Computer and Network Security

Lecture 28:
Digital Conflict and "The Cyber"

Fall 2024
COMP-5370/6370

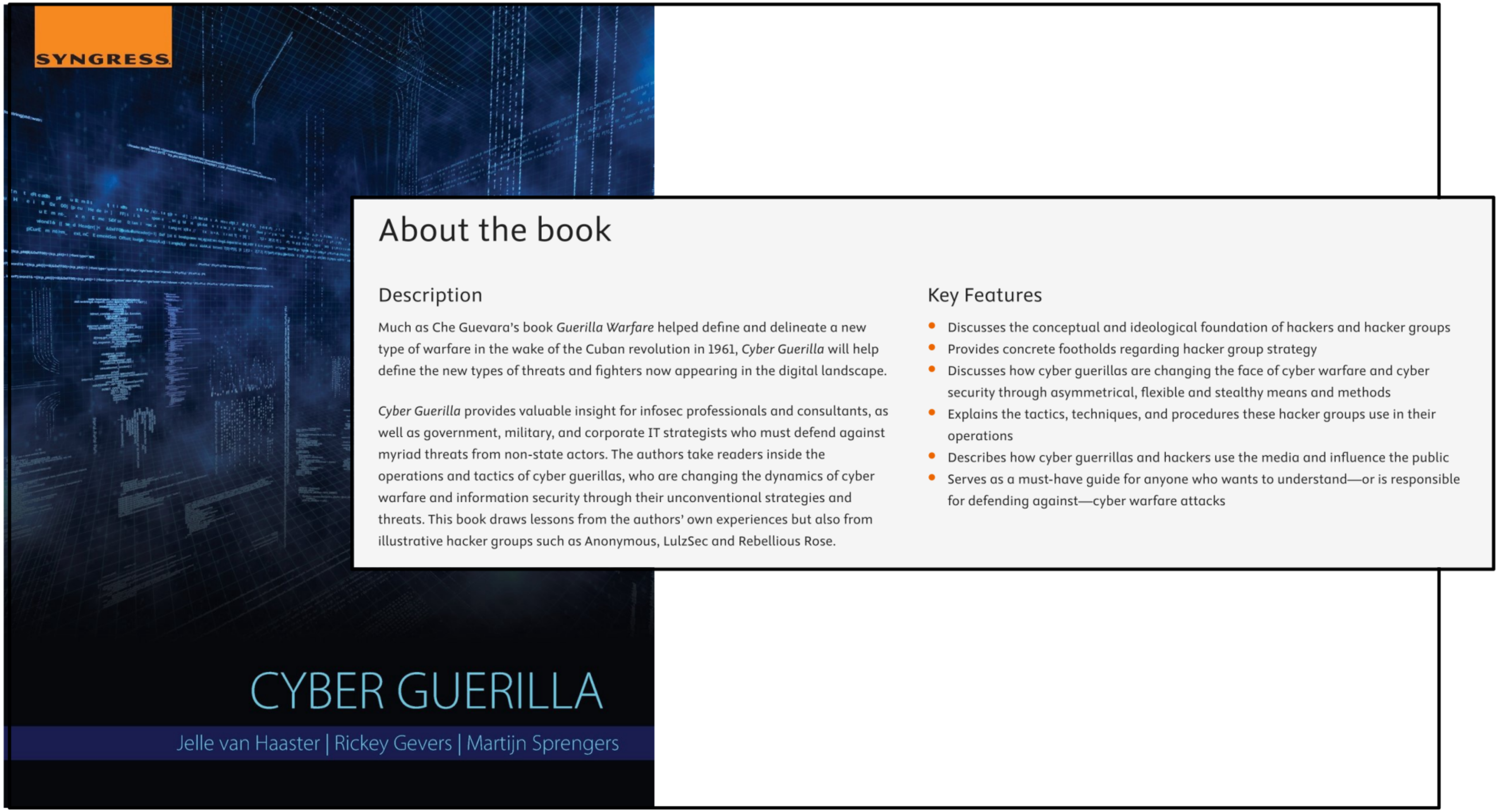
Try to pick which is a security-related term, which is a non-security term, and which I made up on my own:

- cyber-vector
- cyber-cold-war
- cyber-terrorism
- cyber-space
- cyber-attribution
- cyber-psychology
- cyber-evolution
- cyber-english
- cyber-guerilla
- cyber-security
- cyber-physical
- cyber-company
- cyber-ai
- cyber-stalking
- cyber-sale
- cyber-slam
- cyber-performance
- cyber-espionage
- cyber-ceiling fan
- cyber-mechanics
- cyber-anatomy
- cyber-netics
- cyber-truck
- "the cyber"

Try to pick which is a security-related term, which is a non-security term, and which I made up on my own:

- cyber-vector
- cyber-cold-war
- cyber-terrorism
- cyber-space
- cyber-attribution
- cyber-psychology
- cyber-evolution
- cyber-english
- cyber-guerilla
- cyber-security
- cyber-physical
- cyber-company
- cyber-ai
- cyber-stalking
- cyber-sale
- cyber-slam
- cyber-performance
- cyber-espionage
- cyber-ceiling fan
- cyber-mechanics
- cyber-anatomy
- cyber-netics
- cyber-truck
- "the cyber"

Yes, Cyber Guerilla is Real



SYNGRESS

CYBER GUERILLA

Jelle van Haaster | Rickey Gevers | Martijn Sprengers

About the book

Description

Much as Che Guevara's book *Guerilla Warfare* helped define and delineate a new type of warfare in the wake of the Cuban revolution in 1961, *Cyber Guerilla* will help define the new types of threats and fighters now appearing in the digital landscape.

Cyber Guerilla provides valuable insight for infosec professionals and consultants, as well as government, military, and corporate IT strategists who must defend against myriad threats from non-state actors. The authors take readers inside the operations and tactics of cyber guerillas, who are changing the dynamics of cyber warfare and information security through their unconventional strategies and threats. This book draws lessons from the authors' own experiences but also from illustrative hacker groups such as Anonymous, LulzSec and Rebellious Rose.

Key Features

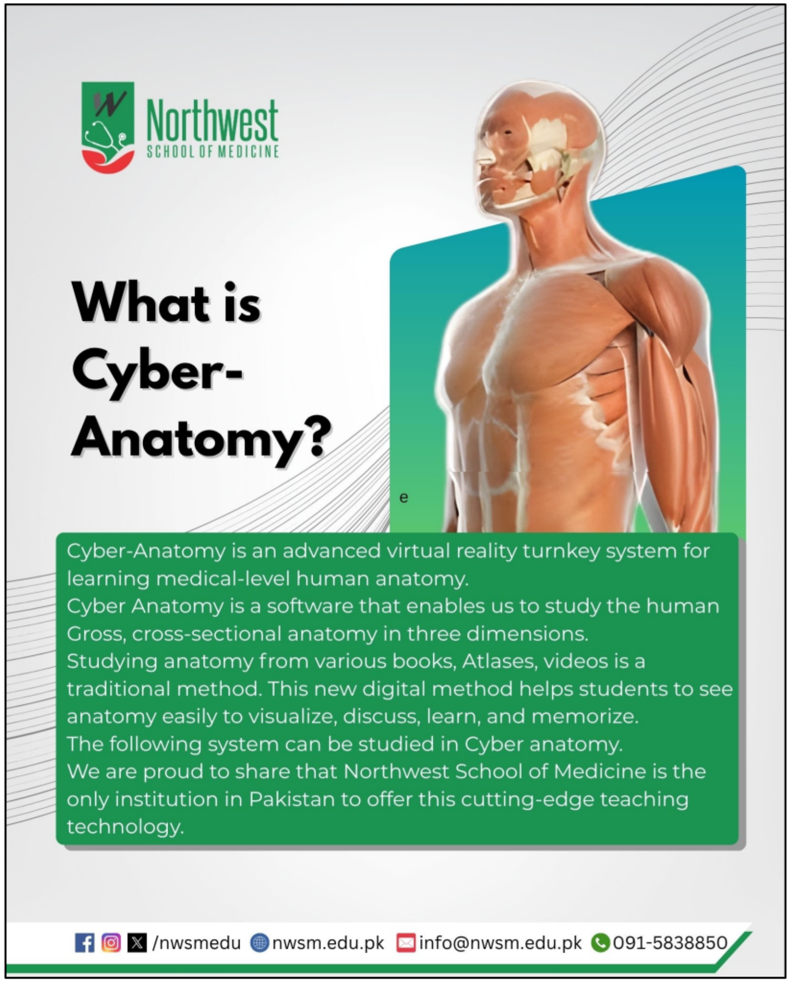
- Discusses the conceptual and ideological foundation of hackers and hacker groups
- Provides concrete footholds regarding hacker group strategy
- Discusses how cyber guerillas are changing the face of cyber warfare and cyber security through asymmetrical, flexible and stealthy means and methods
- Explains the tactics, techniques, and procedures these hacker groups use in their operations
- Describes how cyber guerrillas and hackers use the media and influence the public
- Serves as a must-have guide for anyone who wants to understand—or is responsible for defending against—cyber warfare attacks

Try to pick which is a security-related term, which is a non-security term, and which I made up on my own:

- cyber-vector
- cyber-cold-war
- cyber-terrorism
- cyber-space
- cyber-attribution
- cyber-psychology
- cyber-evolution
- cyber-english
- cyber-guerilla
- cyber-security
- cyber-physical
- cyber-company
- cyber-ai

- cyber-stalking
- cyber-sale
- cyber-slam
- cyber-performance
- cyber-espionage
- cyber-ceiling fan
- cyber-mechanics
- cyber-anatomy
- cyber-netics
- cyber-truck
- "the cyber"

Yes, Cyber-Anatomy is Real


Northwest
SCHOOL OF MEDICINE
e

What is Cyber-Anatomy?

Cyber-Anatomy is an advanced virtual reality turnkey system for learning medical-level human anatomy.
Cyber Anatomy is a software that enables us to study the human Gross, cross-sectional anatomy in three dimensions.
Studying anatomy from various books, Atlases, videos is a traditional method. This new digital method helps students to see anatomy easily to visualize, discuss, learn, and memorize.
The following system can be studied in Cyber anatomy.
We are proud to share that Northwest School of Medicine is the only institution in Pakistan to offer this cutting-edge teaching technology.

/nwsmedu nwsm.edu.pk info@nwsm.edu.pk ☎ 091-5838850

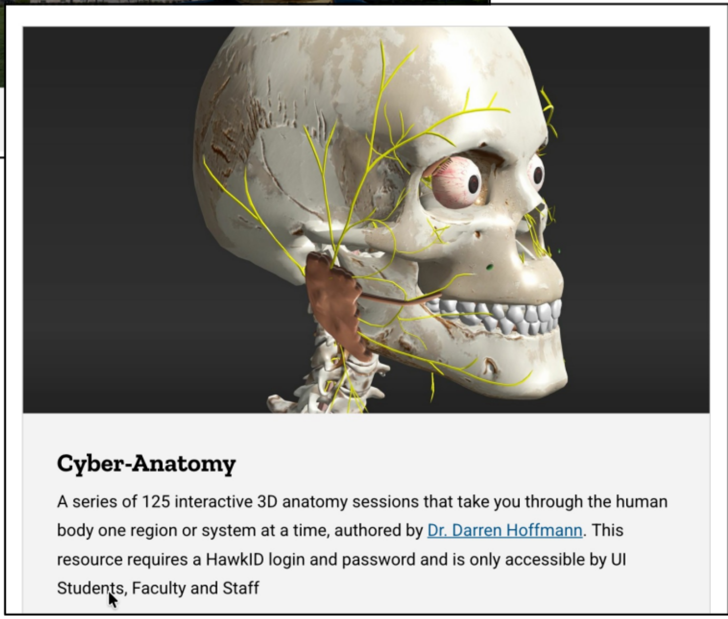
Carver College of Medicine

Department of Anatomy and Cell Biology

Join Our Team Support the Department

EDUCATIONAL RESOURCES

SECTION MENU



Cyber-Anatomy

A series of 125 interactive 3D anatomy sessions that take you through the human body one region or system at a time, authored by Dr. Darren Hoffmann. This resource requires a HawkID login and password and is only accessible by UI Students, Faculty and Staff

Type: Cyber ?Kneecapping?

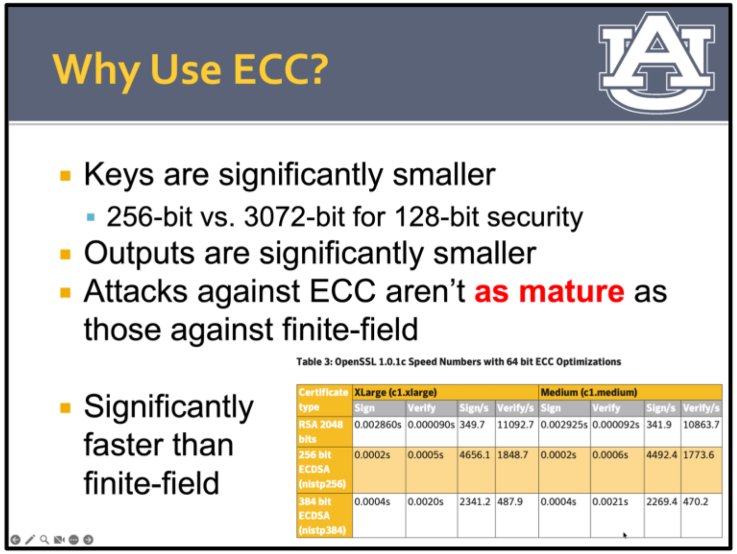
Cyber kneecapping is a made-up phrase to characterize how some nation-states are intentionally limiting users' protection under the rationale of "protecting from harm".

Useful Context

- Four Horsemen of the Information Apocalypse

  Terrorists, drug dealers, pedophiles, organized crime

Remember This?

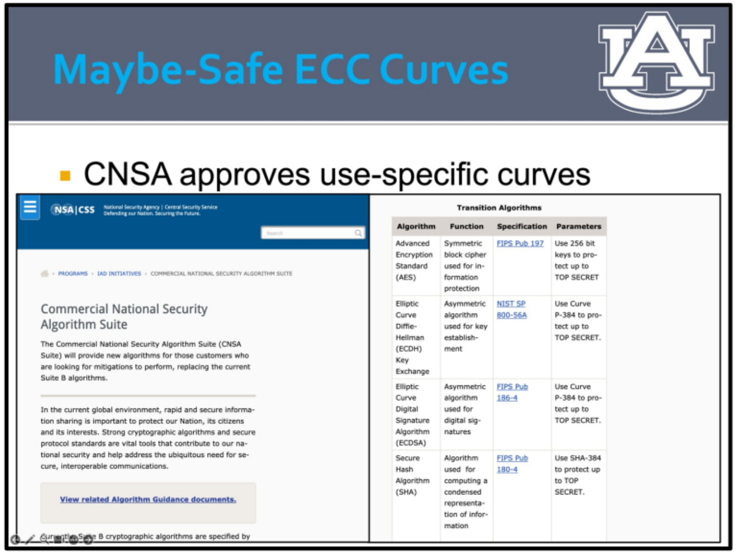


Why Use ECC?

- Keys are significantly smaller
  - 256-bit vs. 3072-bit for 128-bit security
- Outputs are significantly smaller
- Attacks against ECC aren't **as mature** as those against finite-field
- Significantly faster than finite-field

Table 3: OpenSSL 1.0.1c Speed Numbers with 64 bit ECC Optimizations

Certificate type	XLarge (c1.xlarge)				Medium (c1.medium)			
	Sign	Verify	Sign/s	Verify/s	Sign	Verify	Sign/s	Verify/s
RSA 2048 bits	0.002860s	0.000090s	349.7	11092.7	0.002925s	0.000092s	341.9	10863.7
256 bit ECDSA (nistp256)	0.0002s	0.0005s	4656.1	1848.7	0.0002s	0.0006s	4492.4	1773.6
384 bit ECDSA (nistp384)	0.0004s	0.0020s	2341.2	487.9	0.0004s	0.0021s	2269.4	470.2



Maybe-Safe ECC Curves

- CNSA approves use-specific curves

NSA|CSS National Security Agency | Central Security Service Defending our Nation. Securing the Future.
Search
PROGRAMS › IAD INITIATIVES › COMMERCIAL NATIONAL SECURITY ALGORITHM SUITE

Commercial National Security Algorithm Suite

The Commercial National Security Algorithm Suite (CNSA Suite) will provide new algorithms for those customers who are looking for mitigations to perform, replacing the current Suite B algorithms.

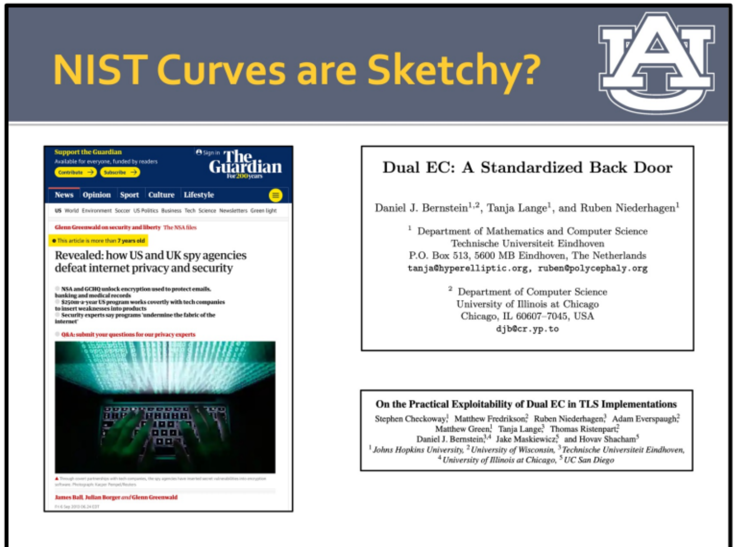
In the current global environment, rapid and secure information sharing is important to protect our Nation, its citizens and its interests. Strong cryptographic algorithms and secure protocol standards are vital tools that contribute to our national security and help address the ubiquitous need for secure, interoperable communications.

View related Algorithm Guidance documents.

Currently, Suite B cryptographic algorithms are specified by

Transition Algorithms

Algorithm	Function	Specification	Parameters
Advanced Encryption Standard (AES)	Symmetric block cipher used for information protection	FIPS Pub 197	Use 256 bit keys to protect up to TOP SECRET
Elliptic Curve Diffie-Hellman (ECDH) Key Exchange	Asymmetric algorithm used for key establishment	NIST SP 800-56A	Use Curve P-384 to protect up to TOP SECRET.
Elliptic Curve Digital Signature Algorithm (ECDSA)	Asymmetric algorithm used for digital signatures	FIPS Pub 186-4	Use Curve P-384 to protect up to TOP SECRET.
Secure Hash Algorithm (SHA)	Algorithm used for computing a condensed representation of information	FIPS Pub 180-4	Use SHA-384 to protect up to TOP SECRET.



NIST Curves are Sketchy?

Support the Guardian
Available for everyone, funded by readers
Contribute →
Subscribe →
Sign in
The Guardian
For 200 years
News
Opinion
Sport
Culture
Lifestyle
US World Environment Soccer US Politics Business Tech Science Newsletters Green light

Glenn Greenwald on security and liberty The NSA files

This article is more than 7 years old

Revealed: how US and UK spy agencies defeat internet privacy and security

- NSA and GCHQ unlock encryption used to protect emails, banking and medical records
- $250m-a-year US program works covertly with tech companies to insert weaknesses into products
- Security experts say programs 'undermine the fabric of the internet'

Q&A: submit your questions for our privacy experts

Through covert partnerships with tech companies, the spy agencies have inserted secret vulnerabilities into encryption software. Photograph: Kacper Pempel/Reuters

James Ball, Julian Borger and Glenn Greenwald

Fri 6 Sep 2013 06.24 EDT

Dual EC: A Standardized Back Door

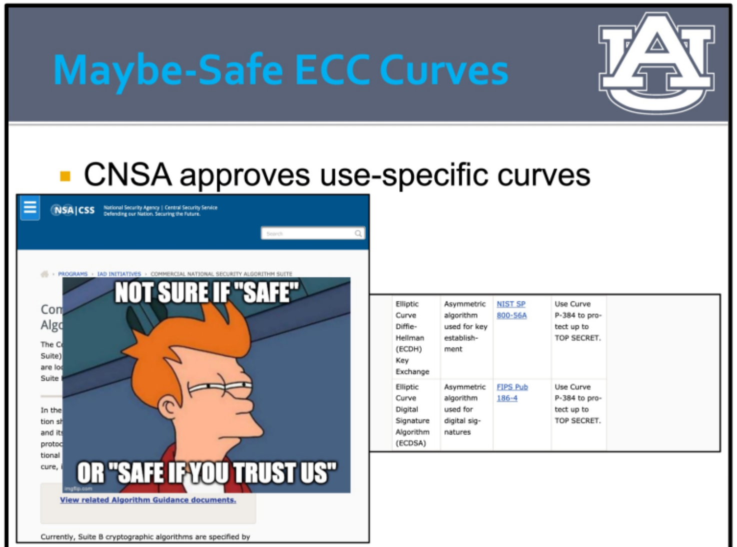
Daniel J. Bernstein[1,2], Tanja Lange[1], and Ruben Niederhagen[1]

[1] Department of Mathematics and Computer Science
Technische Universiteit Eindhoven
P.O. Box 513, 5600 MB Eindhoven, The Netherlands
tanja@hyperelliptic.org, ruben@polycephaly.org

[2] Department of Computer Science
University of Illinois at Chicago
Chicago, IL 60607–7045, USA
djb@cr.yp.to

On the Practical Exploitability of Dual EC in TLS Implementations

Stephen Checkoway[1] Matthew Fredrikson[2] Ruben Niederhagen[3] Adam Everspaugh[2]
Matthew Green[1] Tanja Lange[3] Thomas Ristenpart[2]
Daniel J. Bernstein[3,4] Jake Maskiewicz[5] and Hovav Shacham[5]
[1] Johns Hopkins University, [2] University of Wisconsin, [3] Technische Universiteit Eindhoven,
[4] University of Illinois at Chicago, [5] UC San Diego



Maybe-Safe ECC Curves

- CNSA approves use-specific curves

NSA|CSS National Security Agency | Central Security Service Defending our Nation. Securing the Future.
Search
PROGRAMS › IAD INITIATIVES › COMMERCIAL NATIONAL SECURITY ALGORITHM SUITE
NOT SURE IF "SAFE"
OR "SAFE IF YOU TRUST US"
imgflip.com

Com
Algo

The C
Suite)
are lo
Suite

In the
tion sh
and its
protoc
tional
cure, i

View related Algorithm Guidance documents.

Currently, Suite B cryptographic algorithms are specified by

Elliptic Curve Diffie-Hellman (ECDH) Key Exchange	Asymmetric algorithm used for key establishment	NIST SP 800-56A	Use Curve P-384 to protect up to TOP SECRET.
Elliptic Curve Digital Signature Algorithm (ECDSA)	Asymmetric algorithm used for digital signatures	FIPS Pub 186-4	Use Curve P-384 to protect up to TOP SECRET.

DUAL_EC

DUAL_EC_DRBG was a CSPRING approved by NIST as “safe” even though it was known to be *less-than-ideal* at the time.

- Was extremely slow compared to others
- Theoretical attacks discovered between proposal and standardization (constants)
- Almost everyone agreed to not uses

Very Likely an NSA Operation

- Pushed for its standardization when no one else supported it or even wanted it
- Changed the constants but didn't explain why or admit that they did
- Secretly paid $10M to make it the default RNG source for many enterprises.
  - RSA Inc's BSAFE library
- Strong-armed companies to adding it to their own software (Juniper NetScreen)

Juniper + DUAL_EC

- 2008: Dept. of Defense demanded Juniper implement and use DUAL_EC
- 2012: APT5 compromised Juniper and altered NSA's constants to own constants
- 2015: Altered constants discovered and patch released to return to NSA constants
- 2018: NSA notifies Sen. Wyden that NSA created a "lessons learned" report
- 2021: NSA tells Sen. Wyden that they "cannot locate this document"

The Fallacy of NOBUS

Cyber capabilities are often asserted to be **“No One But US” (NOBUS)** in terms of:

- No malicious actor has capability to exploit
- No malicious actor will ever be able to exploit
- No harm could ever come from neglecting to patch the underlying vulnerabilities

NOBUS mentality is not only false, but is also dangerously arrogant.

The Fallacy of NOBUS

Cyber capabilities are often claimed in terms of **“No One But US” (NOBUS)** but that mentality is not only false, but is also dangerously arrogant.

- Access to OPM data was NOBUS
  - Until it wasn’t
- Exploitation of ETERNAL BLUE was NOBUS
  - Until it wasn’t
- Crypto defeat via DUAL_EC was NOBUS
  - Until it wasn’t

Computer and Network Security

Lecture 28
Surveillance

Fall 2025
COMP-5370/6370

Nation-State Actors

- Highly Knowledgeable and Specialized
- Highly Privileged
- Exceptional Access to Resources

Surveillance

Surveillance is the act of monitoring a person, place, or group for explicit purpose of gathering information on their activities.

- HUMINT: Human Intelligence
  - Alice says Bob is at work right now
- GEOINT: Geospatial Intelligence
  - Imagery says Bob is at work right now
- SIGINT: Signals Intelligence
  - ELINT: Bob’s phone is at his work right now
  - COMINT: Bob texted his wife that he was at work

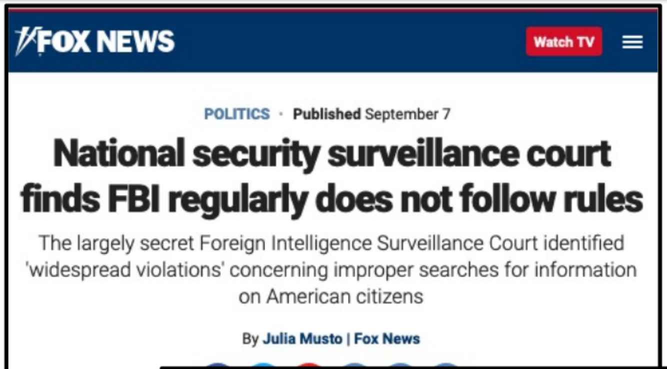
Uses of Surveillance

There are perfectly valid and justified uses of surveillance and intelligence collection.

- Goal is to protect country and citizens
- There are many actors to protect against

- Oversight protects against abuse and protect against tyrannical power

US Intelligence Abuses

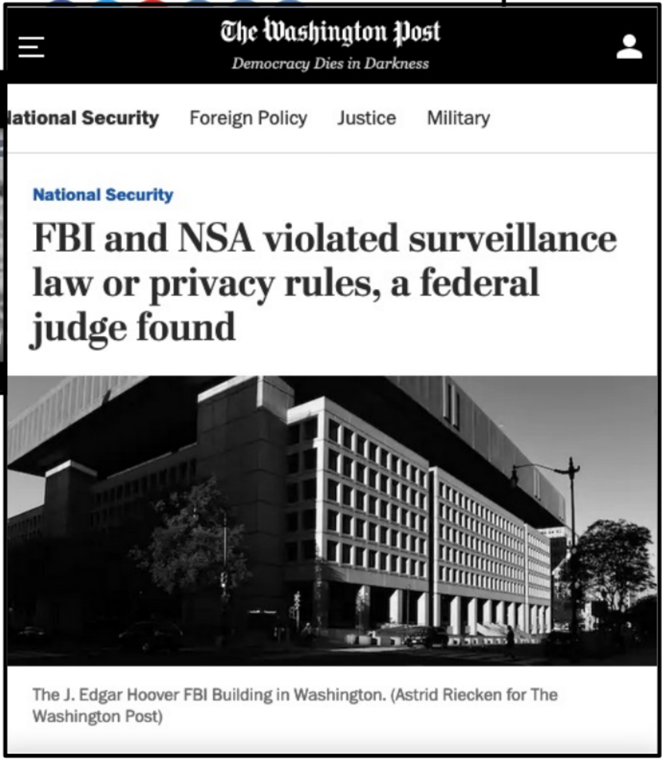


POLITICS · **Published** September 7

National security surveillance court finds FBI regularly does not follow rules

The largely secret Foreign Intelligence Surveillance Court identified 'widespread violations' concerning improper searches for information on American citizens

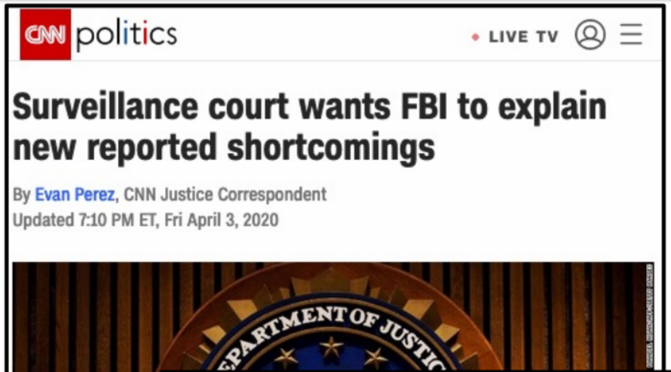
By **Julia Musto** | **Fox News**



National Security

FBI and NSA violated surveillance law or privacy rules, a federal judge found

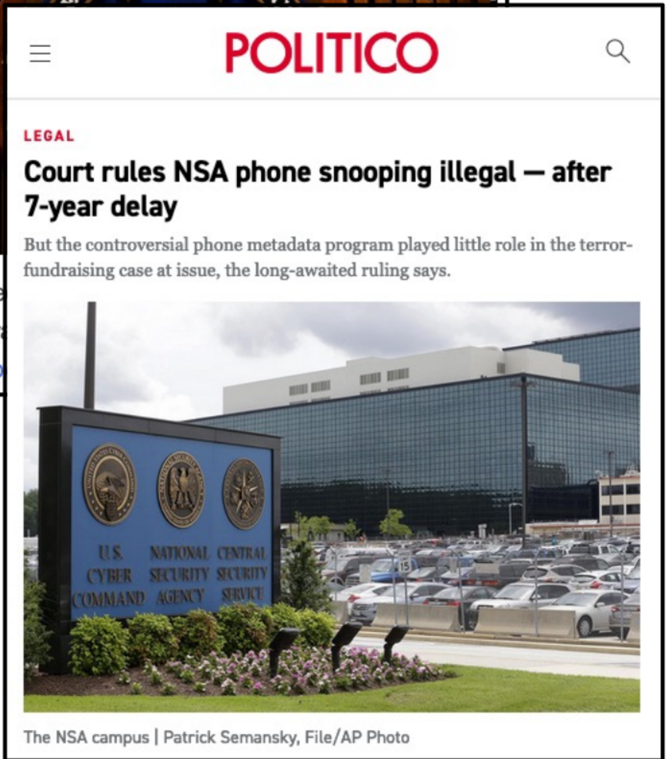
The J. Edgar Hoover FBI Building in Washington. (Astrid Riecken for The Washington Post)



Surveillance court wants FBI to explain new reported shortcomings

By **Evan Perez**, CNN Justice Correspondent
Updated 7:10 PM ET, Fri April 3, 2020

(CNN) — The fe
surveillance w
missteps in go



LEGAL

Court rules NSA phone snooping illegal — after 7-year delay

But the controversial phone metadata program played little role in the terror-fundraising case at issue, the long-awaited ruling says.

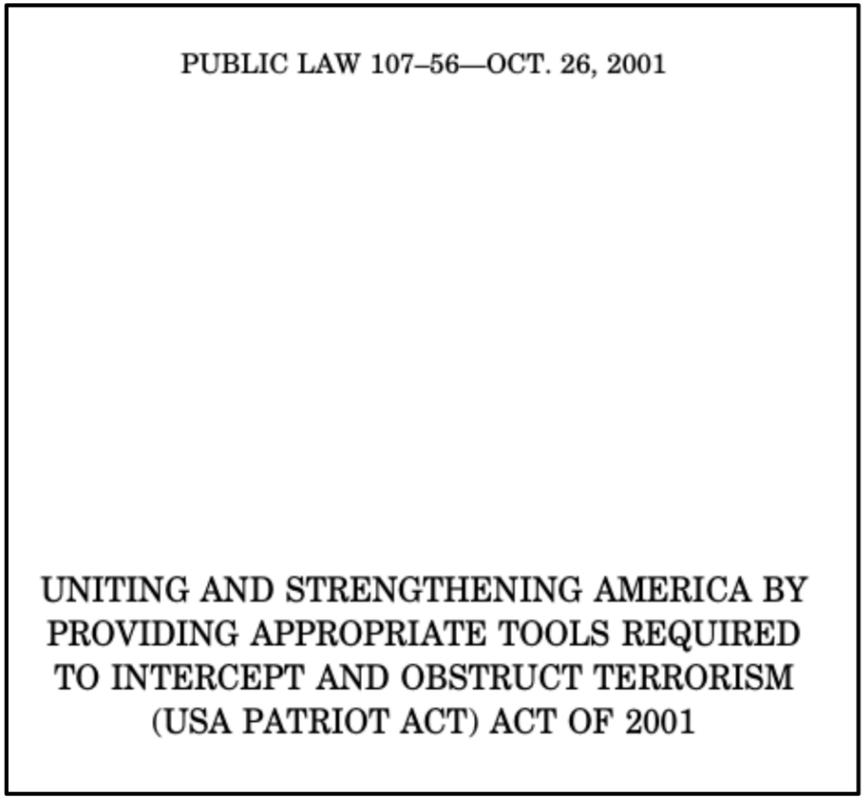
The NSA campus | Patrick Semansky, File/AP Photo

September 11, 2001

- Completely unexpected
- Lots of fear, uncertainty, and doubt for a long time afterwards
- People were scared

This can't be allowed to happen again.

Oct 2001: USA Patriot Act

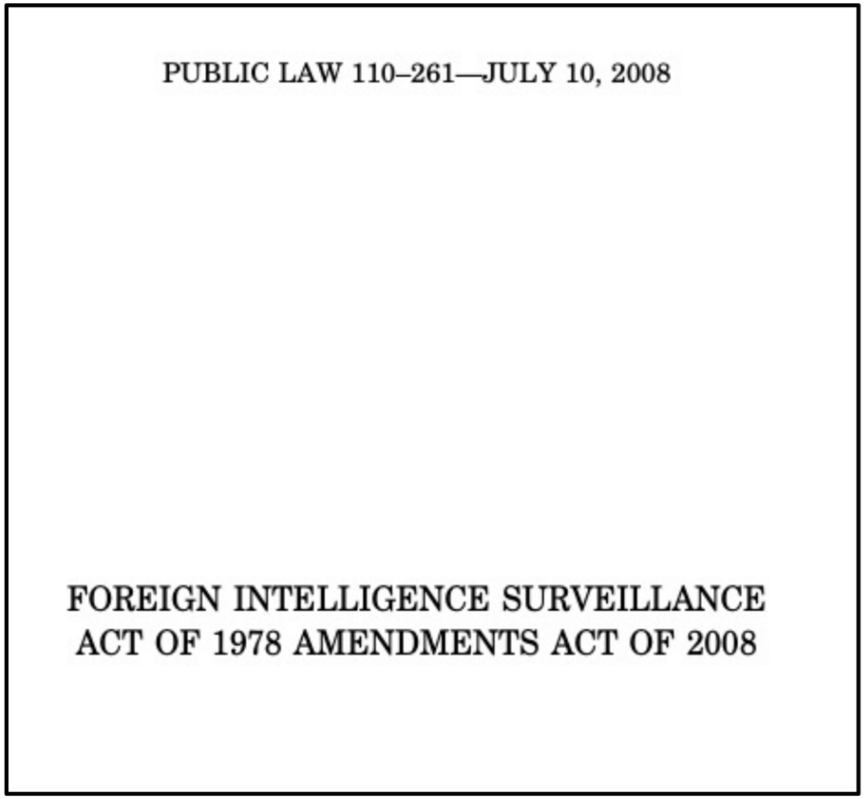


PUBLIC LAW 107–56—OCT. 26, 2001

UNITING AND STRENGTHENING AMERICA BY PROVIDING APPROPRIATE TOOLS REQUIRED TO INTERCEPT AND OBSTRUCT TERRORISM (USA PATRIOT ACT) ACT OF 2001

- Major rule changes on Law Enforcement access to information
- Major focus on “Tangible things” and “Business Records”

Jul 2008: FISA Amendments Act

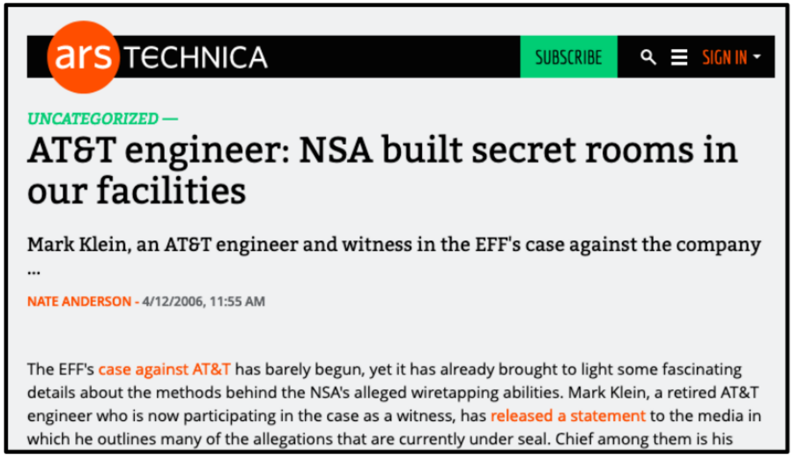


PUBLIC LAW 110–261—JULY 10, 2008

FOREIGN INTELLIGENCE SURVEILLANCE
ACT OF 1978 AMENDMENTS ACT OF 2008

- Allows Attorney General and DNI to authorize monitoring
- Is very explicitly not allowed to target ”US-Persons”

2006 – 2013



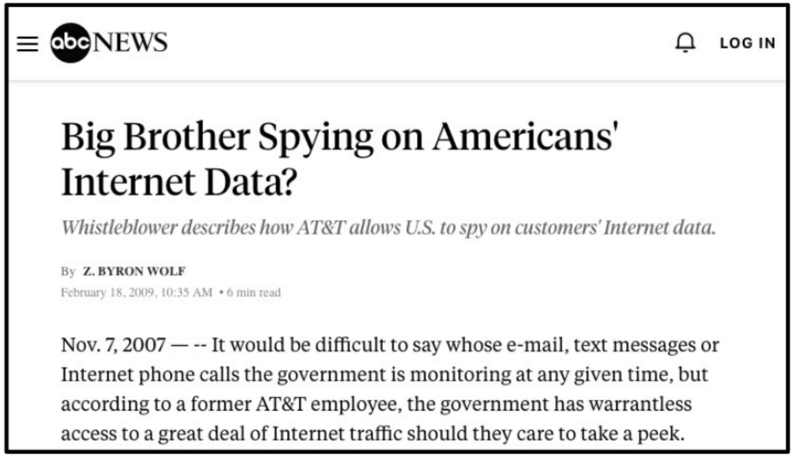
UNCATEGORIZED —

AT&T engineer: NSA built secret rooms in our facilities

Mark Klein, an AT&T engineer and witness in the EFF's case against the company ...

NATE ANDERSON - 4/12/2006, 11:55 AM

The EFF's case against AT&T has barely begun, yet it has already brought to light some fascinating details about the methods behind the NSA's alleged wiretapping abilities. Mark Klein, a retired AT&T engineer who is now participating in the case as a witness, has released a statement to the media in which he outlines many of the allegations that are currently under seal. Chief among them is his



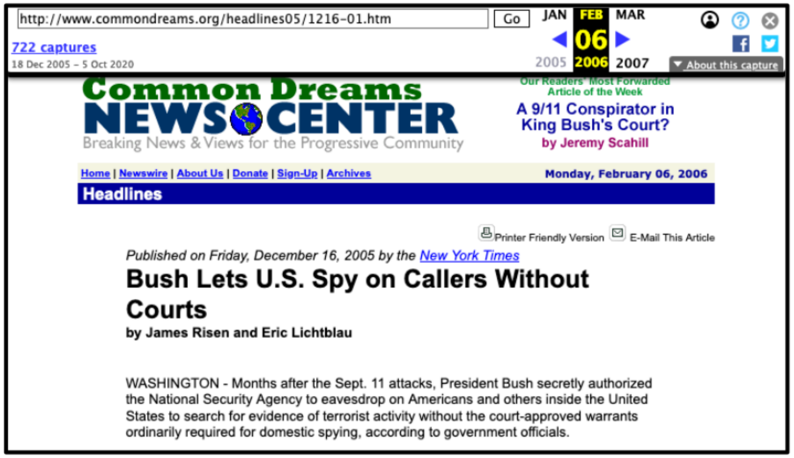
Big Brother Spying on Americans' Internet Data?

Whistleblower describes how AT&T allows U.S. to spy on customers' Internet data.

By Z. BYRON WOLF

February 18, 2009, 10:35 AM • 6 min read

Nov. 7, 2007 — -- It would be difficult to say whose e-mail, text messages or Internet phone calls the government is monitoring at any given time, but according to a former AT&T employee, the government has warrantless access to a great deal of Internet traffic should they care to take a peek.


http://www.commondreams.org/headlines05/1216-01.htm
Go
JAN
FEB
MAR
06
2005
2006
2007
722 captures
18 Dec 2005 – 5 Oct 2020
About this capture
Common Dreams
NEWS CENTER
Breaking News & Views for the Progressive Community
Home | Newswire | About Us | Donate | Sign-Up | Archives
Printer Friendly Version
E-Mail This Article

Our Readers' Most Forwarded Article of the Week

A 9/11 Conspirator in King Bush's Court?
by Jeremy Scahill

Monday, February 06, 2006

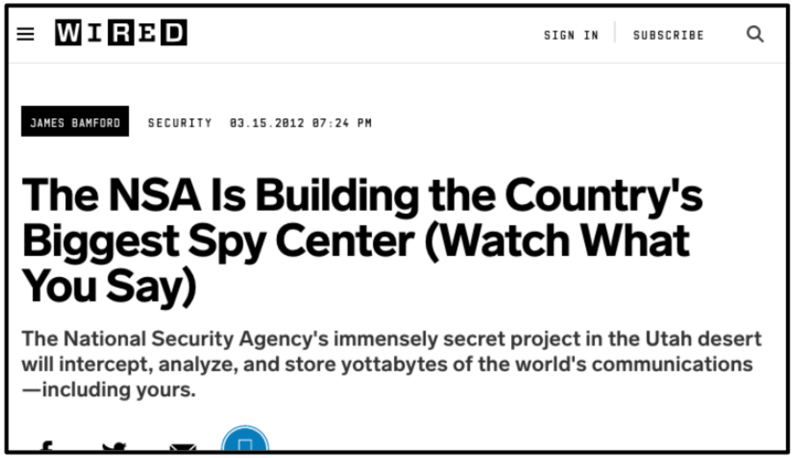
Headlines

Published on Friday, December 16, 2005 by the New York Times

Bush Lets U.S. Spy on Callers Without Courts

by James Risen and Eric Lichtblau

WASHINGTON - Months after the Sept. 11 attacks, President Bush secretly authorized the National Security Agency to eavesdrop on Americans and others inside the United States to search for evidence of terrorist activity without the court-approved warrants ordinarily required for domestic spying, according to government officials.

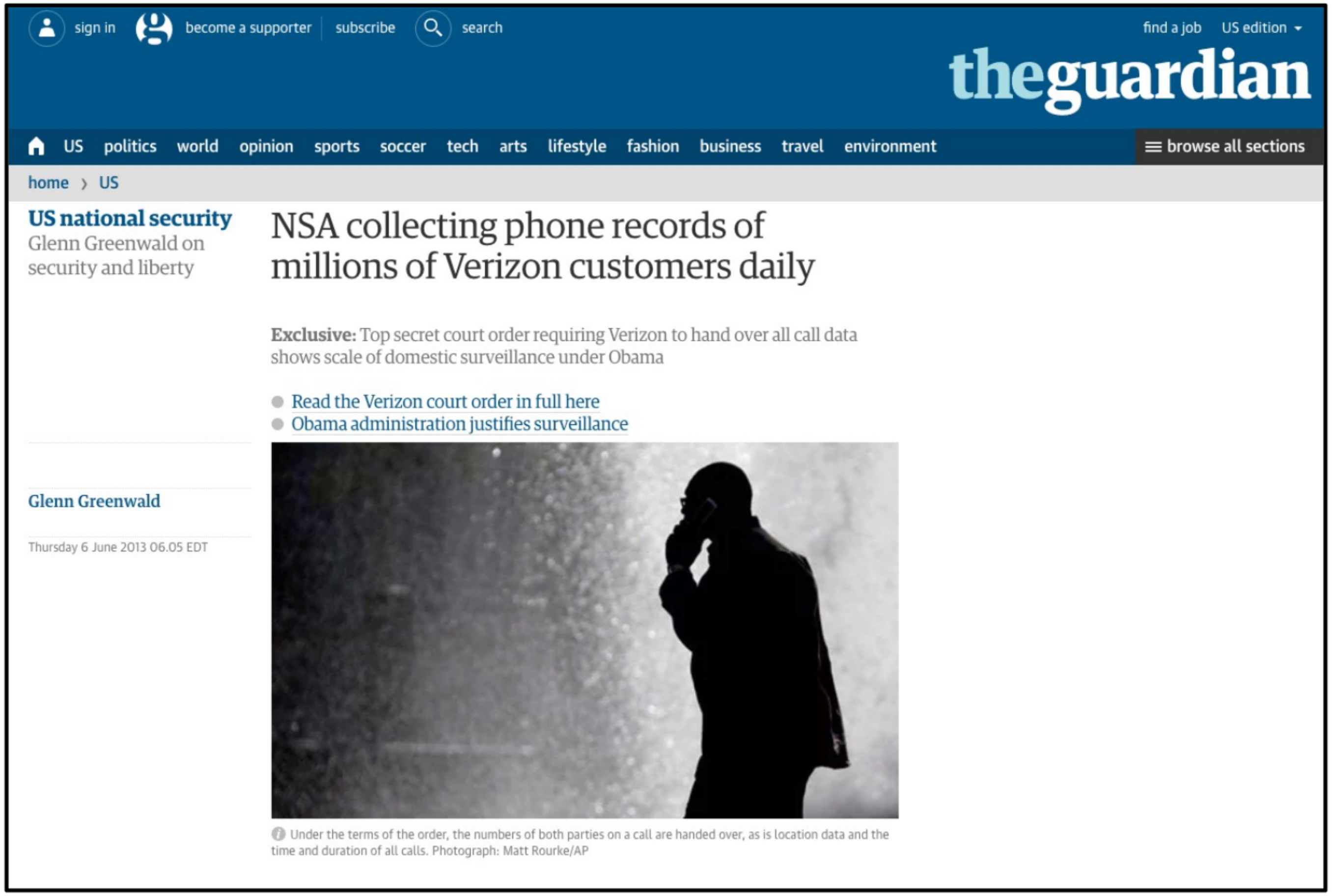


JAMES BAMFORD SECURITY 03.15.2012 07:24 PM

The NSA Is Building the Country's Biggest Spy Center (Watch What You Say)

The National Security Agency's immensely secret project in the Utah desert will intercept, analyze, and store yottabytes of the world's communications—including yours.

June 6, 2013



US national security
Glenn Greenwald on security and liberty

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

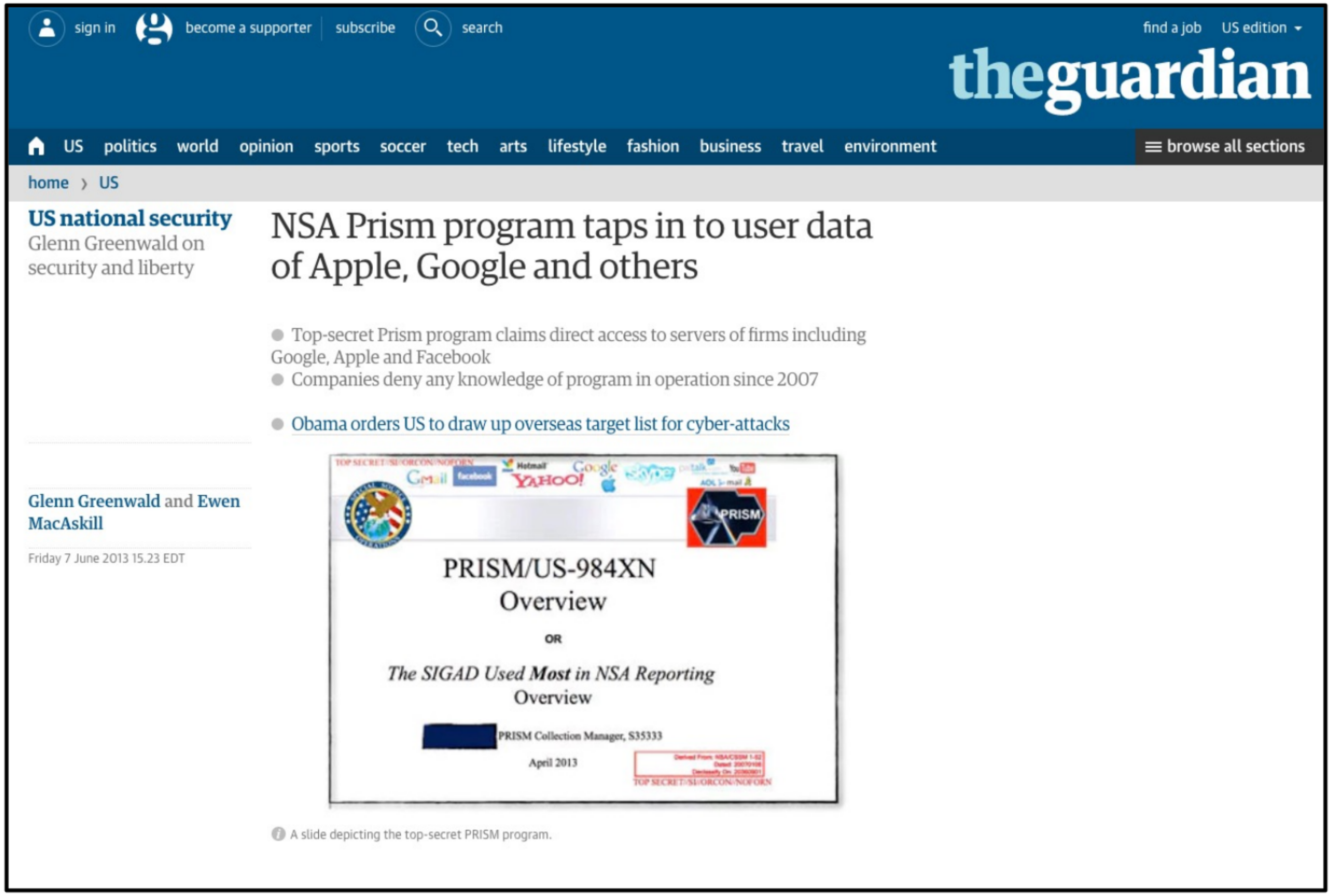
- Read the Verizon court order in full here
- Obama administration justifies surveillance

Glenn Greenwald

Thursday 6 June 2013 06.05 EDT

Under the terms of the order, the numbers of both parties on a call are handed over, as is location data and the time and duration of all calls. Photograph: Matt Rourke/AP

June 7, 2013



US national security
Glenn Greenwald on security and liberty

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
- Obama orders US to draw up overseas target list for cyber-attacks

Glenn Greenwald and **Ewen MacAskill**

Friday 7 June 2013 15.23 EDT

PRISM/US-984XN
Overview

OR

The SIGAD Used ***Most*** *in NSA Reporting*
Overview

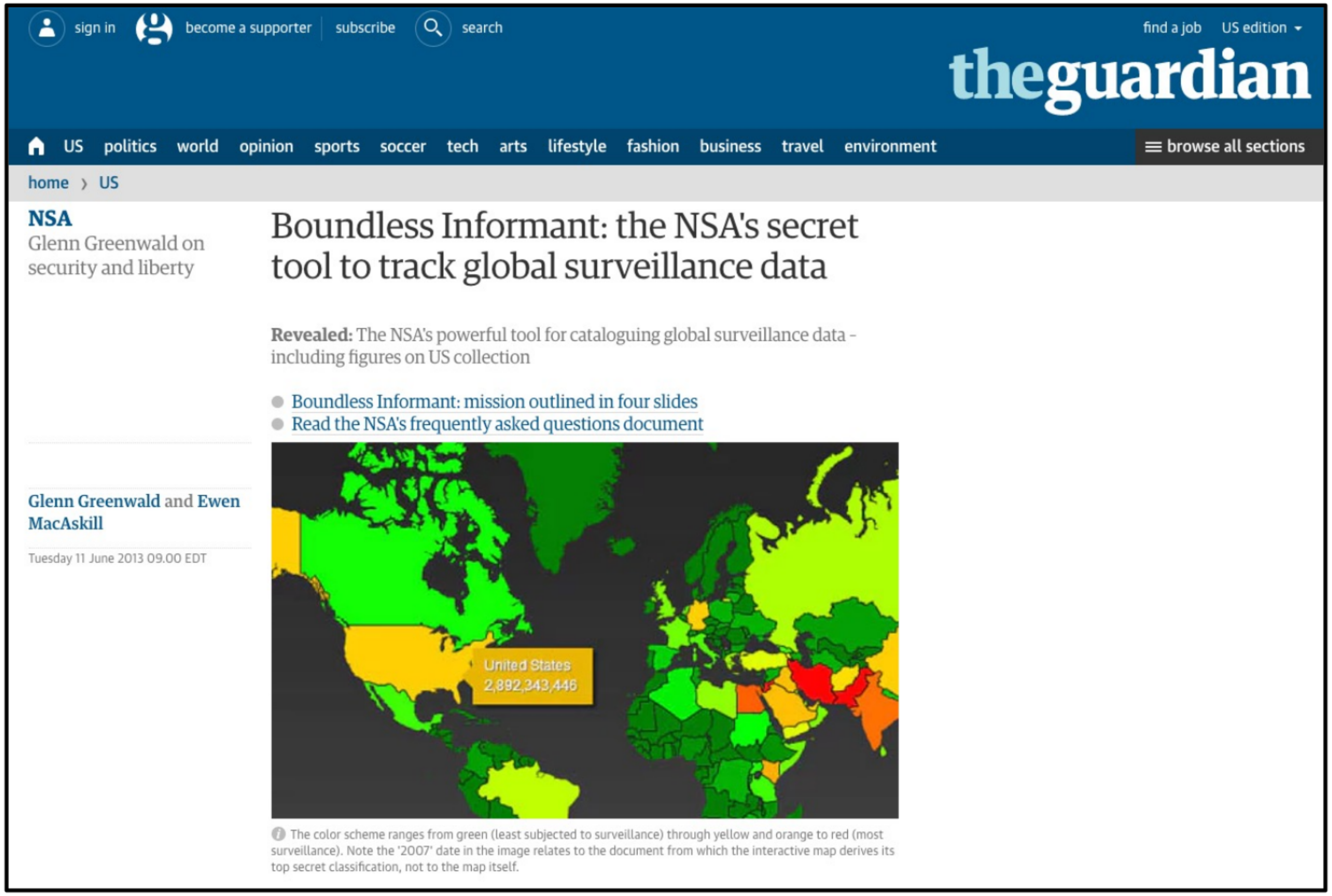
[redacted] PRISM Collection Manager, S35333

April 2013

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20360901
TOP SECRET//SI//ORCON//NOFORN

A slide depicting the top-secret PRISM program.

June 8, 2013



NSA
Glenn Greenwald on security and liberty

Boundless Informant: the NSA's secret tool to track global surveillance data

Revealed: The NSA's powerful tool for cataloguing global surveillance data - including figures on US collection

- Boundless Informant: mission outlined in four slides
- Read the NSA's frequently asked questions document

The color scheme ranges from green (least subjected to surveillance) through yellow and orange to red (most surveillance). Note the '2007' date in the image relates to the document from which the interactive map derives its top secret classification, not to the map itself.

Glenn Greenwald and Ewen MacAskill

Tuesday 11 June 2013 09.00 EDT

June 9, 2013

Global Passive Adversary

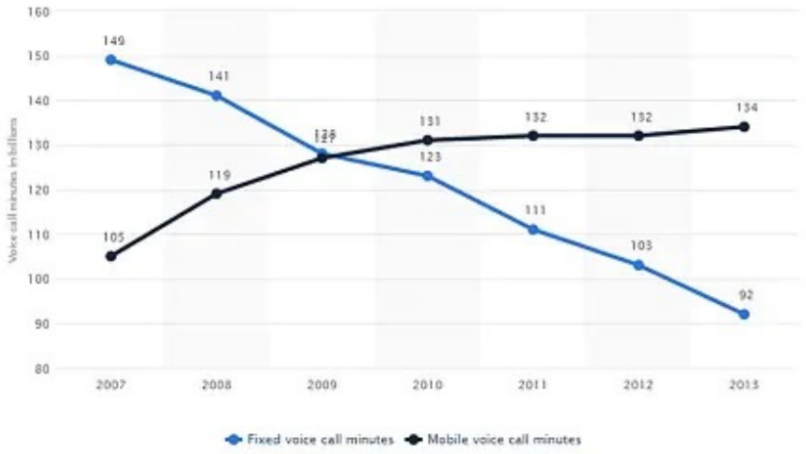
A **Global Passive Adversary** is a type of nation-state behavior that is able to monitor nearly-all traffic on the Internet.

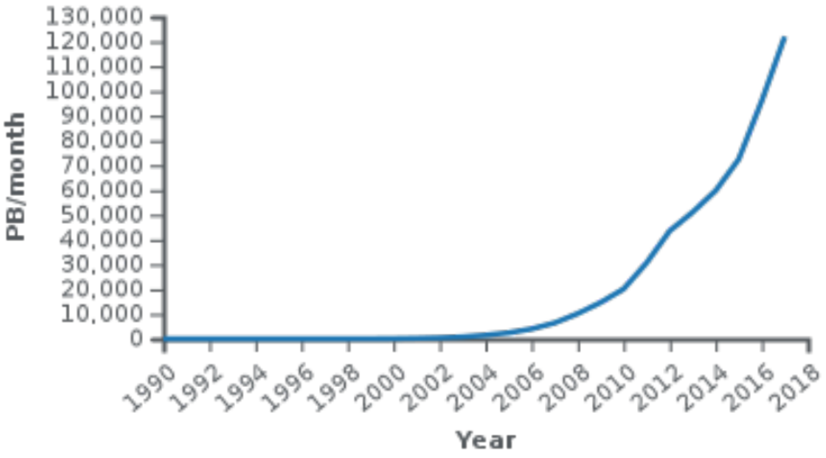
- Do not have full control or insight but effectively do
- Think of a "All-Knowing, Ever-Present Eve"

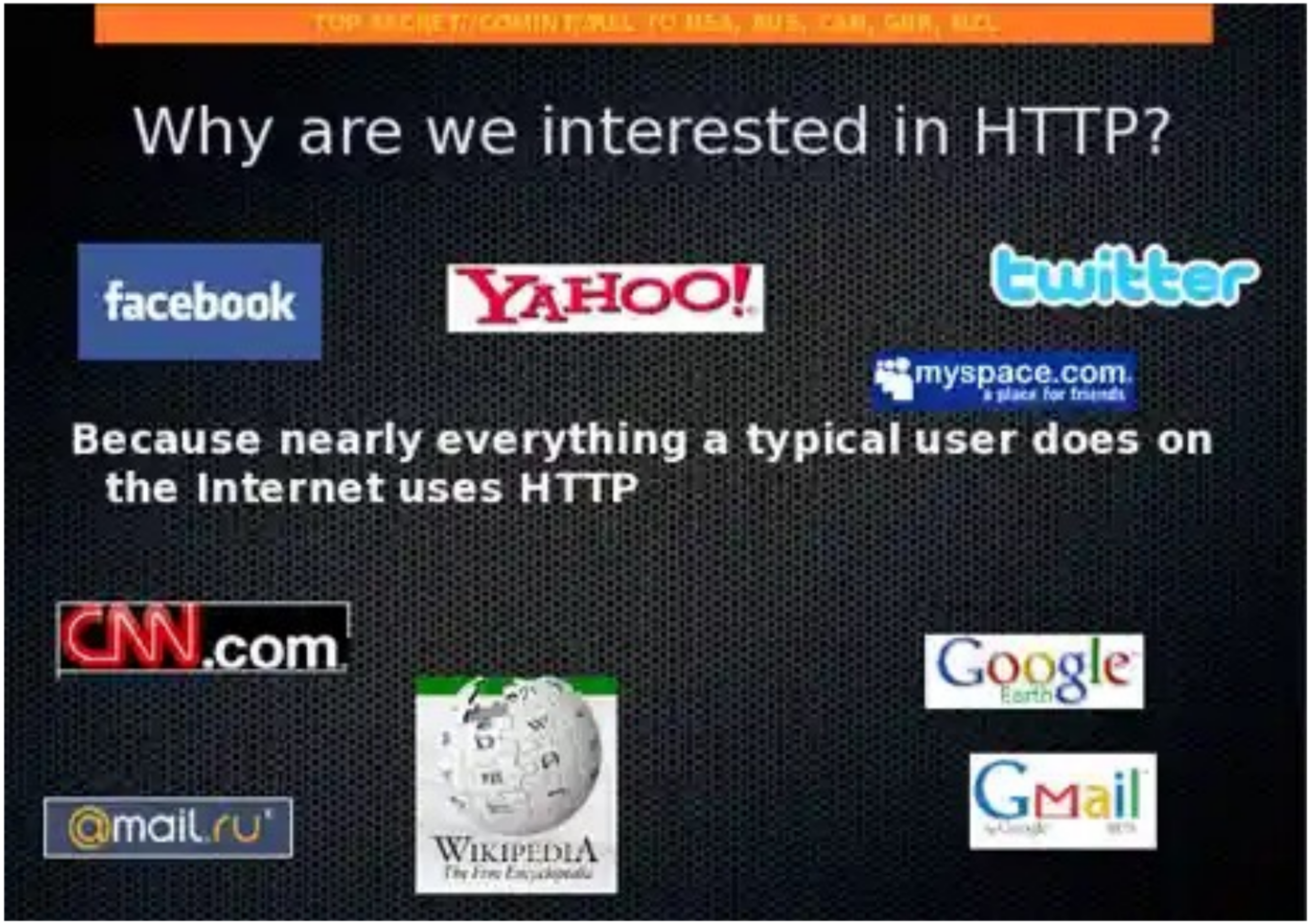
Rise of the Internet

The Internet slowly but surely took over as the primary way to communicate over long-distances and across continents.

Number of total voice call minutes in the United Kingdom (UK) from 2007 to 2013, by fixed and mobile (in billion minutes)







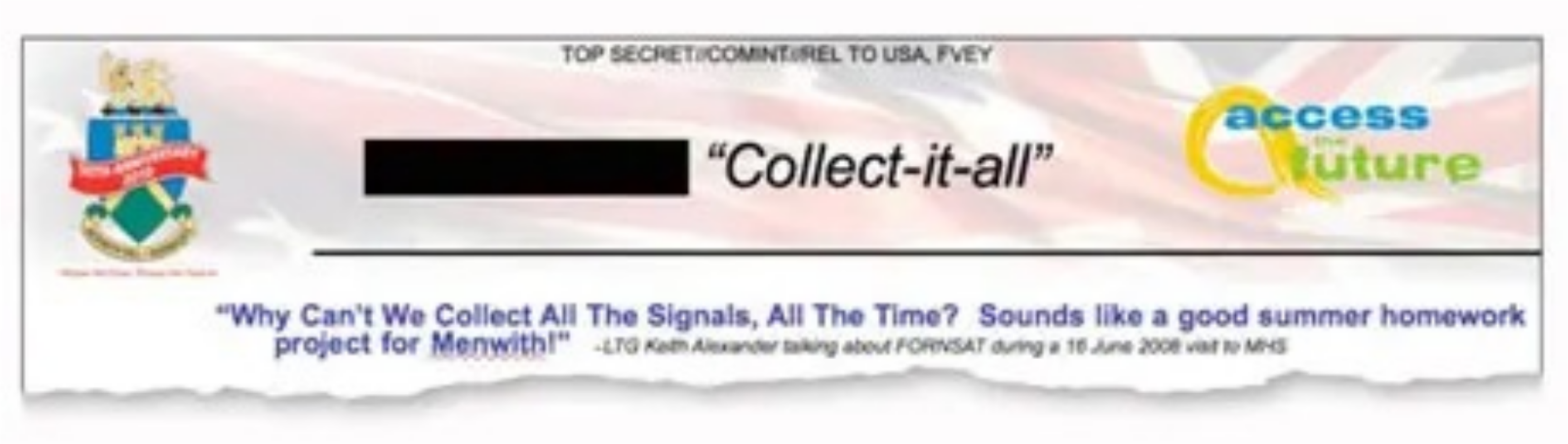
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

Why are we interested in HTTP?

Because nearly everything a typical user does on the Internet uses HTTP

https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data

Bulk Traffic Collection



TOP SECRET//COMINT//REL TO USA, FVEY

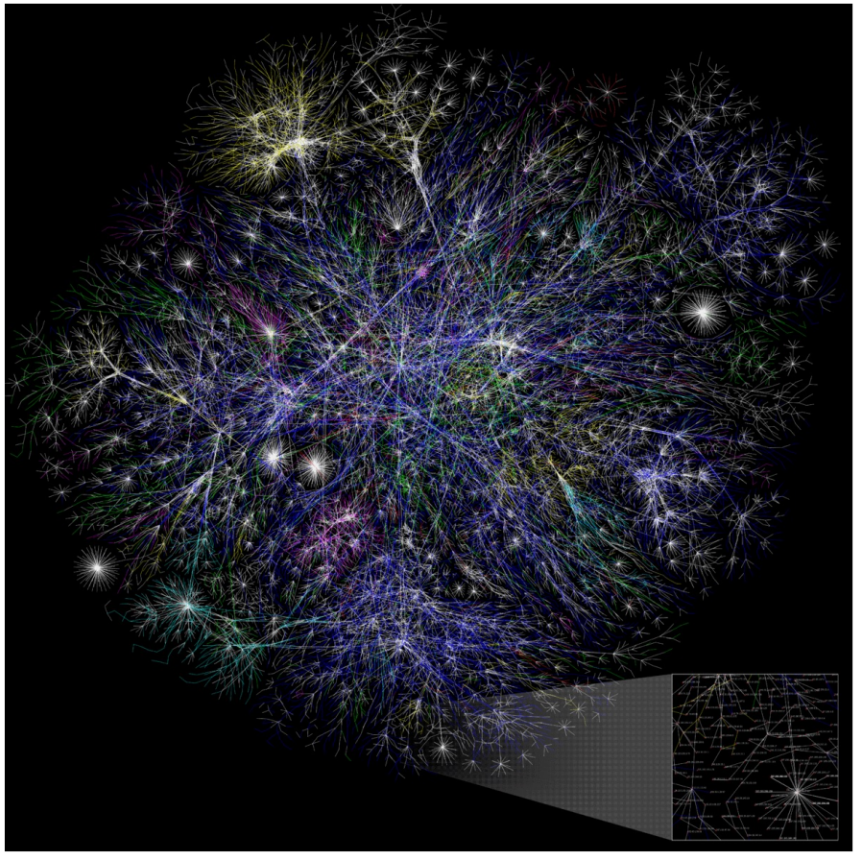
[redacted] "Collect-it-all"

access the future

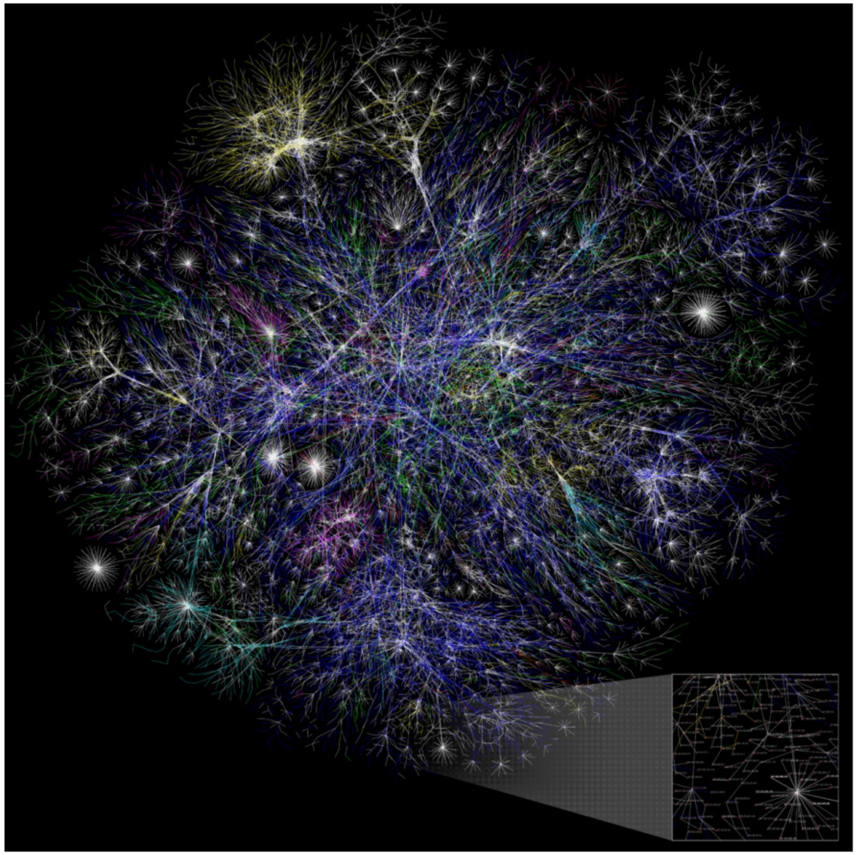
"Why Can't We Collect All The Signals, All The Time? Sounds like a good summer homework project for Menwith!" -LTG Keith Alexander talking about FORNSAT during a 16 June 2008 visit to MHS

https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa

Internet Structure

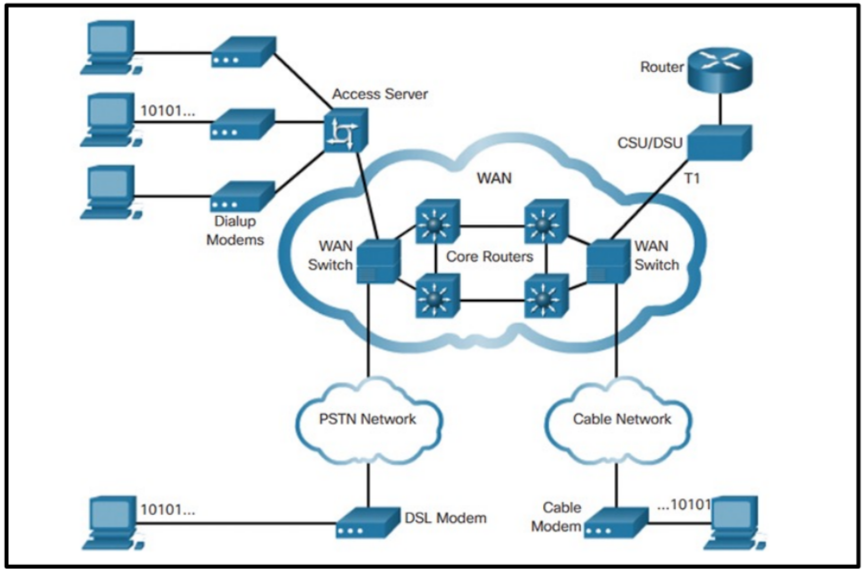


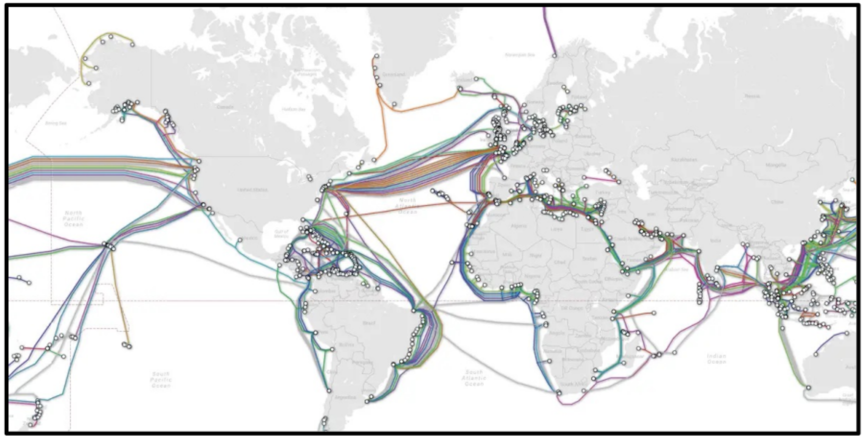
Internet Structure



- The Internet isn't as structured as the telephony network
  - Devices change location
  - Users change location
  - Decentralized by design

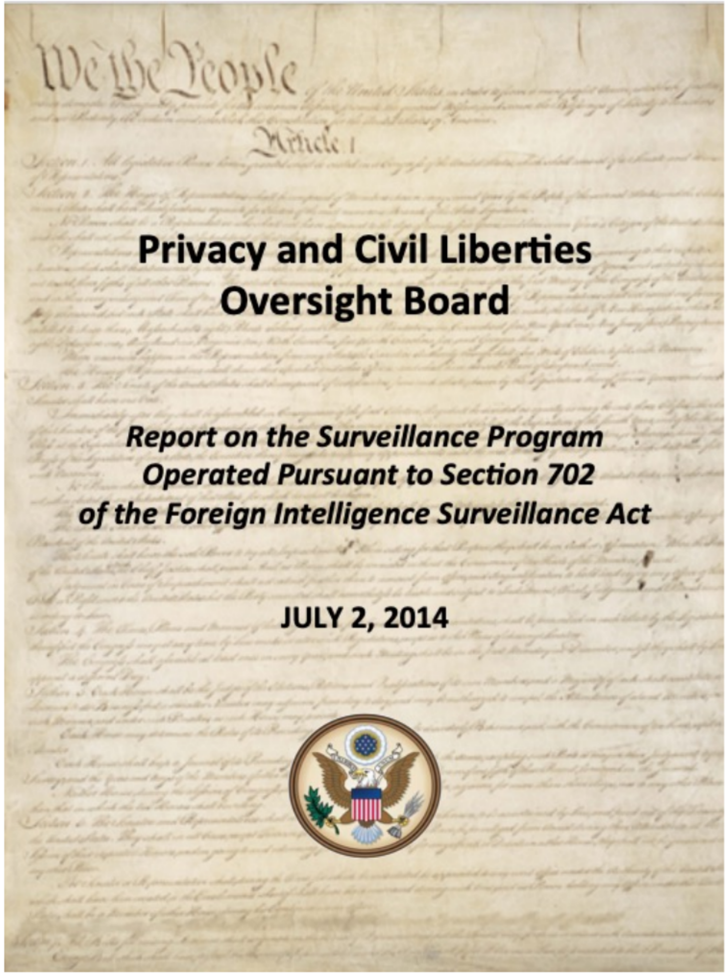
Internet Structure





- The Internet isn’t as structured as the telephony network
  - Devices change location
  - Users change location
  - Decentralized by design
- Internet has structure
- Network choke-points

702 Upstream Program



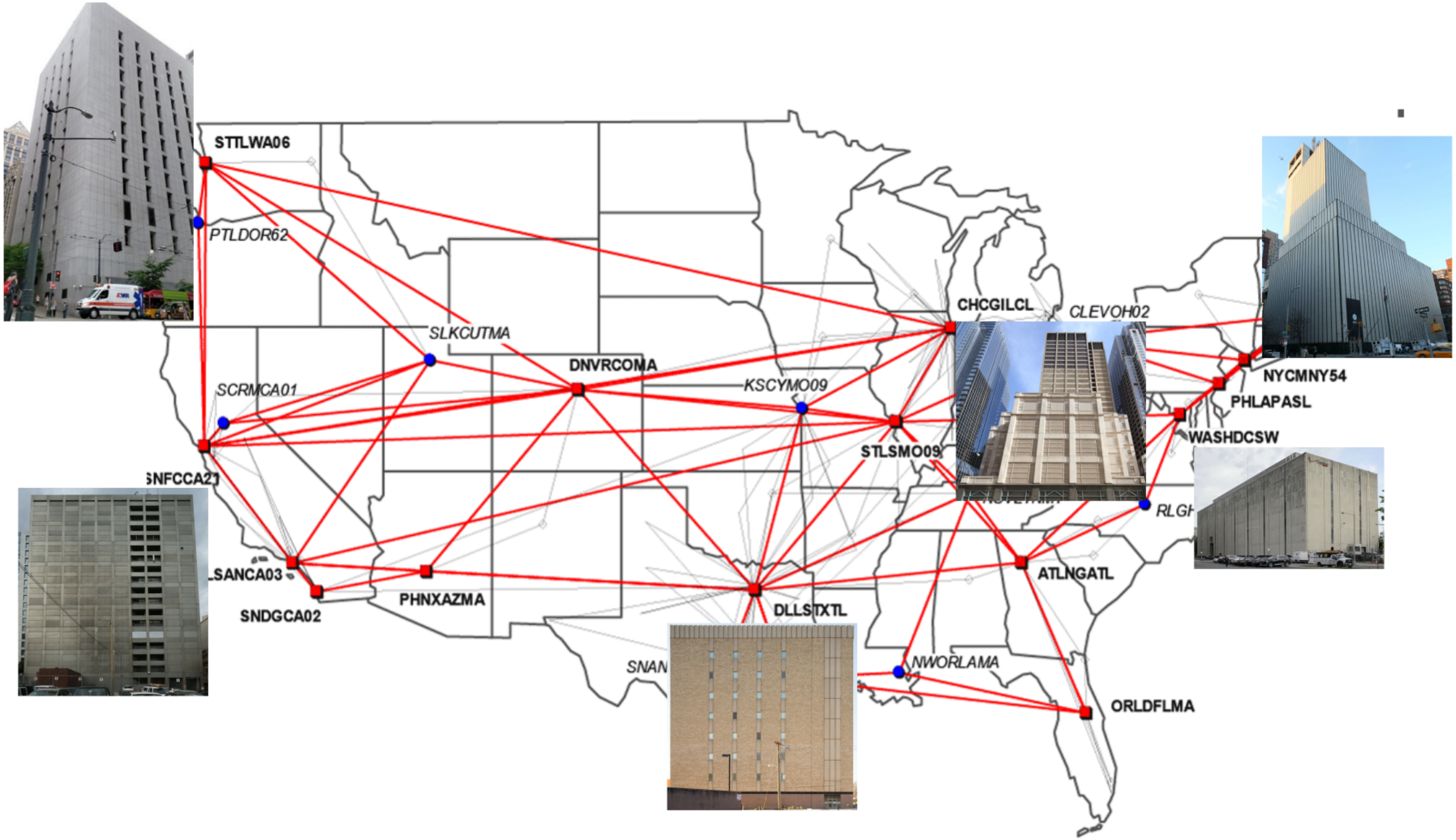
Privacy and Civil Liberties Oversight Board

Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act

JULY 2, 2014

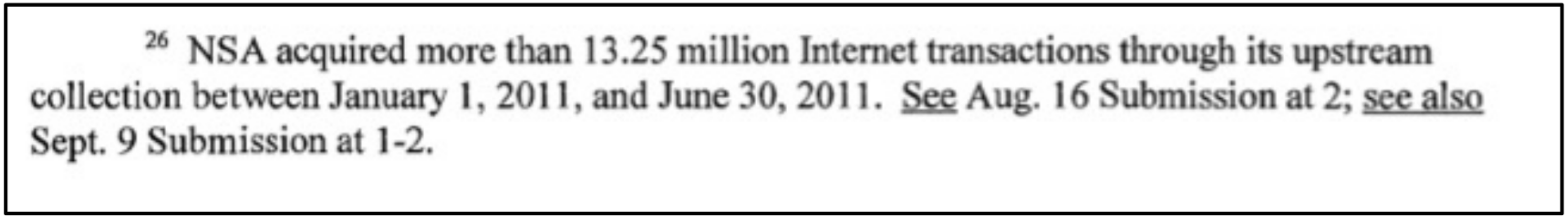
- NSA tapped ISP networks to collect raw network traffic
- “Task” a “selector” to automatically collect
  - Such as email address
- **Not allowed to target US persons**
  - “incidental” collection OK

702 Upstream Program

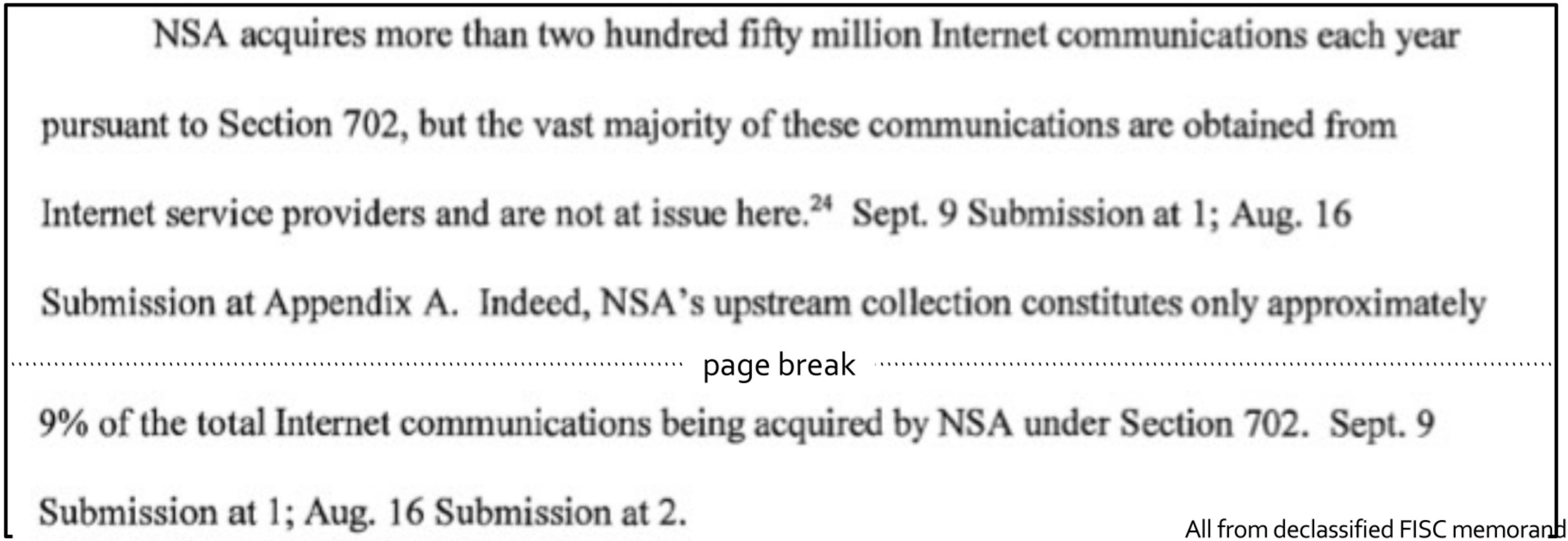


https://theintercept.com/2018/06/25/att-internet-nsa-spy-hubs/
https://mynorthwest.com/1029602/seattle-nsa-spy-hub/?

702 Upstream Program



[26] NSA acquired more than 13.25 million Internet transactions through its upstream collection between January 1, 2011, and June 30, 2011. See Aug. 16 Submission at 2; see also Sept. 9 Submission at 1-2.



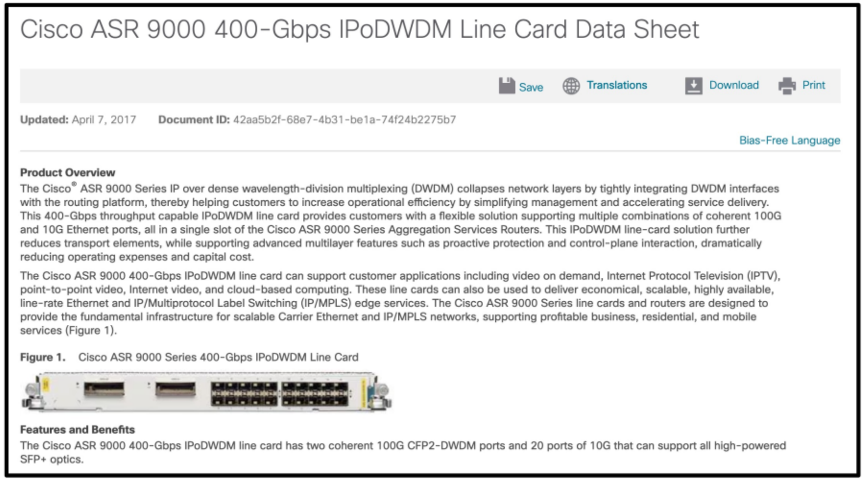
NSA acquires more than two hundred fifty million Internet communications each year pursuant to Section 702, but the vast majority of these communications are obtained from Internet service providers and are not at issue here.[24] Sept. 9 Submission at 1; Aug. 16 Submission at Appendix A. Indeed, NSA's upstream collection constitutes only approximately

page break

9% of the total Internet communications being acquired by NSA under Section 702. Sept. 9 Submission at 1; Aug. 16 Submission at 2.

All from declassified FISC memorandum
https://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf

The Storage Problem



Cisco ASR 9000 400-Gbps IPoDWDM Line Card Data Sheet

Updated: April 7, 2017 **Document ID:** 42aa5b2f-68e7-4b31-be1a-74f24b2275b7

Bias-Free Language

Product Overview

The Cisco® ASR 9000 Series IP over dense wavelength-division multiplexing (DWDM) collapses network layers by tightly integrating DWDM interfaces with the routing platform, thereby helping customers to increase operational efficiency by simplifying management and accelerating service delivery. This 400-Gbps throughput capable IPoDWDM line card provides customers with a flexible solution supporting multiple combinations of coherent 100G and 10G Ethernet ports, all in a single slot of the Cisco ASR 9000 Series Aggregation Services Routers. This IPoDWDM line-card solution further reduces transport elements, while supporting advanced multilayer features such as proactive protection and control-plane interaction, dramatically reducing operating expenses and capital cost.

The Cisco ASR 9000 400-Gbps IPoDWDM line card can support customer applications including video on demand, Internet Protocol Television (IPTV), point-to-point video, Internet video, and cloud-based computing. These line cards can also be used to deliver economical, scalable, highly available, line-rate Ethernet and IP/Multiprotocol Label Switching (IP/MPLS) edge services. The Cisco ASR 9000 Series line cards and routers are designed to provide the fundamental infrastructure for scalable Carrier Ethernet and IP/MPLS networks, supporting profitable business, residential, and mobile services (Figure 1).

Figure 1. Cisco ASR 9000 Series 400-Gbps IPoDWDM Line Card

Features and Benefits

The Cisco ASR 9000 400-Gbps IPoDWDM line card has two coherent 100G CFP2-DWDM ports and 20 ports of 10G that can support all high-powered SFP+ optics.

- @100Gbps:
  - 1 min = 750MB
  - 1 hour = 45TB
  - 1 day = 1PB

The Storage Problem

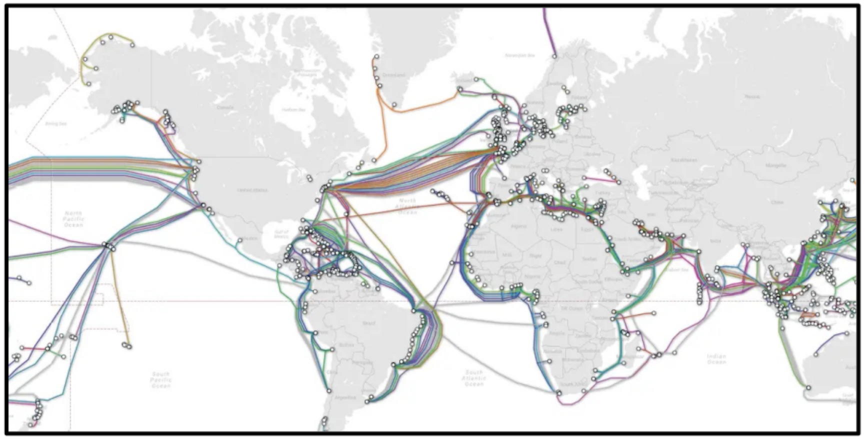
- @100Gbps:
  - 1 min = 750MB
  - 1 hour = 45TB
  - 1 day = 1PB

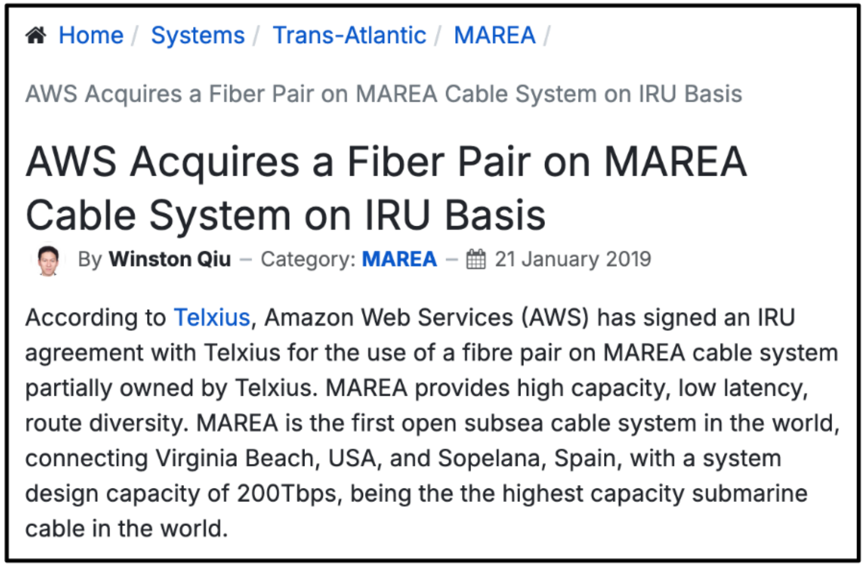
The Storage Problem

NSA's Utah Data Center
Google Maps, Dec2025

- @100Gbps:
  - 1 min = 750MB
  - 1 hour = 45TB
  - 1 day = 1PB

The Storage Problem





🏠 Home / Systems / Trans-Atlantic / MAREA /

AWS Acquires a Fiber Pair on MAREA Cable System on IRU Basis

AWS Acquires a Fiber Pair on MAREA Cable System on IRU Basis

By **Winston Qiu** – Category: **MAREA** – 📅 21 January 2019

According to Telxius, Amazon Web Services (AWS) has signed an IRU agreement with Telxius for the use of a fibre pair on MAREA cable system partially owned by Telxius. MAREA provides high capacity, low latency, route diversity. MAREA is the first open subsea cable system in the world, connecting Virginia Beach, USA, and Sopelana, Spain, with a system design capacity of 200Tbps, being the the highest capacity submarine cable in the world.

- @100Gbps:
  - 1 min = 750MB
  - 1 hour = 45TB
  - 1 day = 1PB
- Under-sea fiber connections operate on 100s of Tbps

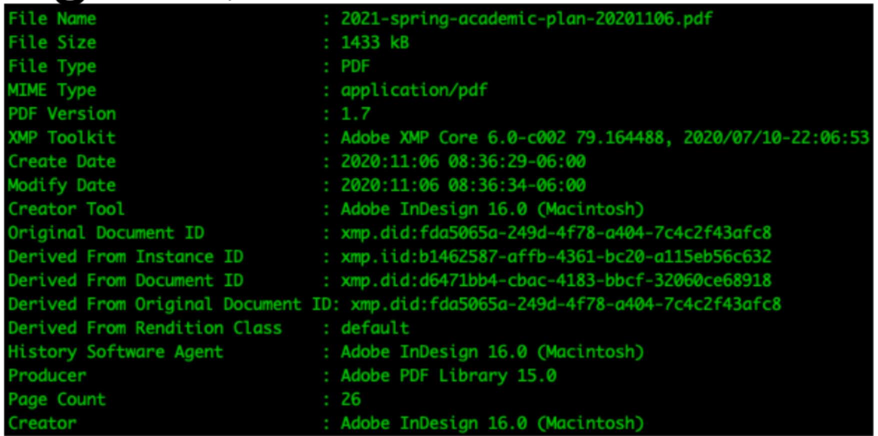
Metadata

Digital **metadata** is any information *about* a digital artifact/object but is explicitly *not* the artifact/object itself.

Metadata

Digital **metadata** is any information *about* a digital artifact/object but is explicitly *not* the artifact/object itself.

- File metadata
  - Author, modify-time, program, etc

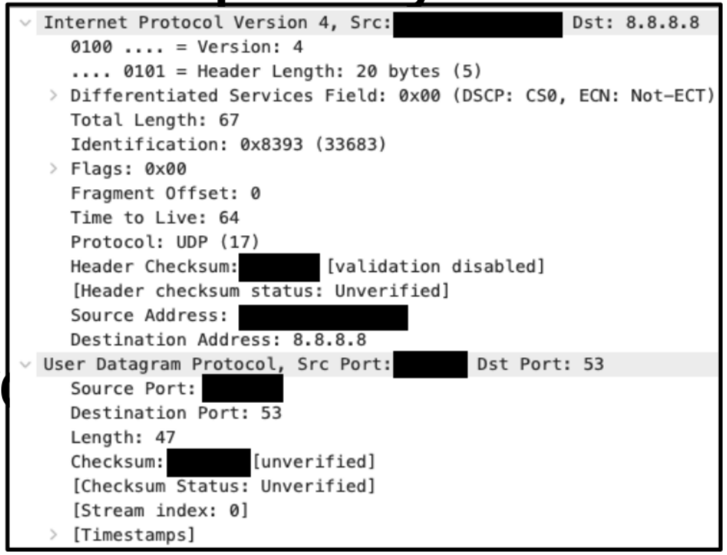


```
File Name                       : 2021-spring-academic-plan-20201106.pdf
File Size                       : 1433 kB
File Type                       : PDF
MIME Type                       : application/pdf
PDF Version                     : 1.7
XMP Toolkit                     : Adobe XMP Core 6.0-c002 79.164488, 2020/07/10-22:06:53
Create Date                     : 2020:11:06 08:36:29-06:00
Modify Date                     : 2020:11:06 08:36:34-06:00
Creator Tool                    : Adobe InDesign 16.0 (Macintosh)
Original Document ID            : xmp.did:fda5065a-249d-4f78-a404-7c4c2f43afc8
Derived From Instance ID        : xmp.iid:b1462587-affb-4361-bc20-a115eb56c632
Derived From Document ID        : xmp.did:d6471bb4-cbac-4183-bbcf-32060ce68918
Derived From Original Document ID: xmp.did:fda5065a-249d-4f78-a404-7c4c2f43afc8
Derived From Rendition Class    : default
History Software Agent          : Adobe InDesign 16.0 (Macintosh)
Producer                        : Adobe PDF Library 15.0
Page Count                      : 26
Creator                         : Adobe InDesign 16.0 (Macintosh)
```

Metadata

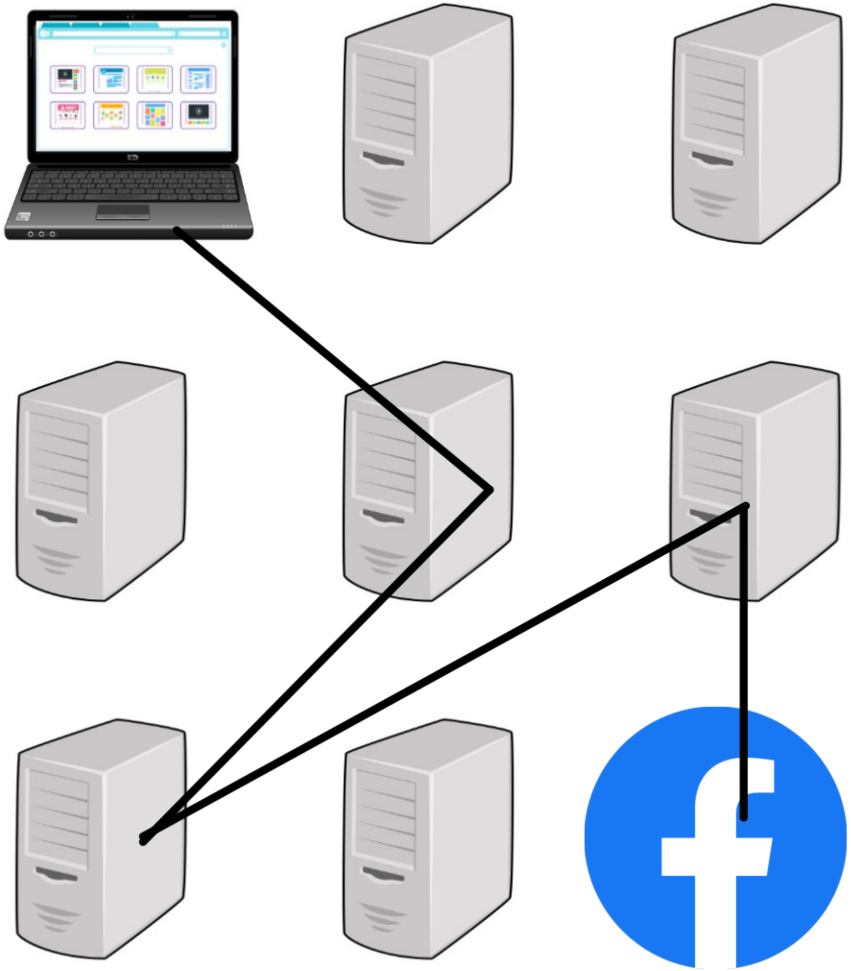
Digital **metadata** is any information *about* a digital artifact/object but is explicitly *not* the artifact/object itself.

- File metadata
  - Author, modify-time, pr
- Network metadata
  - TCP/IP headers, location, size, etc



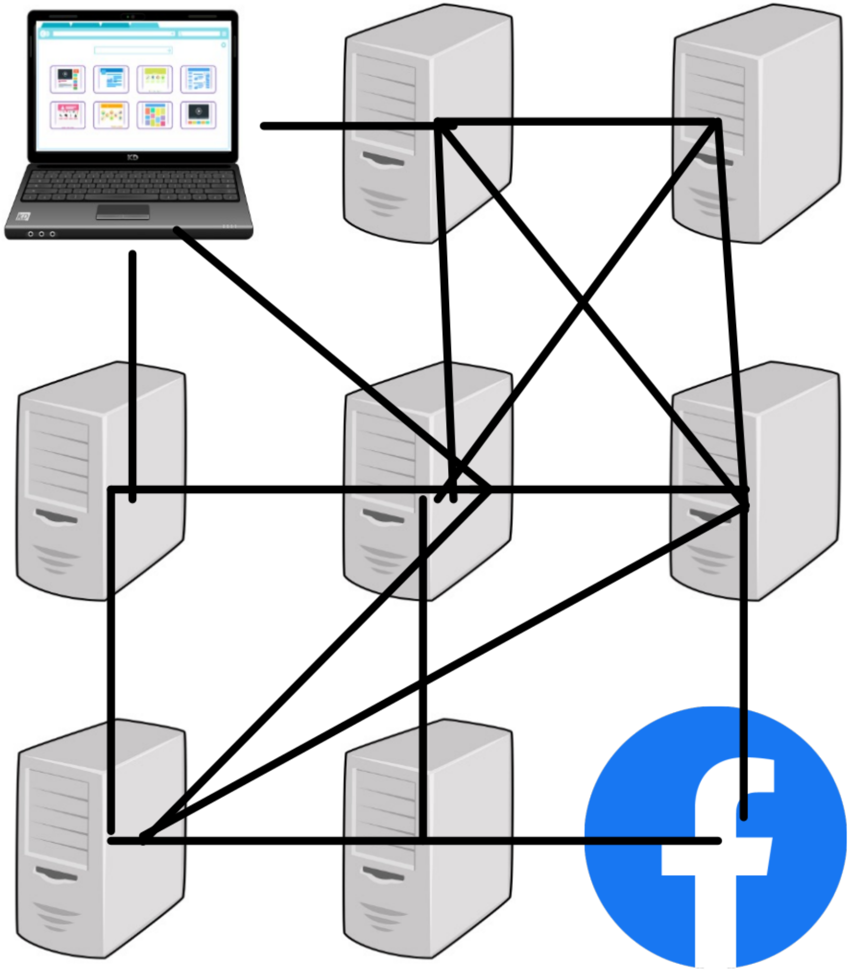
```
⌄ Internet Protocol Version 4, Src: [redacted] Dst: 8.8.8.8
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  › Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 67
    Identification: 0x8393 (33683)
  › Flags: 0x00
    Fragment Offset: 0
    Time to Live: 64
    Protocol: UDP (17)
    Header Checksum: [redacted] [validation disabled]
    [Header checksum status: Unverified]
    Source Address: [redacted]
    Destination Address: 8.8.8.8
⌄ User Datagram Protocol, Src Port: [redacted] Dst Port: 53
    Source Port: [redacted]
    Destination Port: 53
    Length: 47
    Checksum: [redacted] [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  › [Timestamps]
```

Metadata Correlation Attacks



A **Correlation Attack** is a type of side-channel that uses metadata to deanonymize traffic.

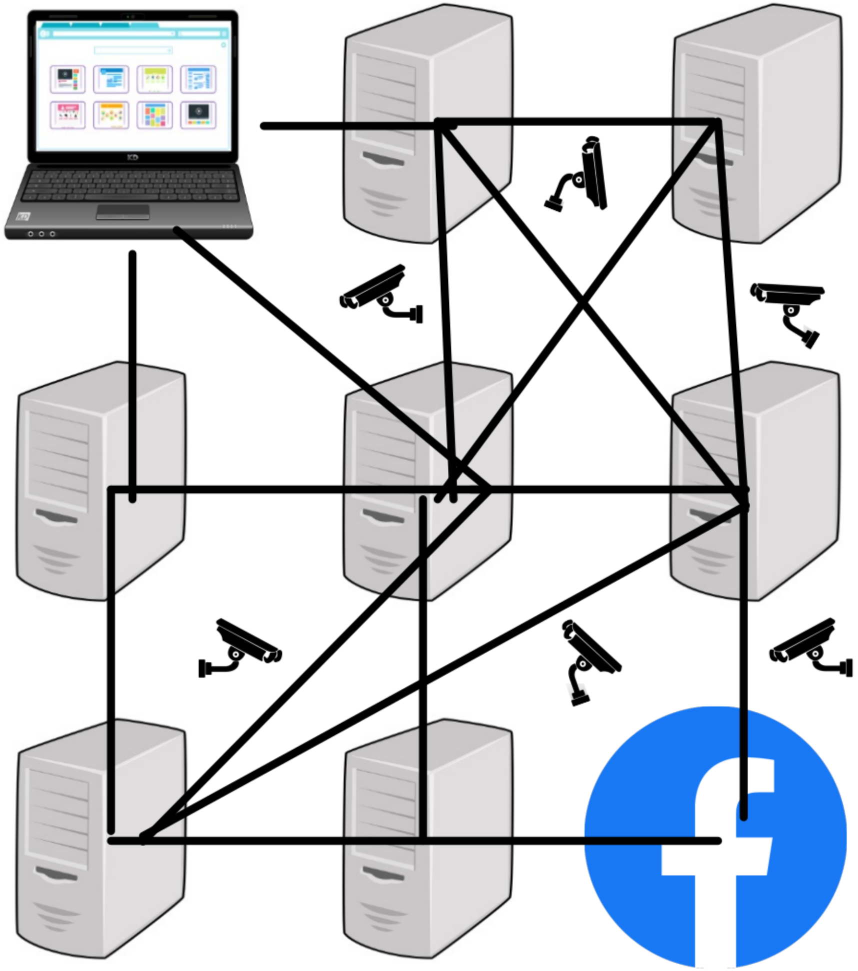
Metadata Correlation Attacks



A **Correlation Attack** is a type of side-channel that uses metadata to deanonymize traffic.

- Only needs 1 identifiable aspect
  - Packet size
  - Packet count
  - Packet timing

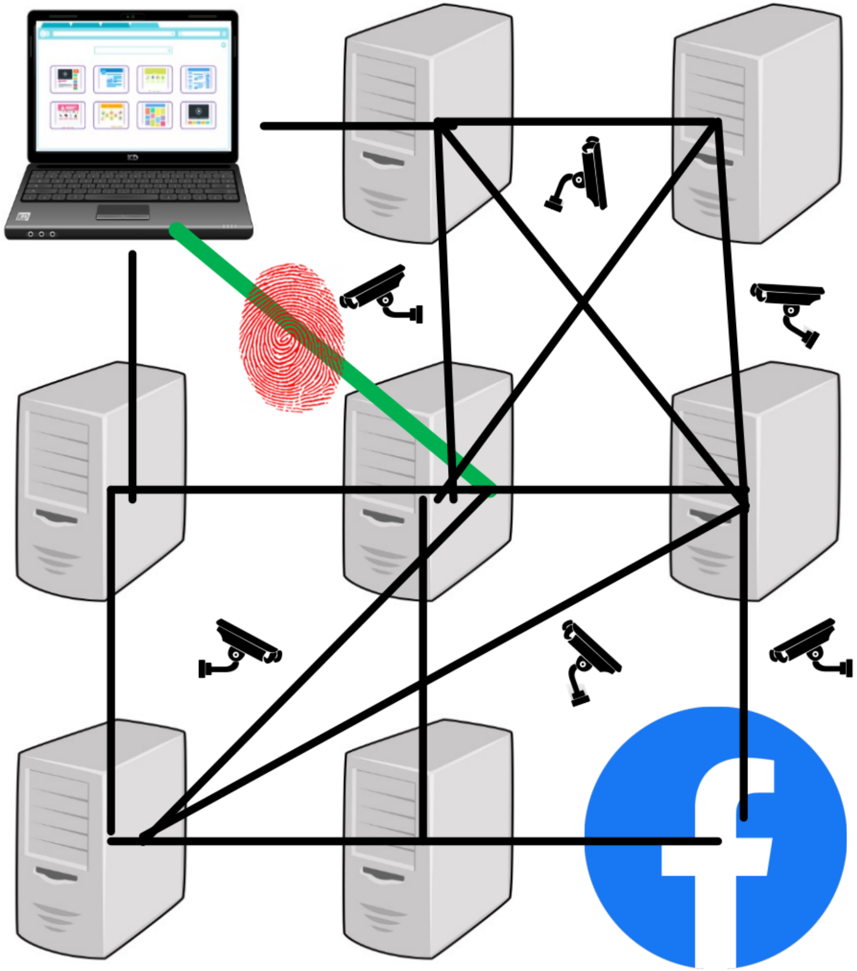
Metadata Correlation Attacks



A **Correlation Attack** is a type of side-channel that uses metadata to deanonymize traffic.

- Onl
  id

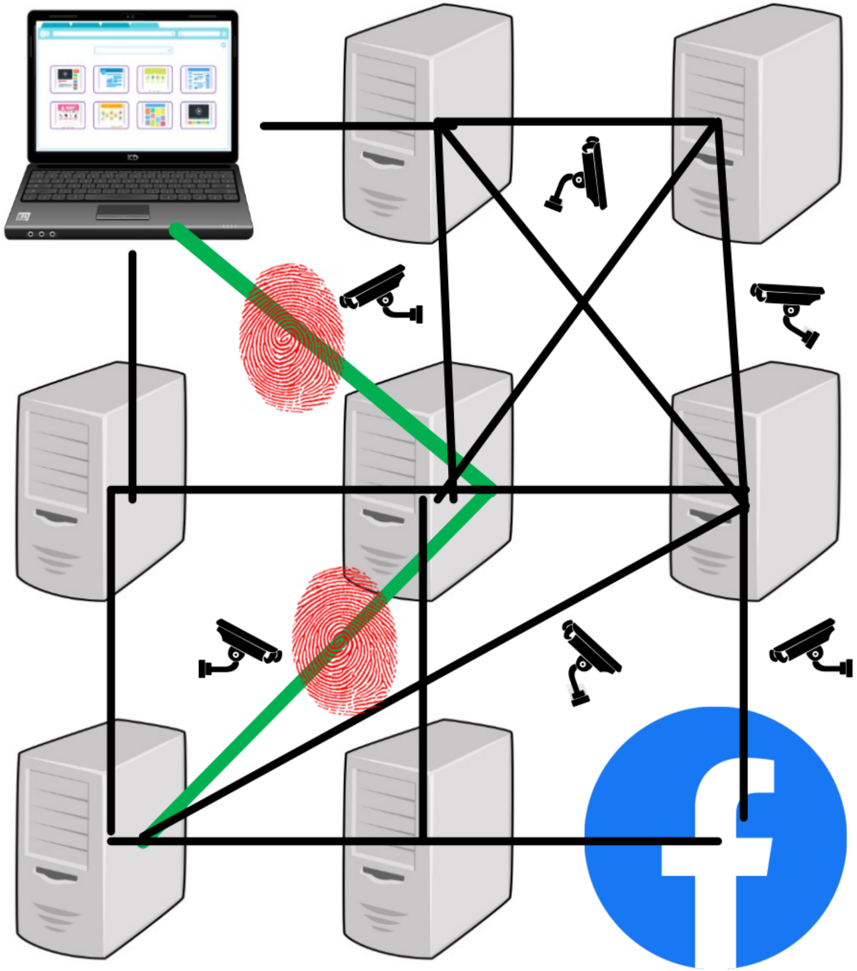
Metadata Correlation Attacks



A **Correlation Attack** is a type of side-channel that uses metadata to deanonymize traffic.

- Only needs 1 identifiable aspect
  - Packet size
  - Packet count
  - Packet timing

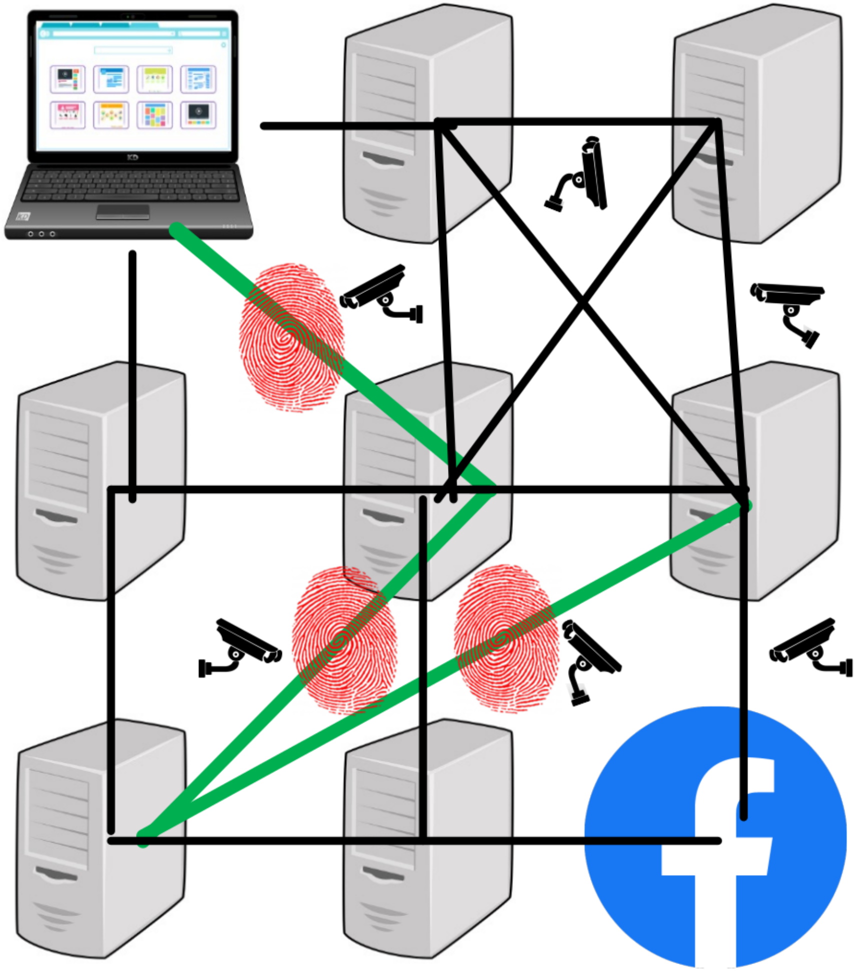
Metadata Correlation Attacks



A **Correlation Attack** is a type of side-channel that uses metadata to deanonymize traffic.

- Only needs 1 identifiable aspect
  - Packet size
  - Packet count
  - Packet timing

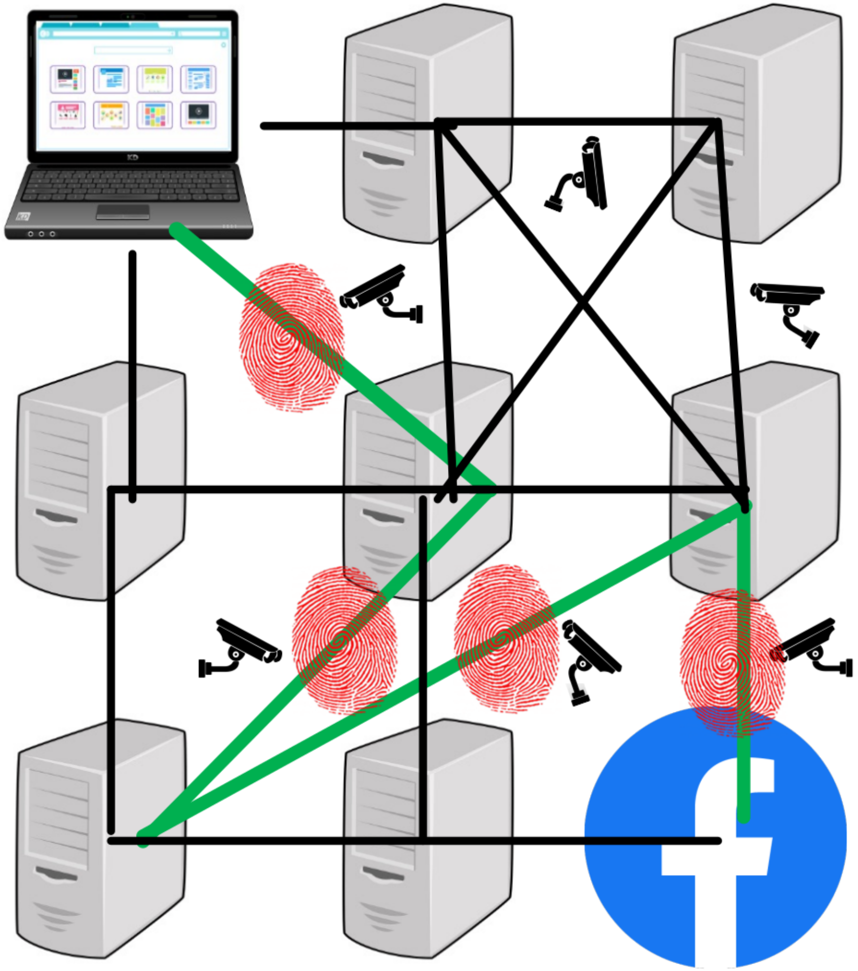
Metadata Correlation Attacks



A **Correlation Attack** is a type of side-channel that uses metadata to deanonymize traffic.

- Only needs 1 identifiable aspect
  - Packet size
  - Packet count
  - Packet timing

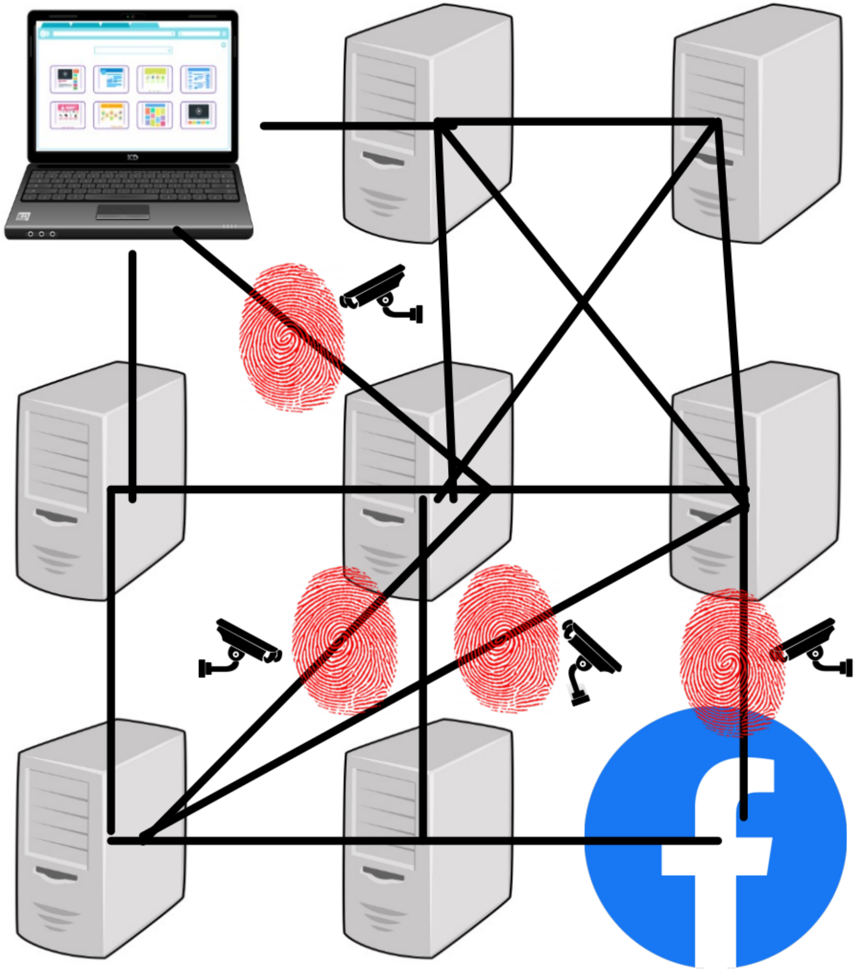
Metadata Correlation Attacks



A **Correlation Attack** is a type of side-channel that uses metadata to deanonymize traffic.

- Only needs 1 identifiable aspect
  - Packet size
  - Packet count
  - Packet timing

Metadata Correlation Attacks



A **Correlation Attack** is a type of side-channel that uses metadata to deanonymize traffic.

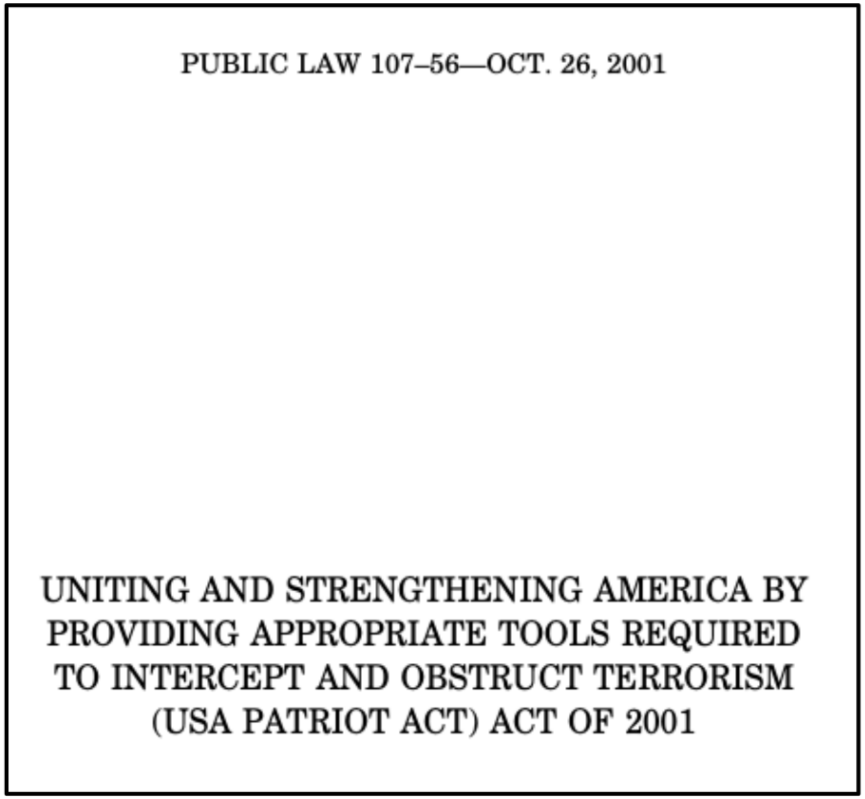
- Only needs 1 identifiable aspect
  - Packet size
  - Packet count
  - Packet timing

Metadata

Digital **metadata** is any information *about* a digital artifact/object but is explicitly *not* the artifact/object itself.

- File metadata
  - Author, modify-time, program, etc
- Network metadata
  - TCP/IP headers, location, size, etc
- Service-side records
  - Billing data, advertising data, etc

Oct 2001: USA Patriot Act



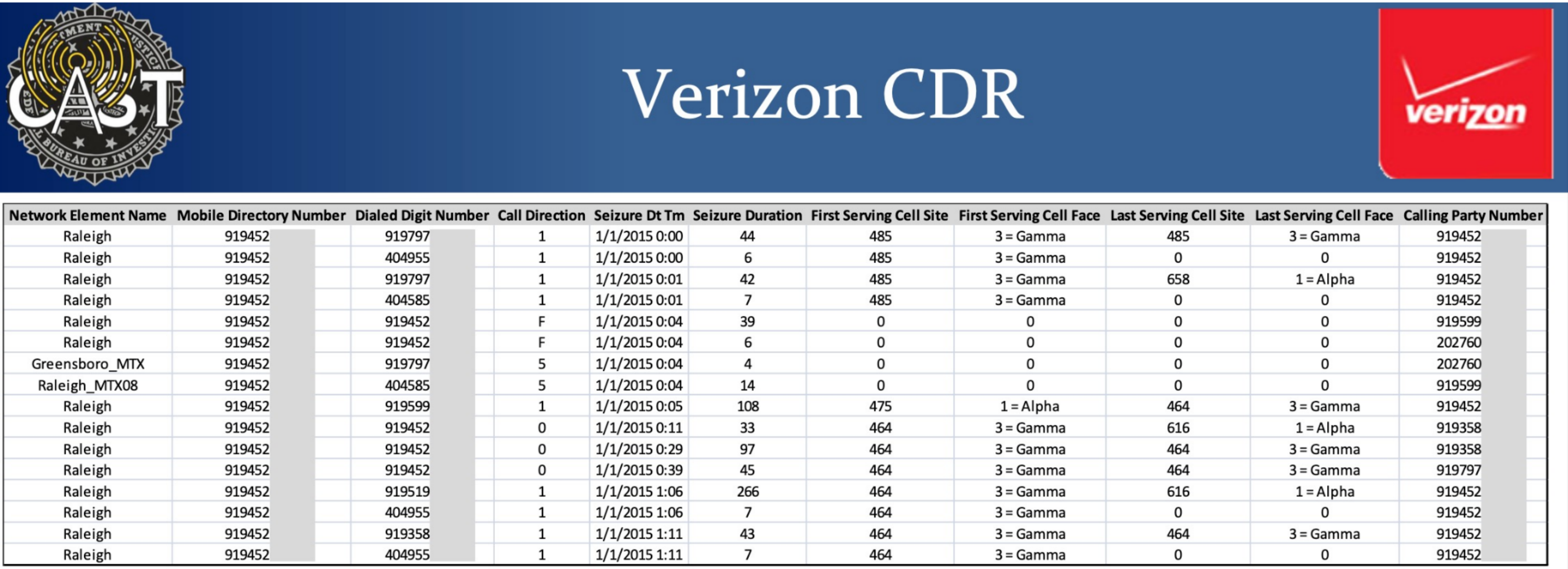
PUBLIC LAW 107–56—OCT. 26, 2001

UNITING AND STRENGTHENING AMERICA BY
PROVIDING APPROPRIATE TOOLS REQUIRED
TO INTERCEPT AND OBSTRUCT TERRORISM
(USA PATRIOT ACT) ACT OF 2001

- Major rule changes on Law Enforcement access to information
- **Major focus on “Tangible things” and “Business Records”**

Call Detail Records (CDRs)

Call Detail Records (CDRs) are metadata about a phone call but not contents.

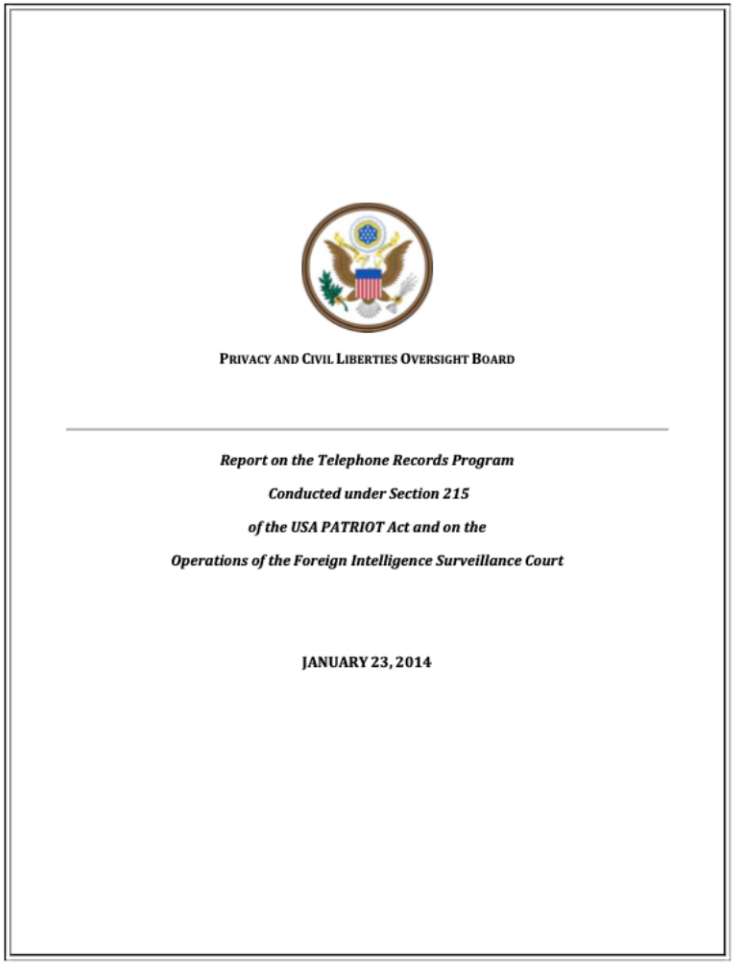


Verizon CDR

Network Element Name	Mobile Directory Number	Dialed Digit Number	Call Direction	Seizure Dt Tm	Seizure Duration	First Serving Cell Site	First Serving Cell Face	Last Serving Cell Site	Last Serving Cell Face	Calling Party Number
Raleigh	919452 [redacted]	919797 [redacted]	1	1/1/2015 0:00	44	485	3 = Gamma	485	3 = Gamma	919452 [redacted]
Raleigh	919452 [redacted]	404955 [redacted]	1	1/1/2015 0:00	6	485	3 = Gamma	0	0	919452 [redacted]
Raleigh	919452 [redacted]	919797 [redacted]	1	1/1/2015 0:01	42	485	3 = Gamma	658	1 = Alpha	919452 [redacted]
Raleigh	919452 [redacted]	404585 [redacted]	1	1/1/2015 0:01	7	485	3 = Gamma	0	0	919452 [redacted]
Raleigh	919452 [redacted]	919452 [redacted]	F	1/1/2015 0:04	39	0	0	0	0	919599 [redacted]
Raleigh	919452 [redacted]	919452 [redacted]	F	1/1/2015 0:04	6	0	0	0	0	202760 [redacted]
Greensboro_MTX	919452 [redacted]	919797 [redacted]	5	1/1/2015 0:04	4	0	0	0	0	202760 [redacted]
Raleigh_MTX08	919452 [redacted]	404585 [redacted]	5	1/1/2015 0:04	14	0	0	0	0	919599 [redacted]
Raleigh	919452 [redacted]	919599 [redacted]	1	1/1/2015 0:05	108	475	1 = Alpha	464	3 = Gamma	919452 [redacted]
Raleigh	919452 [redacted]	919452 [redacted]	0	1/1/2015 0:11	33	464	3 = Gamma	616	1 = Alpha	919358 [redacted]
Raleigh	919452 [redacted]	919452 [redacted]	0	1/1/2015 0:29	97	464	3 = Gamma	464	3 = Gamma	919358 [redacted]
Raleigh	919452 [redacted]	919452 [redacted]	0	1/1/2015 0:39	45	464	3 = Gamma	464	3 = Gamma	919797 [redacted]
Raleigh	919452 [redacted]	919519 [redacted]	1	1/1/2015 1:06	266	464	3 = Gamma	616	1 = Alpha	919452 [redacted]
Raleigh	919452 [redacted]	404955 [redacted]	1	1/1/2015 1:06	7	464	3 = Gamma	0	0	919452 [redacted]
Raleigh	919452 [redacted]	919358 [redacted]	1	1/1/2015 1:11	43	464	3 = Gamma	464	3 = Gamma	919452 [redacted]
Raleigh	919452 [redacted]	404955 [redacted]	1	1/1/2015 1:11	7	464	3 = Gamma	0	0	919452 [redacted]

https://propertyofthepeople.org/document-detail/?doc-id=21088576

215 Telephony Metadata Program



PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

Report on the Telephone Records Program

Conducted under Section 215

of the USA PATRIOT Act and on the

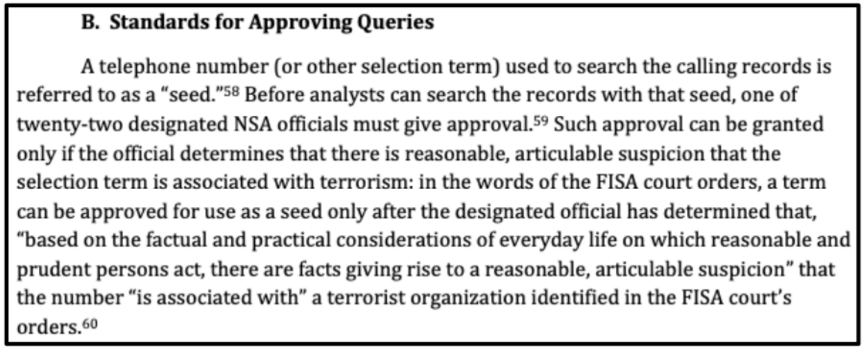
Operations of the Foreign Intelligence Surveillance Court

JANUARY 23, 2014

https://www.dni.gov/files/CLPT/documents/2019_ASTR_for_CY2018.pdf

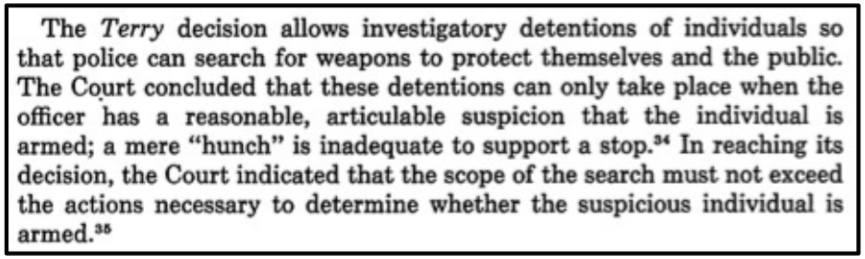
- Bulk collection of all CDRs to/from/in the US
  - Billions per day

215 Telephony Metadata Program



B. Standards for Approving Queries

A telephone number (or other selection term) used to search the calling records is referred to as a "seed."[58] Before analysts can search the records with that seed, one of twenty-two designated NSA officials must give approval.[59] Such approval can be granted only if the official determines that there is reasonable, articulable suspicion that the selection term is associated with terrorism: in the words of the FISA court orders, a term can be approved for use as a seed only after the designated official has determined that, "based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are facts giving rise to a reasonable, articulable suspicion" that the number "is associated with" a terrorist organization identified in the FISA court's orders.[60]



The *Terry* decision allows investigatory detentions of individuals so that police can search for weapons to protect themselves and the public. The Court concluded that these detentions can only take place when the officer has a reasonable, articulable suspicion that the individual is armed; a mere "hunch" is inadequate to support a stop.[34] In reaching its decision, the Court indicated that the scope of the search must not exceed the actions necessary to determine whether the suspicious individual is armed.[35]

- Bulk collection of all CDRs to/from/in the US
  - Billions per day
- Query own database if have "reasonable articulable suspicion" of crime
  - No warrant/subpoena/judge

https://documents.pclob.gov/prod/Documents/OversightReport/ec542143-1079-424a-84b3-acc354698560/215-Report_on_the_Telephone_Records_Program.pdf
https://scholarship.richmond.edu/cgi/viewcontent.cgi?article=1944&context=lawreview

215 Telephony Metadata Program

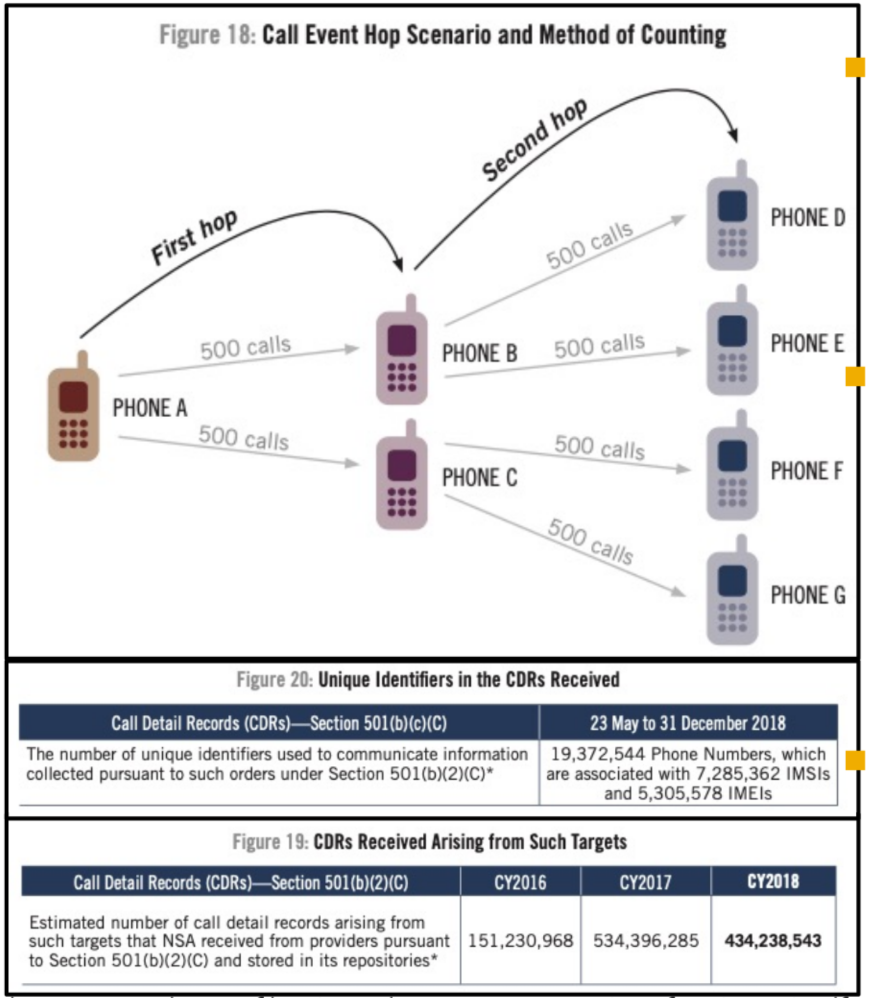


Figure 18: **Call Event Hop Scenario and Method of Counting**

Figure 20: **Unique Identifiers in the CDRs Received**

Call Detail Records (CDRs)—Section 501(b)(c)(C)	23 May to 31 December 2018
The number of unique identifiers used to communicate information collected pursuant to such orders under Section 501(b)(2)(C)*	19,372,544 Phone Numbers, which are associated with 7,285,362 IMSIs and 5,305,578 IMEIs

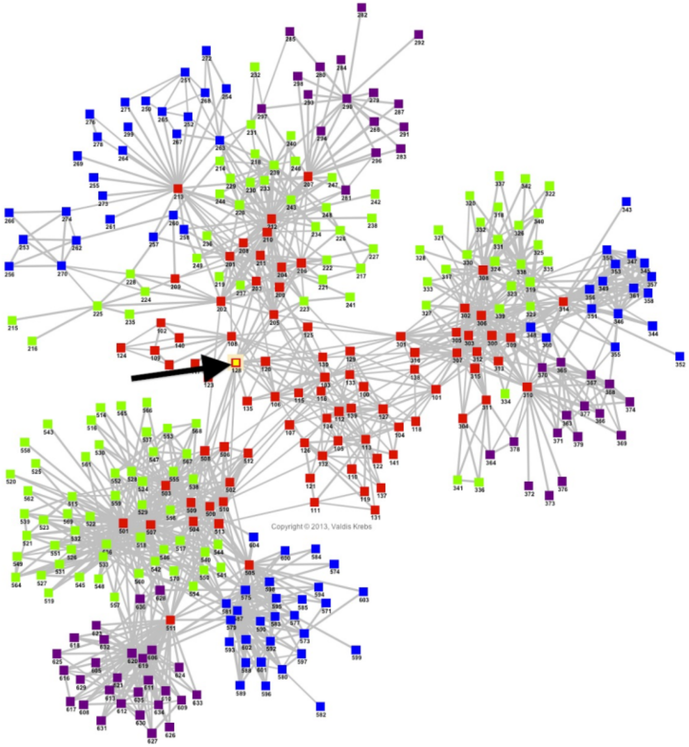
Figure 19: **CDRs Received Arising from Such Targets**

Call Detail Records (CDRs)—Section 501(b)(2)(C)	CY2016	CY2017	CY2018
Estimated number of call detail records arising from such targets that NSA received from providers pursuant to Section 501(b)(2)(C) and stored in its repositories*	151,230,968	534,396,285	**434,238,543**

https://www.dni.gov/files/CLPT/documents/2019_ASTR_for_CY2018.pdf

- Bulk collection of all CDRs to/from/in the US
  - Billions per day
- Query own database if have “reasonable articulable suspicion” of crime
  - No warrant/subpoena/judge
- Allowed to chain multiple layers of people
  - Root at seed number
  - 2/3 “hops” from “seed” number

Contact Chaining



Copyright © 2013, Valdis Krebs

Contact Chaining is a technique in which digital metadata allows recovery of social-graph

- Useful in locating cliques and hidden members of groups
- *Alice, Bob, Charlie call each other a lot*

Computer and Network Security

Lecture 28: Surveillance

Fall 2025
COMP-5370/6370