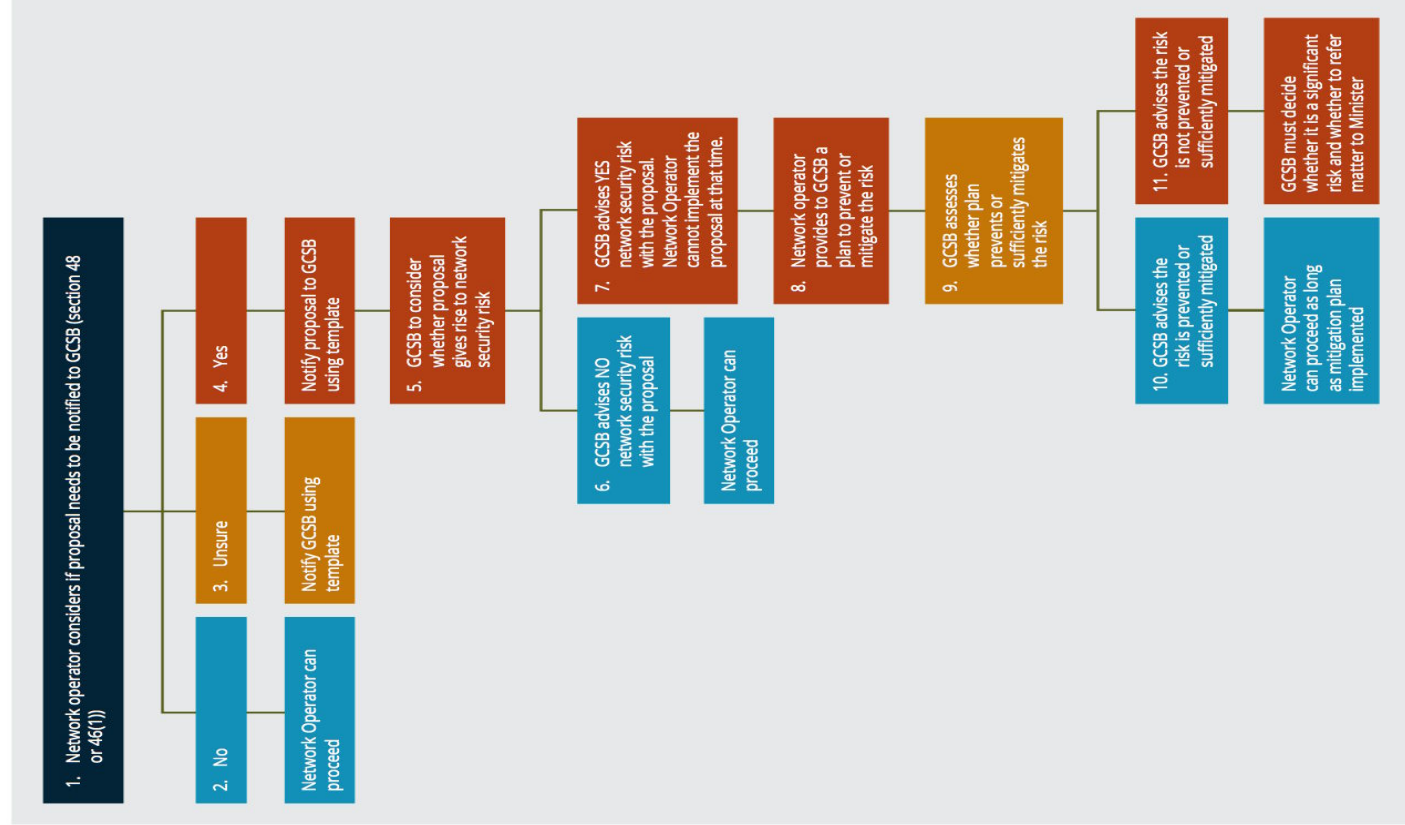
Part 2 Interception capability duties

Subpart 1—Duty to have full interception capability

- 9 Network operators must ensure public telecommunications networks and telecommunications services have full interception capability**
- (1) A network operator must ensure that every public telecommunications network that the operator owns, controls, or operates, and every telecommunications service that the operator provides in New Zealand, has full interception capability.
 - (2) However, subsection (1)—
 - (a) does not require a network operator to ensure that all components of the public telecommunications network or telecommunications service referred to in that subsection have full interception capability; and
 - (b) is sufficiently complied with if a network operator ensures, in whatever manner the network operator thinks fit, that at least 1 component of that network or service has full interception capability.
 - (3) Without limiting subsection (1), the duty under that subsection to have full interception capability includes the duty to ensure that the interception capability is developed, installed, and maintained.

TICSA Also Gives The Government Veto Power On Your Network Architecture and Its Implementation

Figure 1: The Network Proposal Process



Bottom Line For This Section

- Bulk metadata collection is a very contentious issue, and there is huge variability from one country to another.
- While much of the discussion has been happening in the United States and the EU, this is also an area of some sensitivity in other countries.
- What happens in this area can impact your users, but also your company's architecture and operations, as is now the case in New Zealand.
- This is also an issue that is changing rapidly. It behooves you to keep close watch on what's happening.

V. Is Metadata Collection and Traffic Analysis Really That "Big Of A Deal?"

Metadata: "Inconsequential?" (If So, Why Bother?)

- Remember the "going dark due to encryption" speech by FBI Director Comey that I previously mentioned? It included the observation (under "Correcting Misperceptions"):

Some argue that we will still have access to metadata, which includes telephone records and location information from telecommunications carriers. That is true. But metadata doesn't provide the content of any communication. It's incomplete information, and even this is difficult to access when time is of the essence.

- To this, I'd politely suggest that if indeed metadata is of such marginal value, or so hard to use, please let's not waste a lot of time and effort by pervasively collecting metadata!

In Fact...

- Metadata, and the traffic analytic techniques it enables, are *hugely powerful*.
- Edward Snowden certainly knew this:

"Metadata is extraordinarily intrusive. As an analyst, I would prefer to be looking at metadata than looking at content, because it's quicker and easier, and it doesn't lie."

<http://www.zdnet.com/article/can-snowden-finally-kill-the-harmless-metadata-myth/> (September 16th, 2014)

In Fact, People Get Killed Based on Metadata

- Former head of the National Security Agency, Gen. Michael Hayden, has stated that U.S. government “kill[s] people based on metadata” -- but it apparently doesn’t do that with the trove of information collected on American communications.
- Hayden made the remark after saying he agreed with the idea that **metadata** – the information collected by the NSA about phone calls and other communications that does not include content – **can tell the government “everything” about anyone it’s targeting for surveillance, often making the actual content of the communication unnecessary.**
- “[That] description... is absolutely correct. We kill people based on metadata. But that’s not what we do with this metadata,” said Hayden, apparently referring to domestic metadata collection.
- <http://abcnews.go.com/blogs/headlines/2014/05/ex-nsa-chief-we-kill-people-based-on-metadata/>

Real Harms From Routine Pervasive Monitoring

- The biggest problem with pervasive monitoring? The **chilling effect of that activity, once known or reasonably suspected**:
 - An activist may worry that attending a peaceful political meeting or exercising her right to engage in non-violent protest will render her subject to invasive monitoring
 - Citizens may become reluctant to openly support political candidates or advocate for political causes in electoral contests
 - Attorneys may find it difficult or impossible to candidly advise their clients
 - A medical patient, concerned about privacy, may be reluctant to seek relevant information about her condition online, or to discuss her treatments options over the phone with her doctor
 - **Pervasive monitoring has a chilling effect on basic human rights (and Constitutionally-protected speech in the US)**

What Does The IETF Say? They're Blunt. They Say Pervasive Monitoring Is An "Attack"

"Pervasive Monitoring Is a Widespread Attack on Privacy"

"Pervasive Monitoring (PM) is widespread (and often covert) surveillance through intrusive gathering of protocol artefacts, including application content, or protocol metadata such as headers. Active or passive wiretaps and traffic analysis, (e.g., correlation, timing or measuring packet sizes), or subverting the cryptographic keys used to secure protocols can also be used as part of pervasive monitoring. PM is distinguished by being indiscriminate and very large scale, rather than by introducing new types of technical compromise.

"The IETF community's technical assessment is that PM is an attack on the privacy of Internet users and organisations. The IETF community has expressed strong agreement that PM is an attack that needs to be mitigated where possible, via the design of protocols that make PM significantly more expensive or infeasible."

<http://tools.ietf.org/html/rfc7258>

"But Joe! This Is Being Done To Combat Terrorism!"

- I understand that. What's being done is being done with the best of intentions and in an effort to keep us all safe. I *totally* get that.
- I hate terrorists as much as anyone. They **must** be found and they **must** be held accountable.
- I'm just not willing to abandon fundamental human rights (or, in the United States, Constitutionally-protected freedoms), in an effort to deal with potential terrorist threats.
- Most terrorists (except those who may have actual access to weapons of mass destruction), are limited in the damage they can directly cause. Most terrorists need to rely on a sort of "insurgent jujitsu" -- counting on the authorities to over-react in response to relatively localized acts of terror -- in order to make a *real* impact.
- If we let terrorists goad us into ignoring the human rights, the terrorists will *truly* have succeeded, accomplishing far more than they could ever dream of accomplishing by "blowing stuff up."

Effectiveness of Bulk Metadata Against Terrorism?

- Any steps we take in the war against terror must also be **effective**. It's not at all clear that the benefits from the bulk domestic metadata collection program justify its existence:

An analysis of 225 terrorism cases inside the United States since the Sept. 11, 2001, attacks has concluded that the bulk collection of phone records by the National Security Agency **“has had no discernible impact on preventing acts of terrorism.”**

"NSA phone record collection does little to prevent terrorist attacks, group says," *Washington Post*, Jan 12, 2014.

To see the actual report, go to

http://web.archive.org/web/20150102032953/http://www.newamerica.net/sites/newamerica.net/files/policydocs/Bergen_NAF_NSA%20Surveillance_1_0.pdf (cut and paste the 2 and one-half lines of this URL)

Non-terrorism-related Snooping Is Happening, Too...

www.nytimes.com/2013/12/21/world/nsa-drag-net-included-allies-aid-groups-and-business-elite.html

N.S.A. Spied on Allies, Aid Groups and Businesses




Kieran Doherty/Reuters

Satellite dishes in Cornwall, England, at an outpost of Britain's Government Communications Headquarters. The agency has worked closely with the United States.

By JAMES GLANZ and ANDREW W. LEHREN

Published: December 20, 2013

Secret documents reveal more than 1,000 targets of American and British surveillance in recent years, including the office of an Israeli prime minister, heads of international aid organizations, foreign energy companies and a European Union official involved in antitrust battles with American technology businesses.

	SAVE
<hr/>	
EMAIL	
<hr/>	
PRINT	
<hr/>	
SINGLE PAGE	
<hr/>	
DEPRINT	

An Aside: Proven Alternatives To Government Bulk Collection of Domestic Phone Metadata Exist

- See for example "Drug Agents Use Vast Phone Trove, Eclipsing N.S.A.'s," <http://www.nytimes.com/2013/09/02/us/drug-agents-use-vast-phone-trove-eclipsing-nsas.html>

In the HEMISPHERE program:

- Phone metadata stayed with the carrier unless/until subpoenaed, and didn't automatically go to the government
- Government subpoenas were required to get specific items
- Program appeared to meet DEA needs while avoiding bulk domestic metadata collection by the government itself
- Data is reportedly quite fresh, and responses reportedly timely
- **The lesser of two evils?**

What Does the Government Itself Say About The NSA's Bulk Metadata Collection Program?

- Coming back to the NSA's own bulk domestic metadata program...
- Was the government itself squarely aligned behind and supportive of the domestic bulk metadata collection program?
- Or, upon review, does the government itself have profound questions about appropriateness of the bulk metadata collection program?
- We can look at what independent oversight boards, the courts, the legislature, and the executive branch all have to say about this...

The Privacy and Civil Liberties Oversight Board

- "The PCLOB is an independent agency within the executive branch established by the Implementing Recommendations of the 9/11 Commission Act of 2007."
- "The bipartisan, five-member Board is appointed by the President and confirmed by the Senate."
- **"The PCLOB's mission is to ensure that the federal government's efforts to prevent terrorism are balanced with the need to protect privacy and civil liberties."**
- You can read the biographies of the PCLOB membership at <http://www.pclob.gov/about-us/leadership.html>
- The PCLOB's *Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court*, from **January 23, 2014** is available at http://www.pclob.gov/library/215-Report_on_the_Telephone_Records_Program.pdf

The PCLOB Said...

- **"Recommendation 1: The government should end its Section 215 bulk telephone records program. The Section 215 bulk telephone records program lacks a viable legal foundation under Section 215, implicates constitutional concerns under the First and Fourth Amendments, raises serious threats to privacy and civil liberties as a policy matter, and has shown only limited value. As a result, the Board recommends that the government end the program.**

Without the current Section 215 program, the government would still be able to seek telephone calling records directly from communications providers through other existing legal authorities. The Board does not recommend that the government impose data retention requirements on providers in order to facilitate any system of seeking records directly from private databases. Once the Section 215 bulk collection program has ended, the government should purge the database of telephone records that have been collected and stored during the program's operation[...] subject to limits on purging data that may arise under federal law or as a result of any pending litigation." [emphasis added]

Judicial Remedies

- "[...] I will grant Larry Klayman's and Charles Strange's requests for an injunction and enter an order that (1) bars the Government from collecting, as part of the NSA's Bulk Telephony Metadata Program, any telephony metadata associated with their personal Verizon accounts and (2) requires the Government to destroy any such metadata in its possession that was collected through the bulk collection program. **However, in light of the significant national security interests at stake in this case and the novelty of the constitutional issues, I will stay my order pending appeal.**"

Klayman v. Obama, Civil Action No 13-0851 (RJL), U.S. District Court for the District of Columbia,
<https://www.documentcloud.org/documents/901810-klaymanvobama215.html> at page 67, dated Dec 16th, 2013.

That Judicial Process Continues To Lurch Along...

- In November 2014, the Federal appeals court heard arguments in *Klayman v. Obama*. (see https://dockets.justia.com/docket/district_of_columbia/dcdce/1:2013cv00851/160387 for more on the proceedings of this case).
- A decision is now pending.
- Meanwhile, **other** litigation has also been preceding...



N.S.A. Collection of Bulk Call Data Is Ruled Illegal

By CHARLIE SAVAGE and JONATHAN WEISMAN MAY 7, 2015



The entrance to a National Security Agency data collection center in Bluffdale, Utah. George Frey/Getty Images



Email

WASHINGTON — A federal appeals court in New York ruled on Thursday that the once-secret [National Security Agency](#) program that is systematically collecting Americans' phone records in bulk is illegal.

UNITED STATES COURT OF APPEALS
FOR THE SECOND CIRCUIT

August Term, 2014

(Argued: September 2, 2014 Decided: May 7, 2015)

Docket No. 14-42-cv

AMERICAN CIVIL LIBERTIES UNION, AMERICAN CIVIL LIBERTIES UNION FOUNDATION,
NEW YORK CIVIL LIBERTIES UNION, NEW YORK CIVIL LIBERTIES UNION
FOUNDATION,

Plaintiffs-Appellants,

— v. —

JAMES R. CLAPPER, in his official capacity as Director of National Intelligence,
MICHAEL S. ROGERS, in his official capacity as Director of the National Security
Agency and Chief of the Central Security Service, ASHTON B. CARTER, in his
official capacity as Secretary of Defense, LORETTA E. LYNCH, in her official

The House of Representatives Agreed

www.washingtonpost.com/blogs/the-switch/wp/2014/05/22/nsa-reform-bill-passes-house-despite-loss-of-support-from-privacy-advocates/



The Washington Post

Search



Sign In

NSA reform bill passes House, despite loss of support from privacy advocates

By **Andrea Peterson** May 22, 2014



The House of Representatives overwhelmingly passed bill to change the rules for NSA phone record collection. (Reuters)

And Even The Senate Eventually Came Around

www.usnews.com/news/articles/2015/06/02/senate-passes-freedom-act-ending-patriot-act-provision-lapse

Senate Passes Freedom Act, Ending Patriot Act Provision Lapse

The legislation will ban bulk collection of records, backers say.



The Senate approved the USA Freedom Act on Tuesday, delivering a defeat to Senate Majority Leader Mitch McConnell, R-Ky., who first sought a "clean" reauthorization of intelligence laws before pushing unsuccessful amendments.

And President Obama Signed That Legislation

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

A A A

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.

USA Freedom Was A Real Step In The Right Direction

- It wasn't easy, but the United States eventually came to see that dragnet style bulk government surveillance of its own citizens just wasn't the answer.
- Many of the people in this room, or their U.S. colleagues, may end up having to assume new responsibilities given the way government surveillance powers have been refactored, with obligations transferred from the government to service providers.
- It is too soon to characterize new obligations given that the USA Freedom Act was only based into law on June 2nd, 2015, but M3AAWG should pay close attention to the requirements of the USA Freedom Act and how they may impact members.
- And particularly since we're not meeting today in the United States, we also need to recognize that a victory against pervasive monitoring in the US does not eliminate this ill elsewhere.

Technical Measures Are Still Needed

- Just as the community came together to tackle domestic eavesdropping with widespread deployment of encryption – a technical solution – the community also needs to **tackle traffic analysis exposures via technical means**, limited though current options may be.
- We've made progress against pervasive monitoring at home, but tolerating continued bulk collection of metadata **elsewhere**, without question or objection, is equally unconscionable.
- We need to step up and counter the international pervasive monitoring threat via **technical means**.

VI. Technical Approaches To Dealing With Traffic Analysis

What Is the "Traffic Analysis Analog" To The Use of Encryption To Defeat Eavesdropping?

- Our portmanteau of user-based anti-traffic-analysis options, such as they are, is limited, currently consisting of:
 - (1) non-attributable endpoints
 - (2) VPNs
 - (3) Tor ("onion routing")
- Yes, some other options exist, but they're so obscure as to be virtually unused, or so complex as to be impractical for average users.

(1) Non-Attributable Endpoints

- '[former NSA and CIA chief Michael] Hayden, who helped build the intelligence agency's response to the digital age, was pretty clear about how he viewed it, saying "**the problem I have with the Internet is that it's anonymous.**" '
<http://www.washingtonpost.com/blogs/the-switch/wp/2013/10/05/the-nsa-is-trying-to-crack-tor-the-state-department-is-helping-pay-for-it/> [emphasis added]
- "[...] officials surveyed by the [Office of the Inspector General] identified **pre-paid calling cards and pre-paid cell phones** as the **top two threats affecting their ability to conduct electronic surveillance.**" See "The Implementation of the Communications Assistance for Law Enforcement Act," Audit Report 06-13, March 2006 , Office of the Inspector General
<http://www.justice.gov/oig/reports/FBI/a0613/exec.htm>
[emphasis added]

Unauthenticated (Open) Network Access

- There continue to be many unauthenticated or widely available/ nearly-open wireless access points, including ones at **coffee shops** or **fast food restaurants**, free **hotel wireless** networks, etc.
- These access points may sometimes provide less-attributable access that may be valuable for those seeking to casually avoid attribution, however often these access points are subject to abuse by spammers or others who seek to inject unwanted traffic, or are heavily filtered to damp down those complaints.
- Other "open access" wireless access points may actually be outright **malicious, capturing virtually all network traffic seen**. As a random user, your expectations for security and privacy on any open access point you just "stumble upon" should be nil.
- Use of "inadvertently insecure" wireless access points (rather than intentionally-available access points) may also serve as the basis for claims of **computer intrusion**, a felony in some jurisdictions.

Telephonic Non-Attributable Endpoints: Prepaid ("Burner") Cell Phones



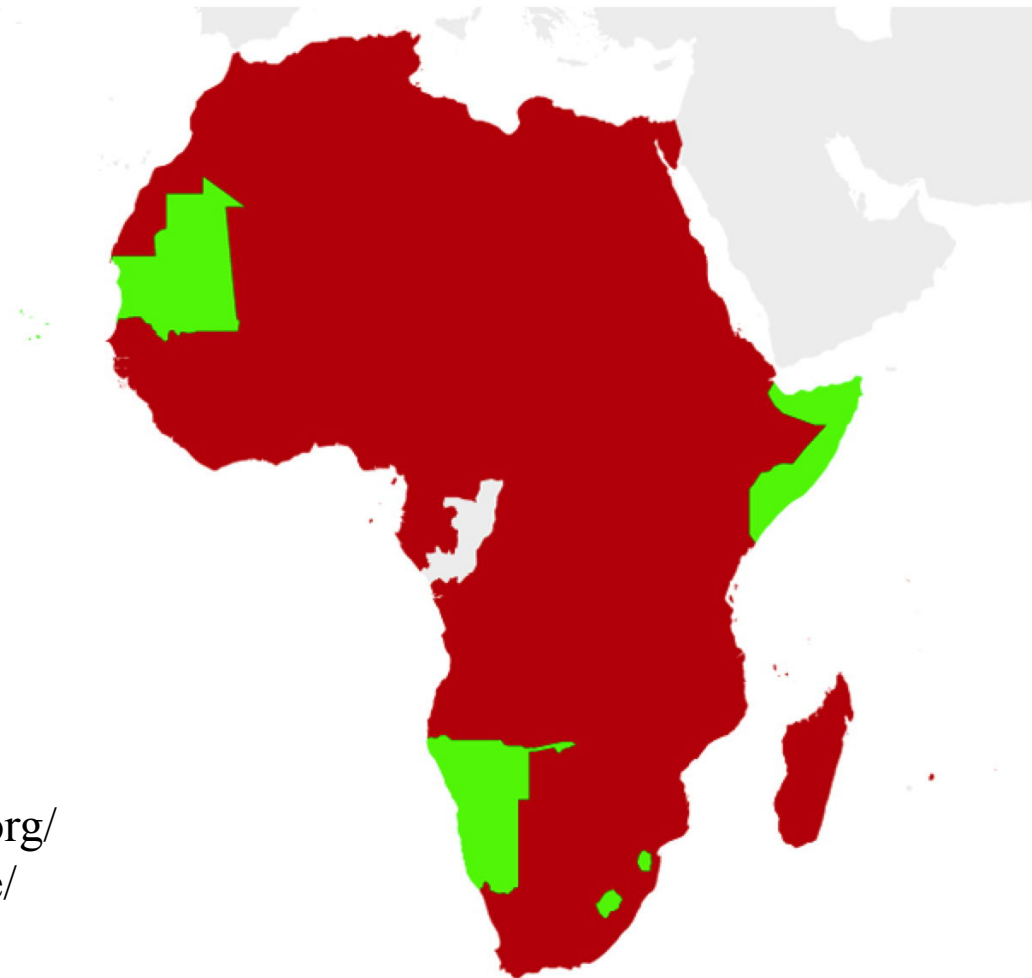
	Prepaid Cell Phone	Contract Cell Phone
Registered?	Not to a personal identity	Yes
Financially tied?	No (if anonymous phone cards are used to 'top up')	Yes (if personal credit card is provided)
Tied to a user's email account?	Often no	Normally yes (incl. backups to "cloud")
Address book?	Minimal or none	Often extensive
Features?	Typically few ("just a simple cheap cell phone")	Often a smart phone with camera, GPS, micro SD cards, apps
Persistently used?	No (cheap; new phones routinely purchased and not directly linked to old phone/phone number)	Yes (~two year life, with old phone chaining to new one upon replacement)
Attributability?	Minimal	Extensive

Expect The World To Eventually Go The Way of Africa And Require Cellphone Registration

Green countries are those in Africa that do NOT require SIM registration as of 2/2014:

Cape Verde
Lesotho
Mauritania
Namibia
Somalia
Swaziland

See <http://firstmonday.org/ojs/index.php/fm/article/view/4351/3820>



Maybe There Are Legitimate Reasons For Requiring Registration, As Many African Countries Have Done?

- Perhaps doing so would hinder fraudulent activity/misuse?
- "[...] to date there is **no evidence** that mandatory registration leads to a reduction in crime. [...] **the United Kingdom, the Czech Republic, Romania and New Zealand, have considered mandating prepaid SIM registration but concluded against it. [...] In Mexico, mandatory SIM registration was introduced in 2009 and repealed three years later** after a policy assessment showed that it had not helped with the prevention, investigation and/or prosecution of associated crimes"

http://www.gsma.com/publicpolicy/wp-content/uploads/2013/11/GSMA_White-Paper_Mandatory-Registration-of-Prepaid-SIM-Users_32pgWEBv3.pdf [emphasis added]

Alternatives to Using A Cell Phone

- **Use a pay phone, instead** (but note that there are now fewer than half a million pay phones remaining in the U.S. according to the American Public Communications Council, see <http://www.apcc.net/i4a/pages/index.cfm?pageid=40>)
- **Consider using a prepaid one-way numeric pager** (these are simple one-way-only devices that receive broadcast pages, so they can't easily be tracked, although messages sent to pagers are obviously not private). N.B.: *two-way* pagers have the same issues as cellphones!
- **Go without a phone** – believe it or not, yes, you can survive without carrying a phone (but the sheer fact that you're choosing to do without may make you "stand out" as an abnormality)
- Be sure to consider the impact of cell phone usage by **family members, too**, if you choose to "go without a cell phone" yourself (their phones may become a proxy for geolocating you)

(2) VPNs

- VPNs are "virtual private networks." **Inbound corporate VPNs** are routinely used to allow remote workers to securely access corporate resources while working "away from the office."
- **Outbound commercial VPN** providers **also** exist. These firms, offering VPN service to any person willing to pay, are often suggested as a "solution" to overcoming traffic analysis exposure.
- If your traffic analysis threat model focuses around **local site monitoring** (e.g., perhaps by your school or your employer), using an outbound VPN may allow you to tunnel past local traffic inspection points. **Use of a VPN will typically NOT be effective as a solution against governmental monitoring.**
- Fundamentally, when you use a VPN, your traffic will "exit" from an alternative location, often somewhere abroad. **You have no way to knowing if the operator of your service is trustworthy,** or is routinely monitoring everything.

Virtual Private Networks (continued)

- When VPN traffic gets routed abroad, it will appear to come *from there*. **International traffic MAY be presumed to NOT be associated with a domestic person, and MAY therefore lose protection from your own country's monitoring. Now add in any local (host country) monitoring that may be happening...**
- VPNs normally mix your traffic with that of other VPN users. While you may be using a VPN for laudable reasons, **other users of that same VPN service may be unsavory** (e.g., at least some of your fellow VPN users may be using a VPN in an effort to hide unlawful activities). **Your innocent traffic (and your innocent identity) may end up comingled and entangled with theirs.**
- Traffic from known VPN exit nodes may also be treated as untrustworthy/unwelcome by at least some mainstream sites.
- All in all, VPNs can be a bit of a "mixed bag" for the average user.

(3) Tor

- If you were to ask technical people to mention one way to avoid classic traffic analysis attacks, the most common thing you'd probably hear mentioned is **Tor (The Onion Router)**.
- If you want to try Tor, it can be downloaded for free for **Windows, Mac and Linux** from <https://www.torproject.org/> ; the Guardian Project has even ported it for **Android**. [You may also want to check out **Tails**, see <https://tails.boum.org/>]
- If you're a less technical person and just want to "buy hardware" in an effort to leverage Tor, see hardware offerings such as:
 - <https://pogoplug.com/safeplug> , or the discussion at
 - "Now Everyone Wants to Sell You a Magical Anonymity Router. Choose Wisely,"
<http://www.wired.com/2014/10/anonymity-routers/>
- Please note! You need to do **more than just install software** (or **more than just run a box**) to really avoid traffic analysis!

Tor Is Not (And Cannot Be) A "Magic Pill"

- Tor tries really hard, but if you fail to practice **strict operational hygiene**, your traffic may end up still being easily attributable (see <http://www.wired.com/2014/12/fbi-metasploit-tor/>)
- If a **bug arises and is exploited**, your traffic may also end up being attributable (see for example <http://www.wired.com/2013/08/freedom-hosting/>)
- Untrustworthy exit node operators may taint executables downloaded through their systems by **adding malware** (<http://threatpost.com/researcher-finds-tor-exit-node-adding-malware-to-binaries/109008> , October 24th, 2014).
- **Tor directory servers may be targeted and attacked/seized** (<http://pando.com/2014/12/21/so-it-begins-operator-of-large-tor-exit-node-cluster-reports-he-has-lost-control-of-his-servers/>)
- See also "**Measuring and mitigating AS-level adversaries against Tor**," <http://arxiv.org/pdf/1505.05173.pdf> , 3 Jun 2015

Tor Was/Is At Least Partially Federally Funded

- In a weird sort of twist that's only possible in America, note that **Tor was originally a product of the Office of Naval Research and DARPA** (see <http://www.onion-router.net/Sponsors.html>)
- **Much of Tor's funding continues to come from the federal government, including the U.S. State Department.**
See <https://www.torproject.org/about/sponsors.html.en>
This is true, notwithstanding reported grumpiness about Tor from members of the intelligence community
(see <http://www.washingtonpost.com/blogs/the-switch/wp/2013/10/05/the-nsa-is-trying-to-crack-tor-the-state-department-is-helping-pay-for-it/>)
- Some may take comfort in the fact that they're using a government funded initiative. Others may be uncomfortable doing so for the same reason, assuming that "something must be up." Ultimately the choice is up to you. (If not Tor, maybe <https://geti2p.net/en/> ?)

So What **MUST** Still Be Done?

- Three Things:

(1) We need an **architecture** that will scale to **Internet-size audiences** and provide **reasonable protection** against traffic analysis for **average users** when they do **average stuff** with **minimal hassle for users or their providers**.

(2) **Users can't be expected to fix the metadata/traffic analysis issue themselves**. Available options are too limited, or too complex. ISPs need to protect their users from traffic analysis.

(3) **Providers who want to protect their users need a non-disruptive solution that they can easily provision without requiring huge expense, or heroic measures**.

End-User Broadband Network Providers

- **End-user broadband provider networks should ensure that they're using many-to-one IPv4 NAT/PAT (many users per public IP address), DHCP with short leases, and no logging.**
- In a NAT/PAT environment, users are connected behind a shared public IP. DHCP is routinely used to dynamically assign IP addresses from a shared pool. To a first approximation, the only one who knows who's on a dynamically assigned DHCP address behind a NAT/PAT gateway is the ISP operating that network. (We'll disregard things like cookies for this initial discussion)
- If providers don't keep DHCP logs and/or NAT/PAT logs, it will be difficult or impossible for external parties to readily map normal wide area traffic to individuals at scale.
- **The US and the EU currently have no mandatory data retention directives** (this is not legal advice; ISPs should check with their own legal team for legal advice on this critical point).

What About Web Hosting Providers?

- Web hosting companies also have options.
- They should ensure that they are putting **as many different web site domains on a single IP address as possible**, and **all** those servers should be protected with SSL/TLS.
- Loading a large number of domains onto a single IP address may be done either on the web server itself (e.g., using regular virtual hosting), or through use of a reverse proxy front end.
- Why would loading many domains onto each IP help with pervasive monitoring? Well, recall that per DOJ policy, with only a few exceptions, web URLs are treated as "content," not "metadata, and as such require a Title III full contents intercept order, not just a pen register/trap and trace order, see http://www.justice.gov/usao/eousa/foia_reading_room/usam/title9/7mcrm.htm#9-7.500

What About ISP's Anti-Abuse Efforts? And What About Carefully-Target Lawful Intercepts by LEOs?

- **The provider** will still have the ability to identify abusers based on internal network traffic monitoring and analysis, done from within the NAT/PAT boundary, or on individual hosts, should they need to do so.
- **Law enforcement officers** can likewise still identify a persistently problematic user, they'd just need to serve the ISP appropriate legal paperwork and work inside the NAT boundary. This might not be fun or easy, nor scale to hundreds of millions of users, but it would be an option if/when it is really needed.
- **Use of NAT/PAT and DHCP without logs, and the practice of hosting many web domains on each IP could also obviously be revisited if/when international bulk metadata collection programs gets re-scoped and subject to appropriate limits.**

Have We Threaded the Needle Again?

- So just as with deployment of encryption for email in transit, use of NAT/PAT without logs, use of DHCP without logs, and heavily shared web hosting appear to represent an example of a deployable solution to hinder bulk metadata collection and traffic analysis attacks, simultaneously ensuring:
 - Average law-abiding users get (some) protection from bulk pervasive metadata collection.
 - ISPs can inexpensively protect their customers while still being able to deal with problematic abuse if it arises.
 - LEOs can still get what they need to deal with the bad guys who truly deserve to be investigated, arrested, tried and punished.

A Closing Thought: IPv4 Runout

- This heavily multiplexed strategy for improved privacy also meshes nicely with the realities of IPv4 address runout and slow IPv6 uptake by the ISP community.
- **Are people really paying attention to the fact that we're either already out or will soon be out of IPv4 address space? If not, please see <http://www.potaroo.net/tools/ipv4/>**
 - APNIC, the Asian Pacific address registry, ran out 19-Apr-2011.
 - RIPE NCC, the European address registry, ran out 14-Sep-2012.
 - LACNIC, the Latin American address registry, ran out 10-Jun-2014.
- **Reminder: In North America, ARIN will likely be running out of IPv4 address space in a little over a month, on 20-Jul-2015.**
- **Unless you have ALL the IPv4 address space you'll EVER need, you'd really better be figuring out what you're going to do next. "Carrier grade" NAT? IPv6? Pursue designated transfers of existing blocks in exchange for a fee? Or???**

Thanks for the Chance to Talk Today!

- Are there any questions?
- These slides are publicly available online at

<https://www.stsauver.com/joe/dublin-traffic-analysis/>