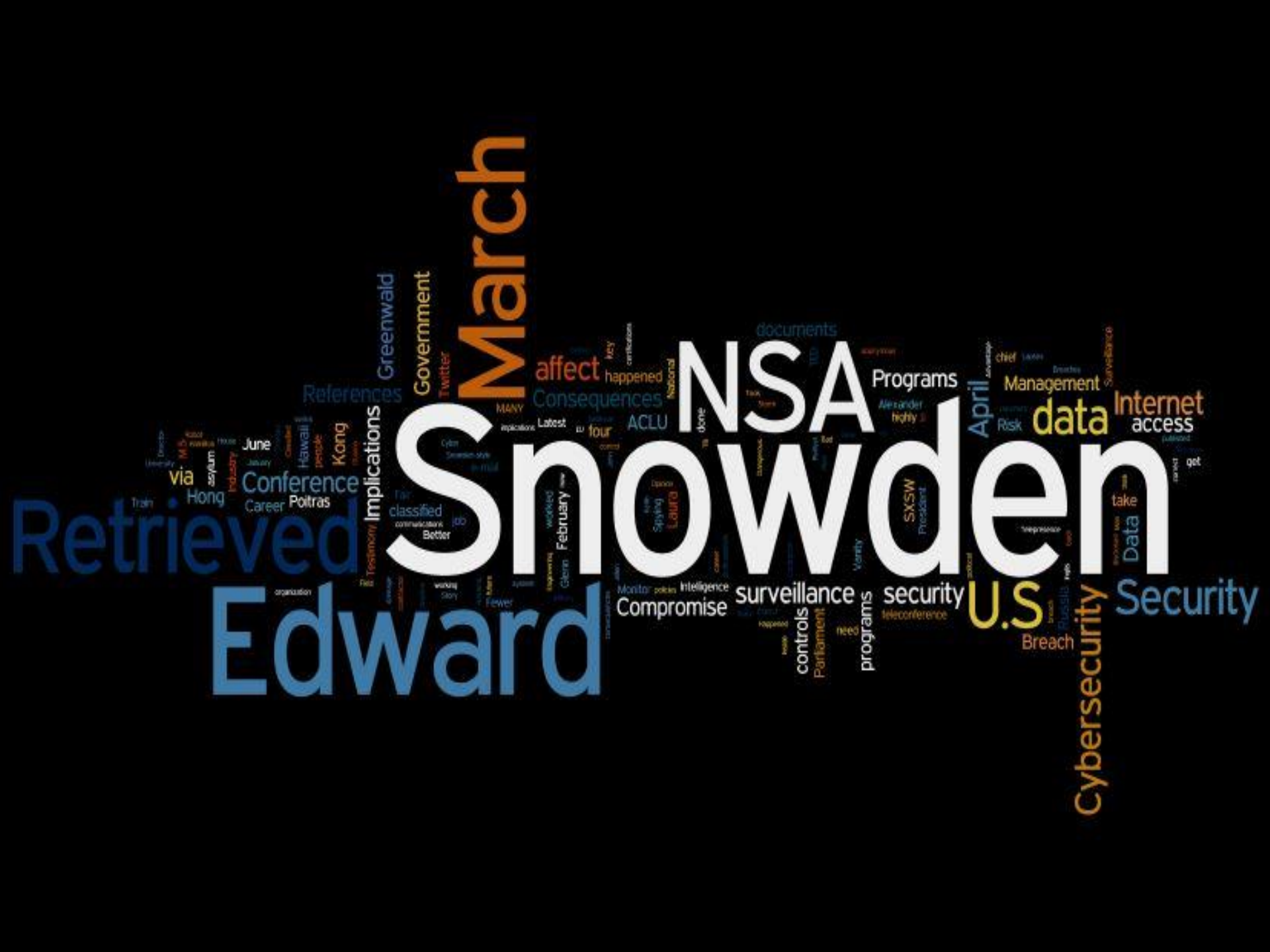
ASIS Illinois North Shore Chapter
Advancing Security Worldwide

Photo Credit:
Wired Magazine
August 13, 2014


Snowden
Edward
Retrieved
March
NSA
Greenwald
Government
References
Twitter
affect
happened
Consequences
MANY
Latest
four
ACLU
documents
Programs
Management
April
Risk
data
Internet
access
Implications
June
Hawaii
Kong
via
Hong
Conference
Career
Poitras
classified
Better
February
Laura
SXSW
take
Data
Monitor
Intelligence
Compromise
surveillance
security
U.S
Security
Cybersecurity
Breach
controls
Parliament
programs
need
Fewer

The Edward Snowden NSA Data Breach of 2013: How it Happened; Its Consequences & Implications

for the U.S. and the IT Industry and the Security Industry

William Favre Slater, III, M.S. MBA, PMP, CISSP, CISA
Owner, Slater Technologies, Inc.
Adjunct Professor, IIT School of Applied Technology
A Presentation for ASIS Northshore Illinois Chapter
August 14, 2014

ILLINOIS INSTITUTE OF TECHNOLOGY

Presentation Location

http://1drv.ms/1oF3LU0

ILLINOIS INSTITUTE OF TECHNOLOGY

WAKE UP AMERICA

"In the end the Obama administration is not afraid of whistleblowers like me, Bradley Manning or Thomas Drake. We are stateless, imprisoned and powerless. No the Obama administration is afraid of you. It is afraid of an informed, angry public demanding the constitutional Government it was promised - and it should be."

- Edward Joseph Snowden

Politifake.org

Edward Snowden's Christmas Message to America, December 2013

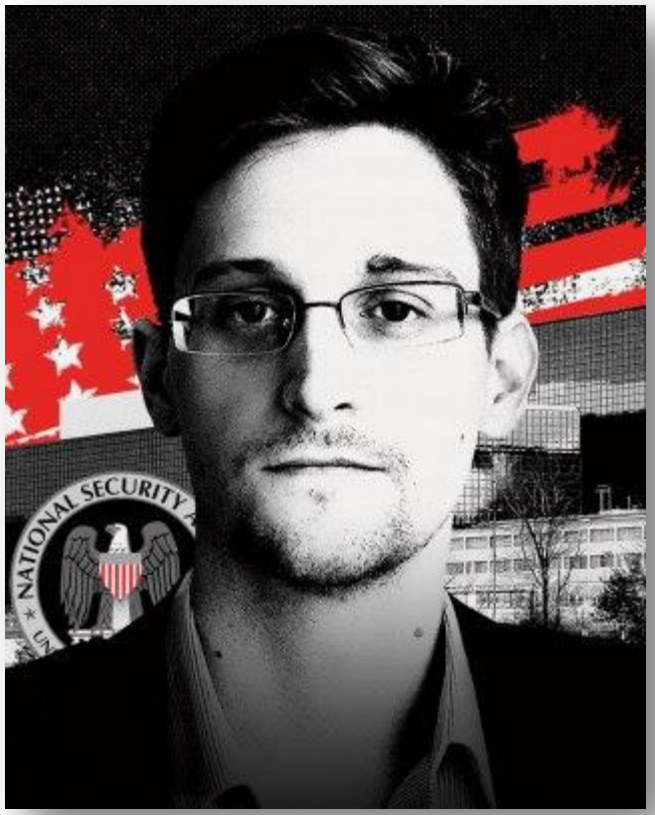
Agenda

- **Introduction**
- **What Happened?** What Did Edward Snowden Do?
- **How** did he accomplish this?
- **What** has he disclosed?
- **Consequences**
- **Implications**
- **The Latest Developments** on Edward Snowden
- **Audience Opinion:** Do you think Edward Snowden was correct in doing what he did?
- **Latest Developments on Snowden and Other Stuff**
- **My Own Assessments**
- **NSA Fallout**
- **Conclusion**
- **Questions**
- **References**

ILLINOIS INSTITUTE OF TECHNOLOGY

Introduction

- The Edward Snowden 2013 NSA Data Breach was arguably the most damaging (known) data breach to ever impact the U.S. Intelligence Community. This presentation will cover what happened, how it happened, why it happened, the data breach's consequences, its implications for the future, and how such breaches can be prevented in the future.



Edward Snowden
Vanity Fair Artwork

ILLINOIS INSTITUTE OF TECHNOLOGY

Some Previous Bad Security Breaches

A BRIEF HISTORY OF TOP SECURITY BREACHES

Data security has been a concern since the dawn of the spoken word, and breaches throughout history have led to both good and bad results for society. Today, with our information being mostly digital, hacks have become even more common. Employment of information security analysts, web developers and computer network architects is projected to grow 22% from 2010 to 2020[1] — faster than the average for all occupations. So, when did these data breaks begin? Here are some of history's top information breaches.

1600

THE GUNPOWDER PLOT
November 5, 1605
A scheme to kill King James I using 36 barrels of gunpowder that Guy Fawkes was guarding was uncovered.

1700

CASANOVA
Spies for Venetian Inquisitors
1774—1783
Casanova spied for the Venetian Inquisitors of State.

THE MIDNIGHT RIDE
April 18, 1775
Paul Revere warns colonists about movement of British troops.

1800

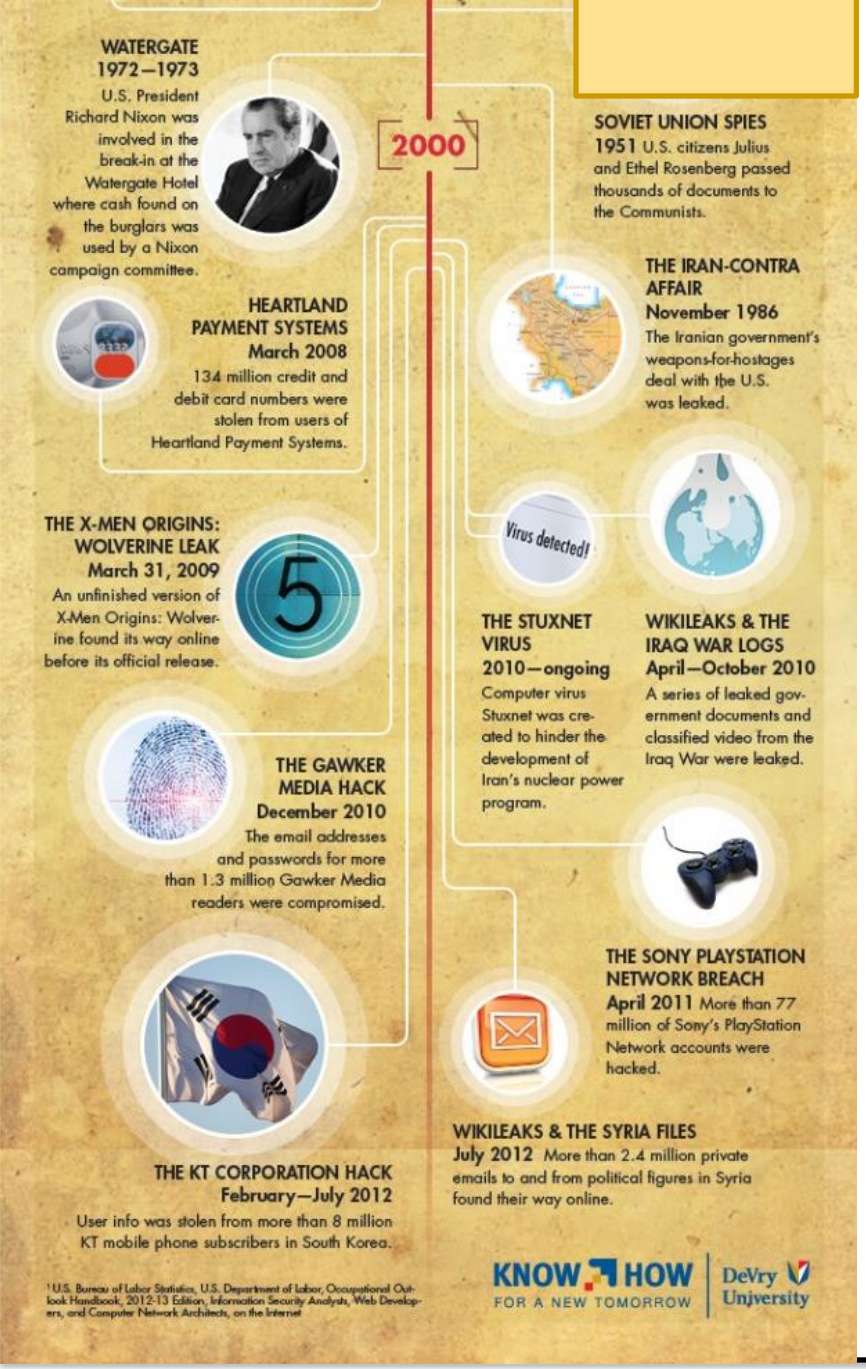
WEST POINT SECRETS
April—September 1780
Benedict Arnold attempts to sell secrets to the British about American troops and West Point.

THE ENIGMA MACHINE
December1932
Polish Cipher Bureau
The Polish government's cryptography agency decoded the cipher for Germany's early Enigma machines.

1900

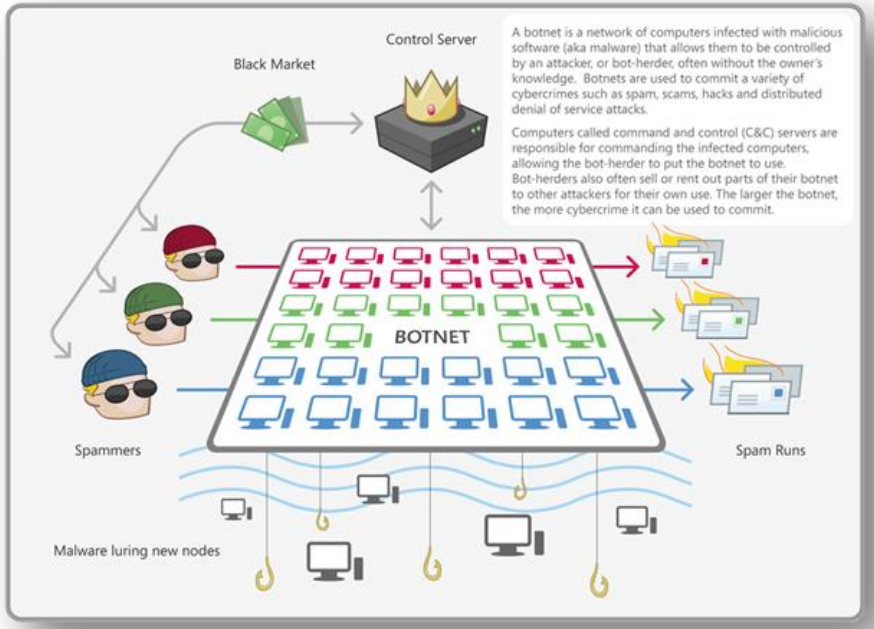
ILLINOIS INSTITUTE OF TECHNOLOGY

Some Previous Bad Security Breaches



ILLINOIS INSTITUTE OF TECHNOLOGY

Spectacular Data Breaches: 2013 - 2014



August 2014 – Russian Hacker Bot
(1.2 Billion User Credentials)

Spring 2013 - Edward Snowden

December 2013 – Target

April 2014 – Heart Bleed, OpenSSL

April 2014 – eBay

May 2014 – P. F. Chang's

Gregg Steinhafel
Former Target CEO

Attackers took advantage of weak security at a Target vendor, gaining a foothold in Target's inner network.

Attackers took advantage of weak controls within Target's network and successfully maneuvered into the network's most sensitive areas.

Recon | Weaponize | Deliver | Exploit | Install | Command & Control | Action

Target missed warnings from its anti-intrusion software that attackers were installing malware in its network.

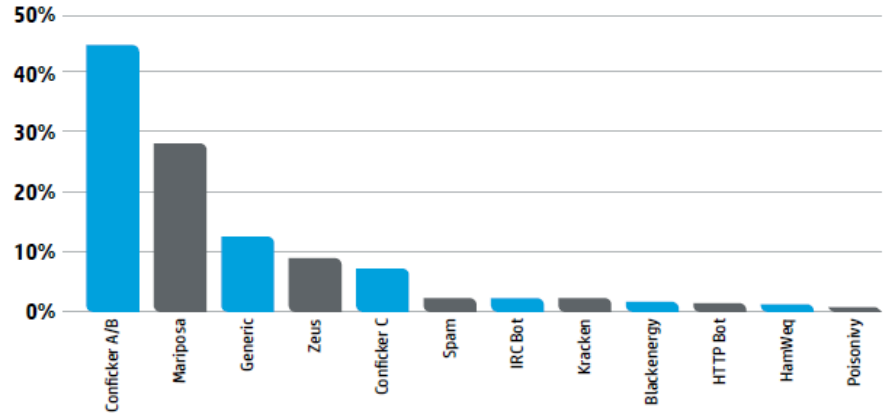
Target missed information provided by its anti-intrusion software about the attackers' escape plan, allowing attackers to steal as many as 110 million customer records.

Source: http://docs.ismgcorp.com/files/external/Target_Kill_Chain_Analysis_FINAL.pdf

ILLINOIS INSTITUTE OF TECHNOLOGY

Russian Hacker BotNet Data Breach

- **August 2014 –** Russians used a BotNet harvest over 1.2 Billion credentials
- (Change your passwords)



Number of drones in several well-known botnets; HP 2010 Full Year Cyber Security Risks Report, April 2011.

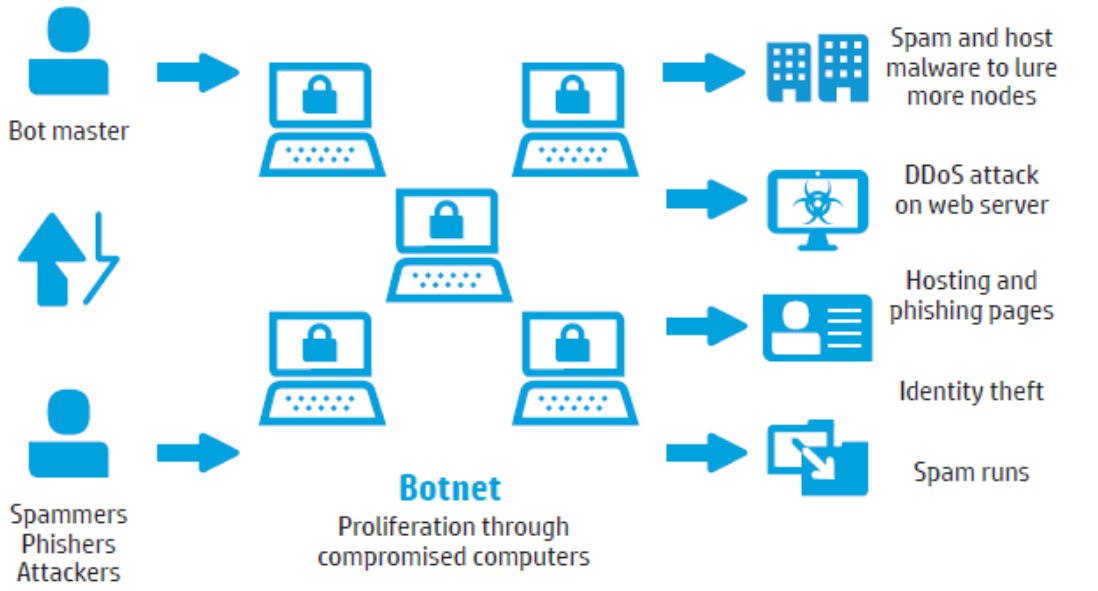


Diagram Source: HP White Paper on Botnets, 4AA3-9451ENW, November 2012

Persons in the Snowden Data Breach Story

Laura Poitras,
Reporter

Barack Obama,
President of the United States

Edward J. Snowden,
Former NSA Contractor

Glen Greenwald,
Reporter for the U.K. Guardian

Vladimir Putin,
President of Russia

General Keith Alexander,
Former NSA Director and Director of US Cyber Command

What Happened? What Did Snowden Do?

- In May 2013, after a series of secret communications with two experienced reporters (Laura Poitras and Glenn Greenwald), NSA Contractor and System Administrator Edward Snowden took four laptops, each with a 1 TB drive and flew to Hong Kong and later flew to Russia (supposedly en route to Cuba or South America)

- Approximately 1.7 million classified documents were copied and removed from the NSA's infrastructure while Snowden was on duty in Hawaii

- The damage to the National Security of the United States is said to be "incalculable" and the **WORST U.S. DATA BREACH EVER**.

Edward Snowden

ILLINOIS INSTITUTE OF TECHNOLOGY

The Time Line

- **June 21, 1983** – Edward J. Snowden born in Elizabeth City, North Carolina
- **1999 –** Dropped out of High School
- **2004** – Joined the U.S. Army Reserve because he was patriotic, later washed out
- **2005 -** worked s a "security specialist" at the University of Maryland's Center for Advanced Study of Language
- **2006 - 2007** - Joined the CIA and worked as a system administrator in Geneva, Switzerland
- **2009 -** Became a contractor and worked at Dell for the NSA in Japan
- **2012 -** Was identified as having downloaded several sensitive documents from the NSA
- **January 2013** – Snowden initiates communications with a New York Times Reporter, Laura Poitras, setting the protocol for strong public key / private key encryption due to fears of being discovered
- **March 2013 –** Snowden joined Booz Allen Hamilton as a systems administrator working for the NSA; moved to Hawaii
- **May 2013 –** Snowden traveled from Hawaii to Hong Kong with Four Laptops; Meets Glenn Greenwald and Laura Poitras in Hong Kong
- **June 3 – 5, 2013** – Glen Greenwald published a series of articles in the U.K.'s Guardian newspaper disclosing the extent of the NSA's surveillance programs, both foreign and domestic spying
- **June 21, 2013** – At the request of President Barack Obama, the U.S. Department of Justice files (sealed) criminal espionage charges against Snowden and demands extradition

ILLINOIS INSTITUTE OF TECHNOLOGY

The Time Line

- **August 1, 2013** – Snowden granted temporary political asylum in Russia by President Vladimir Putin after spending more than four weeks at the Moscow International Airport
- **March 7, 2014** - Testimony at EU Parliament via teleconference, e-mail, Twitter, and the Internet
- **March 10, 2014** – SXSW Conference via ACLU sponsored teleconference, Twitter, and the Internet
- **March 18, 2014 –** the ACLU published all NSA documents that Snowden had disclosed so far, in an online database that is searchable by topic, title and date. The URL: https://www.aclu.org/nsa-documents-search
- **March 18, 2014** – TED Conference Talk via Telepresence Robot, software and the Internet
- **April 6, 2014** – ACLU Conference via teleconference, e-mail, Twitter, and the Internet
- **April 8, 2014** – Edward Snowden Interview in Vanity Fair magazine
- **April 8, 2014** – Edward Snowden Interview in Vanity Fair magazine
- **May 28, 2014** – Snowden appears on an NBC News Interview with Brian Williams
- **July 19, 2014 – Article by Rusbridger and MacAskill:** I, spy: Edward Snowden in exile Revealed that Oliver Stone will make a Snowden Movie
- **August 7, 2014** - Snowden gets a 3-year extension on his stay in Russia
- **August 13, 2014** – Wired Magazine Weekly Article: Edward Snowden: The Most Wanted in the World

ILLINOIS INSTITUTE OF TECHNOLOGY

How Did Snowden Accomplish His Data Breach?

- **Violated Trust and Confidence placed in him by the NSA**
- **Social Engineering**
  - Achieved Elevated Privileges and Access by getting colleagues to share their login credentials
  - Defeating security controls that were designed to compartmentalize data and data access based on a need to know
- **Intimate knowledge of systems, security management, and weaknesses in controls**
- **Copied data to four Laptops** – 1 TB each
- **Communicated with Reporters** starting in January 2013 via encrypted e-mails
- **Left Hawaii to Hong Kong gave reporters key details**
- **Left Hong Kong for Russia**
- **Communicating now via the Internet** (e-mail, secure webcast, Twitter, Telepresence Robot control, phone, etc.)

Snowden at Press Conference in Moscow with Russian Lawyers July 2013

ILLINOIS INSTITUTE OF TECHNOLOGY

What Has Snowden Disclosed?

- **Details about**
  - MANY NSA Classified Programs
  - MANY GCHQ Classified Joint Programs
  - Spying on Americans
  - Spying on Allies
  - Spying on our “Enemies”
  - Social Engineering and Discrediting Campaign Tactics
  - NSA working Microsoft, Google, Yahoo. Etc.
  - Offensive and Defensive Cyberwarfare activities and actors
  - Workings of the NSA and his job responsibilities
  - His philosophies and believes about the Government, surveillance, the Internet, and personal freedoms
- **Promises to disclose a great deal more**

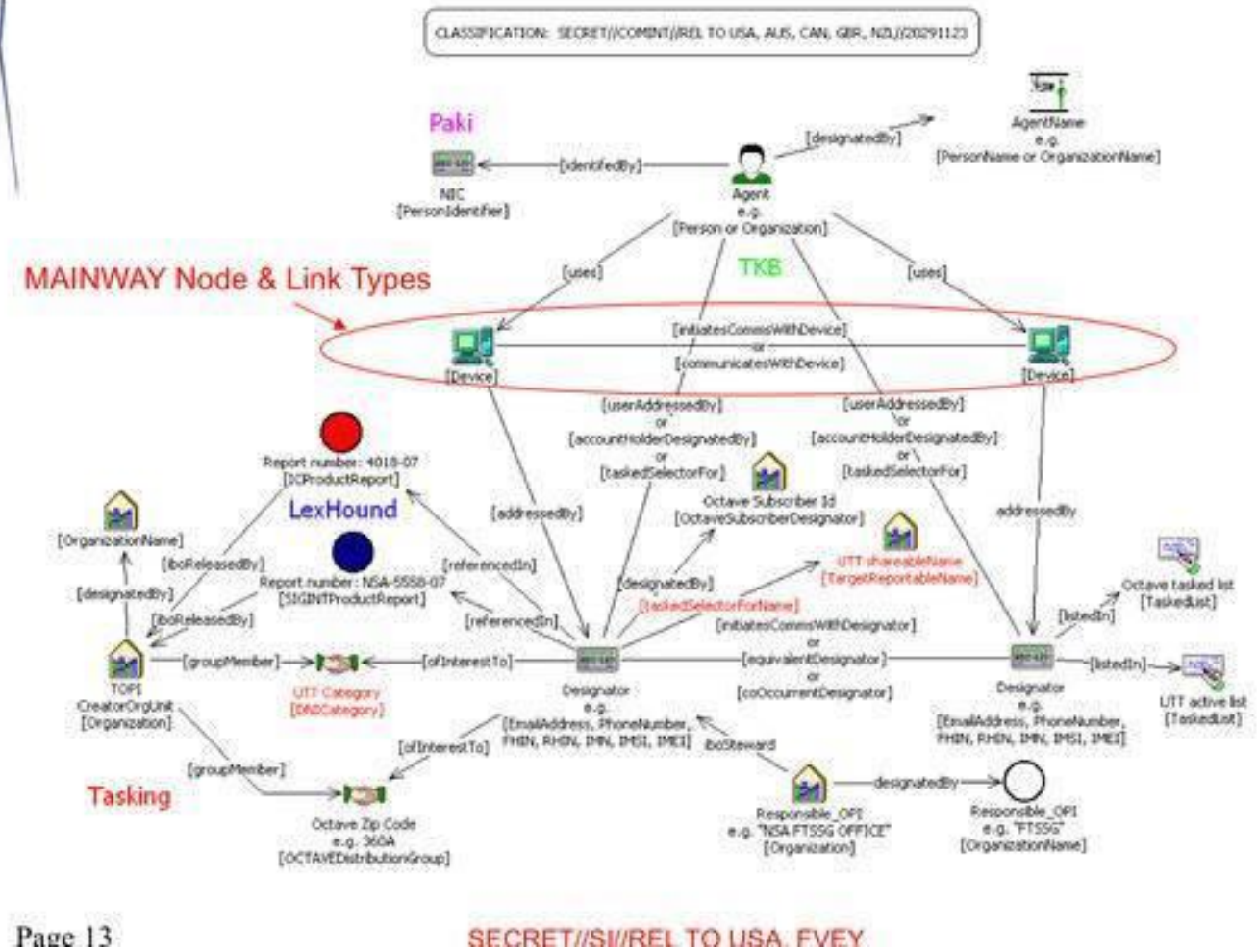
Edward Snowden

ILLINOIS INSTITUTE OF TECHNOLOGY

NSA Surveillance Programs – Now Known

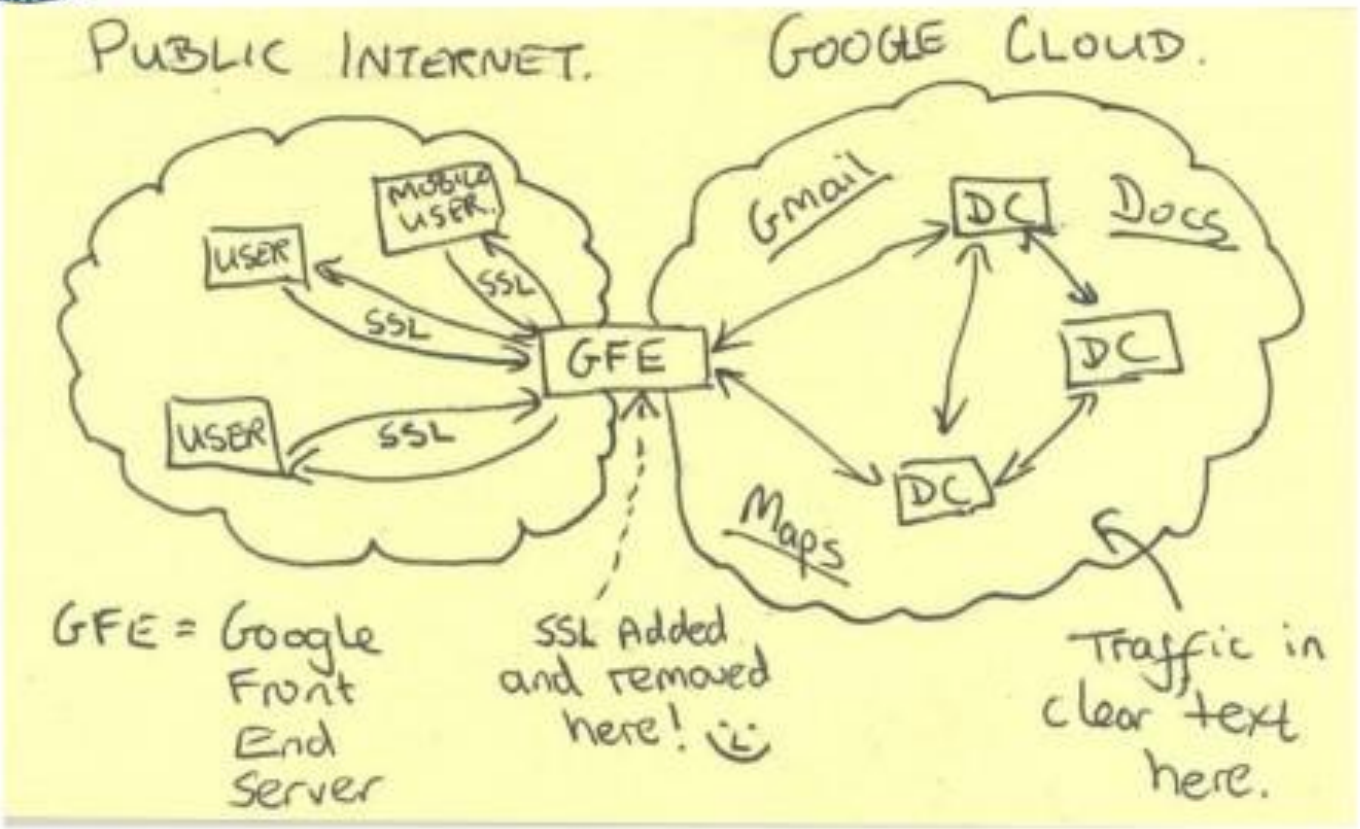
ILLINOIS INSTITUTE OF TECHNOLOGY

(S//SI//REL USA, FVEY) SYANPSE Data Model



Slide from Snowden Data Breach, Disclosed by Glen Greenwald.

Current Efforts - Google



TOP SECRET//SI//NOFORN

Slide from Snowden Data Breach, Disclosed by Glen Greenwald.

Slide from Snowden Data Breach, Disclosed by Glen Greenwald.

PRISM

TOP SECRET || SI || ORCON || NOFORN

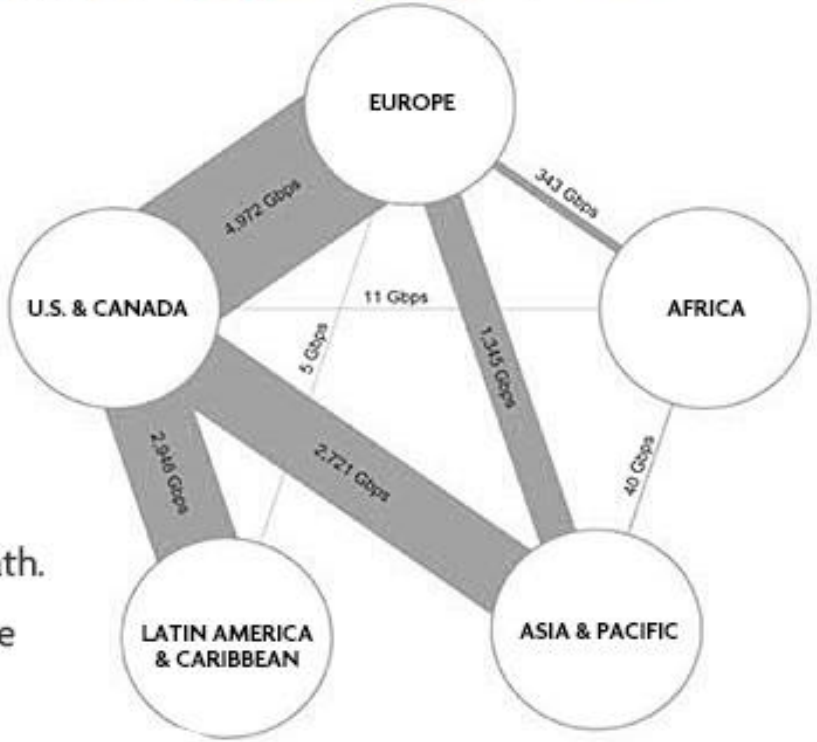
Gmail facebook Hotmail YAHOO! Google skype paltalk.com YouTube AOL mail

TS | SI | NF

INTRODUCTION

US as World Telecommunications Backbone

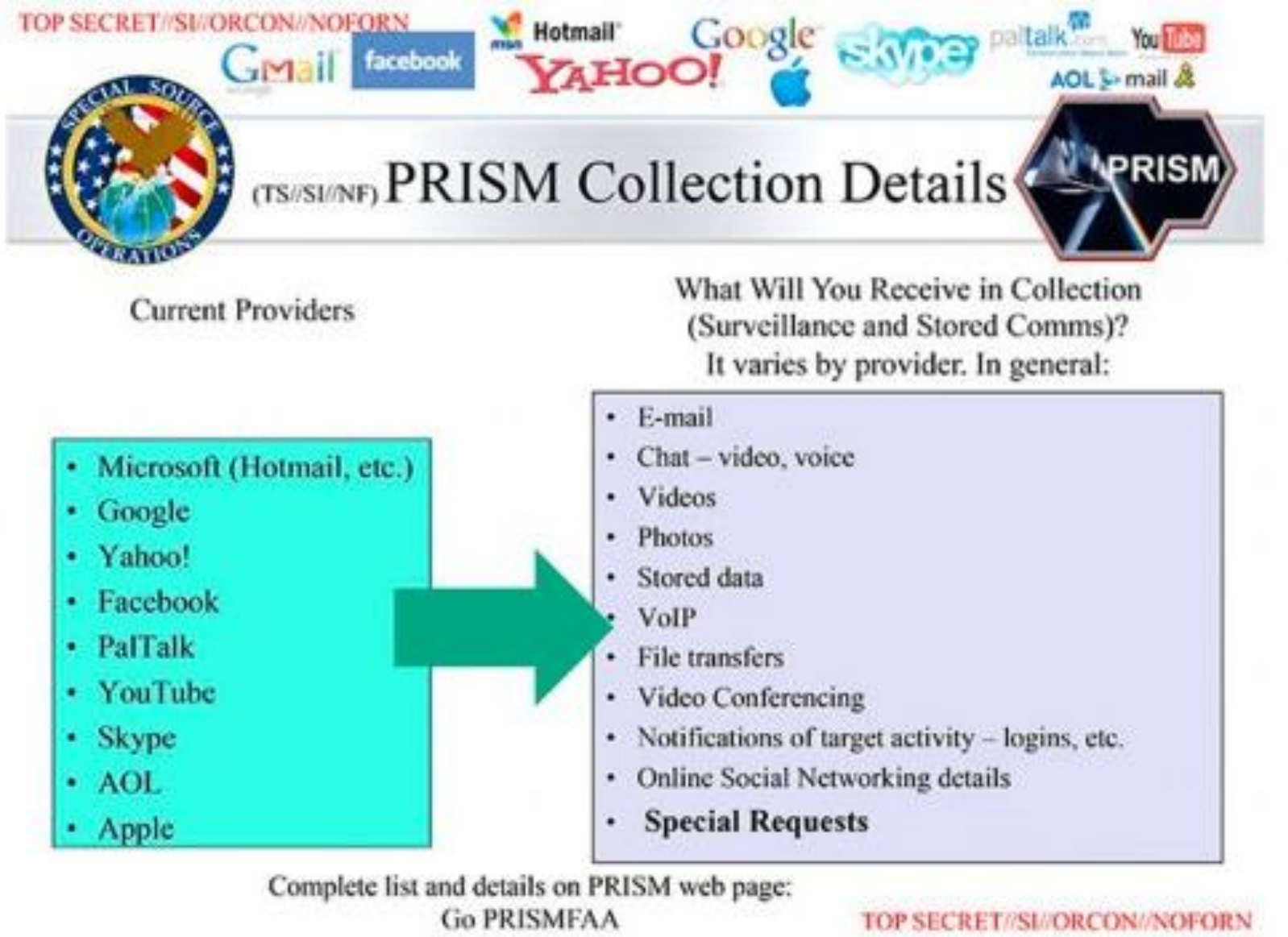
- Much of the world's communications flow through the US.
- A target's email, phone call or chat will take **the cheapest path, not the physically most direct path**—you can't always predict the path.
- Your target's communications could easily be flowing into and through the US.



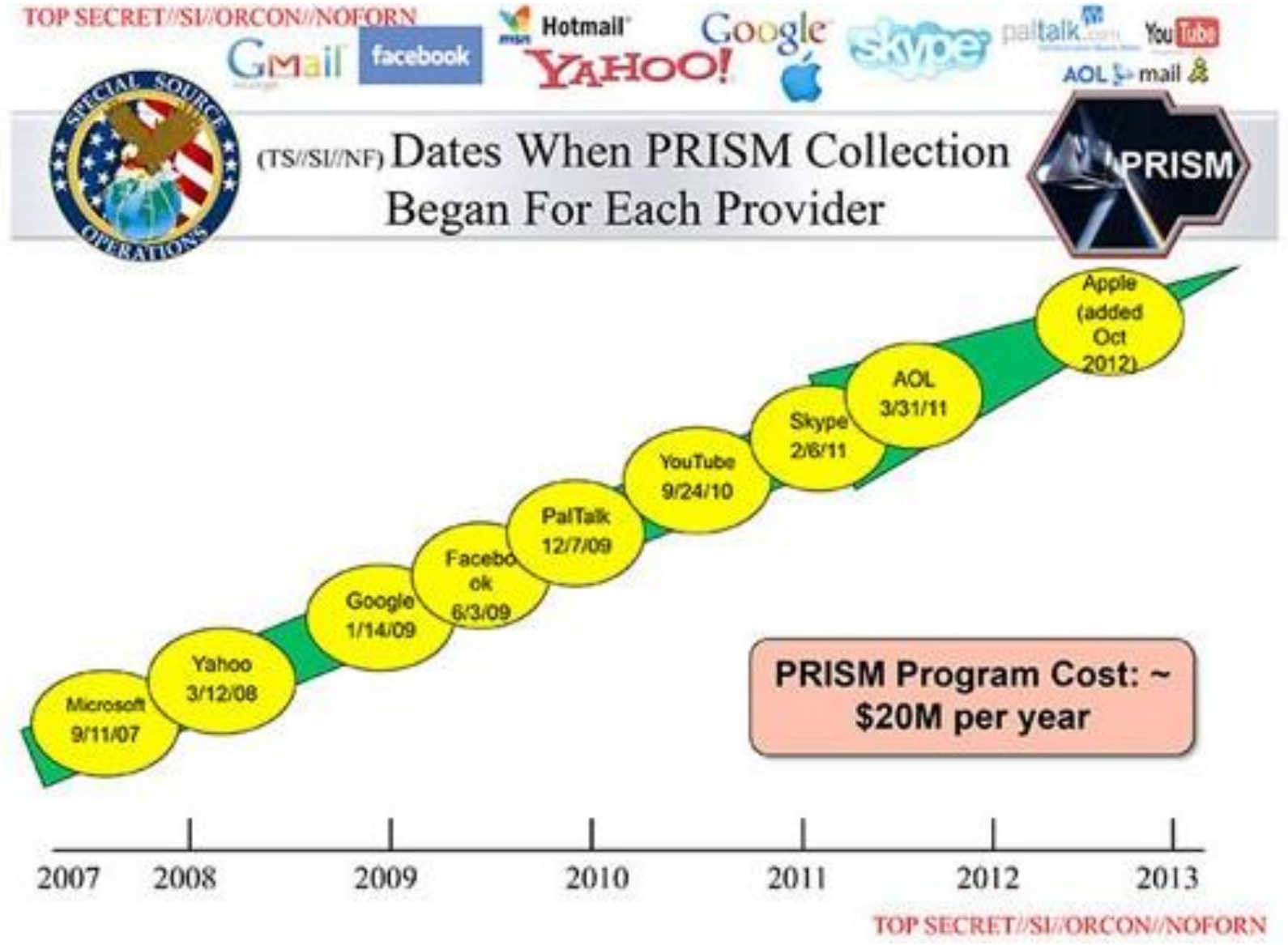
International Internet Regional Bandwith Capacity in 2011
Source: Telegeography Research

TOP SECRET || SI || ORCON || NOFORN PRISM

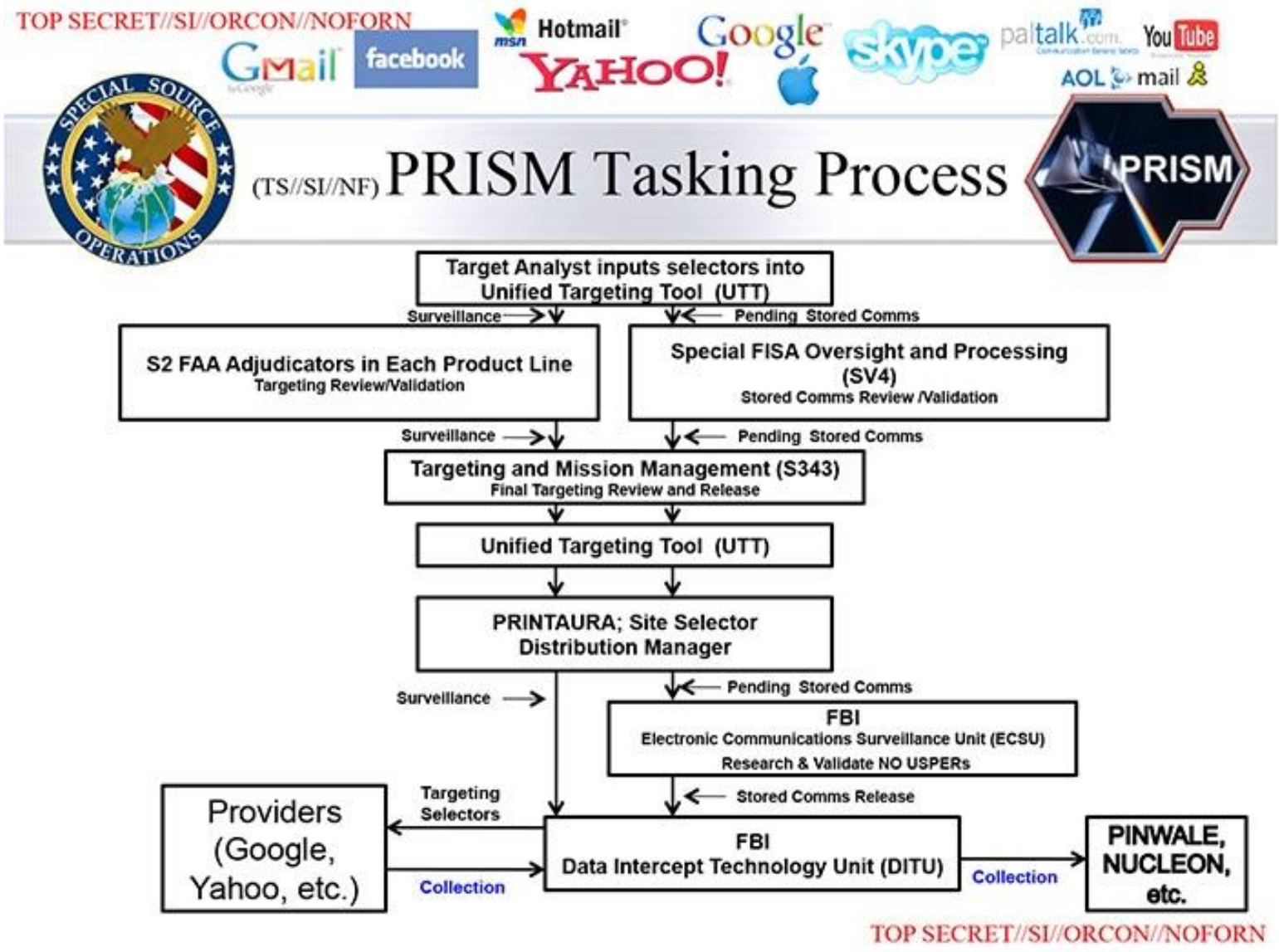
Slide from Snowden Data Breach, Disclosed by Glen Greenwald.



Slide from Snowden Data Breach, Disclosed by Glen Greenwald.



Slide from Snowden Data Breach, Disclosed by Glen Greenwald.



Slide from Snowden Data Breach, Disclosed by Glen Greenwald.

Slide from Snowden Data Breach, Disclosed by Glen Greenwald.

Slide from Snowden Data Breach, Disclosed by Glen Greenwald.

SECRET//SI//REL TO USA, FVEY

Gambits for Deception

Attention	Control attention Conspicuity & Expectancies	The big move covers the little move	The Target looks where you look	Attention drops at the perceived end	Repetition reduces vigilance
Perception	Mask/Mimic Eliminate - Blend Recreate - Imitate	Repackage/Invent Modify old cues Create new cues	Dazzle/Decoy Blur old cues Create alternate cues	Make the cue dynamic	Stimulate multiple sensors
Sensemaking	Exploit prior beliefs	Present story fragments	Repetition creates expectancies	Haversack Ruse (The Piece of Bad Luck)	Swap the real for the false, & vice versa
Affect	Create Cognitive Stress	Create Physiological Stress	Create Affective Stress (+/-)	Cialdini+2	Exploit shared affect
Behaviour	Simulate the action	Simulate the outcome	Time-shift perceived behaviour	Divorce behaviour from outcome	Channel behaviour

SECRET//SI//REL TO USA, FVEY

Slide from Snowden Data Breach, Disclosed by Glen Greenwald.

Consequences: How does this affect the NSA and U.S. National Security?

- "We have to assume that the Russians know EVERYTHING about our Surveillance Programs…"
  - One U.S. Government Official

- The U.S. will have to go back to the drawing board to create and implement most of the programs that provided the capabilities they want and need

- The NSA and other Intelligence gathering agencies must now rethink their human security programs

- Fewer people will have access to highly classified data

ILLINOIS INSTITUTE OF TECHNOLOGY

Consequences: How will this Edward Snowden Compromise Affect the U.S. Government?

- Better Risk Assessment and Risk Management Programs
- Better security management
- More money will be spent creating new surveillance programs and data protection programs
- Fewer people will have access to highly classified data
- Those with access to data will be watched more carefully
- Quicker and Harsher punishment for infractions

ILLINOIS INSTITUTE OF TECHNOLOGY

(Sealed) Charges Filed Against Edward Snowden

- **June 21, 2013** – the U.S. filed Criminal Charges Against Former NSA Contractor, Edward Snowden

- If convicted, Snowden could get the death penalty

Edward Snowden
Former NSA Contractor

ILLINOIS INSTITUTE OF TECHNOLOGY

AO 91 (Rev. 08/09) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

Eastern District of Virginia

JUN 14

United States of America
v.
Edward J. Snowden

Case No. 1:13 CR 265 (CMH)

Defendant(s)

UNDER SEAL

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of May 2013 in the county of Not Applicable in the District of Not Applicable, the defendant(s) violated:

Code Section	*Offense Description*
18 U.S.C. 641	Theft of Government Property
18 U.S.C. 793(d)	Unauthorized Communication of National Defense Information
18 U.S.C. 798(a)(3)	Willful Communication of Classified Communications Intelligence Information to an Unauthorized Person

This criminal complaint is based on these facts:

See Attached Affidavit.

Venue is proper pursuant to 18 U.S.C. 3238.

☑ Continued on the attached sheet.

Reviewed by AUSA/SAUSA:

[redacted]

Complainant's signature

John A. Kralik, Jr.
Special Agent, Federal Bureau of Investigation
Printed name and title

Sworn to before me and signed in my presence.

Date: 06/14/2013

/s/ JTC
John F. Anderson
United States Magistrate Judge
Judge's signature

City and state: Alexandria, VA

Hon. John F. Anderson, U.S. Magistrate Judge
Printed name and title

Consequences: Has anyone lost their job as a result of what Edward Snowden has done?

- General Keith Alexander, chief of the NSA, Central Security Service, and U.S. Cyber Command AND his Deputy John Inglis
  - On October 16, 2013, it was announced that General Alexander, and his Deputy John C. Inglis, were leaving the NSA. This announcement came on the heels of four months of NSA spying revelations spawned by press-leaks made by former NSA contractor Edward Snowden.
- Most likely some of Snowden's bosses and colleagues at the NSA and Booz Allen Hamilton were quietly fired

General Keith Alexander

ILLINOIS INSTITUTE OF TECHNOLOGY

Implications: How will the Edward Snowden Compromise Affect the Cybersecurity Career Field?

- **More qualifications and experience**
- **More frequent training**
- **More certifications**
- **More stringent controls**
  - More surveillance
  - Background checks
  - Better control of access to data
  - Two-man policies

M.S. Cybersecurity
01 - CIS 608 Information Security Management
02 - CYBR 515 - Security Architecture and Design
03 - CYBR 510 Physical, Operations, and Personnel Security
04 - CIS 537 Introduction to Cyber Ethics
05 - CIS 607 Computer Forensics
06 - CYBR 520 Human Aspects of Cybersecurity
07 - CYBR 610 Risk Management Studies
08 - CYBR 525 Ethical Hacking and Response
09 - DET 630 Cyber Warfare & Deterrence
10 - CYBR 625 Business Continuity Planning and Recovery
11 - CYBR 615 Cybersecurity Governance and Compliance
12 - CYBR 650 Current Trends in Cybersecurity

CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL
CISSP®

SYSTEMS SECURITY CERTIFIED PRACTITIONER
SSCP®

CPP® Certified Protection Professional
BOARD CERTIFIED IN SECURITY MANAGEMENT

CompTIA Security+

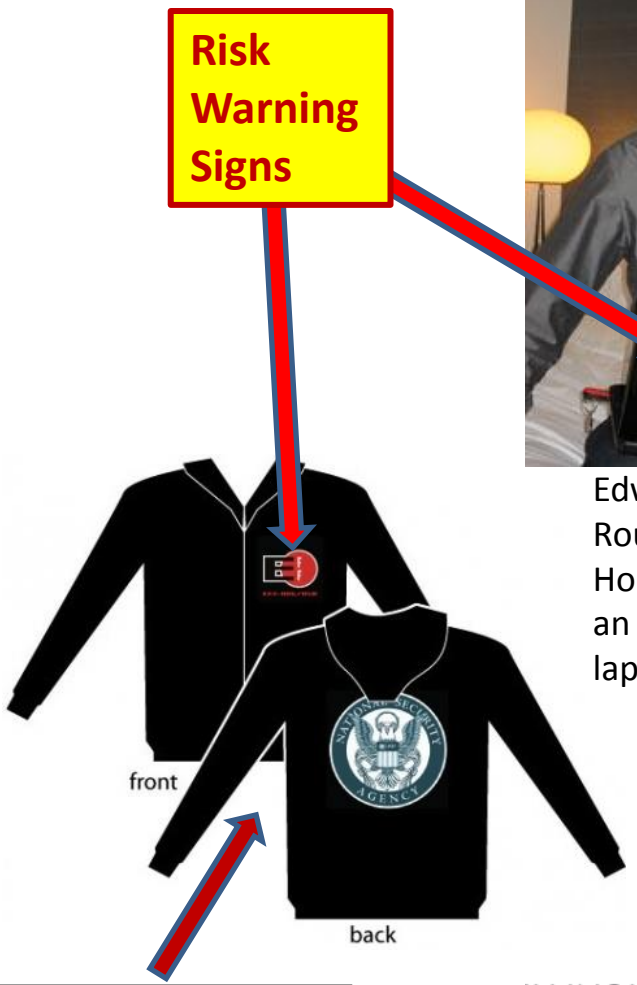
Implications: How will the Edward Snowden Compromise Affect Your Career as an IT Professional and/or a Security Professional?

- **The qualifications bar will be much higher**
  - No more high school drop-outs or GEDs
  - More certifications, cybersecurity-related degrees
- **Stronger examination of backgrounds**
- **Expect more oversight**

ILLINOIS INSTITUTE OF TECHNOLOGY

Implications: How would you prevent an Edward Snowden-style Data Breach in your organization if your were the Cybersecurity Director?

- **Revamp your Risk Assessment and Risk Management Programs**
- **Revamp your Security Management Program**
  - Applying the Control Framework(s) controls that relate to Security Personnel and Asset Management
  - Training on Security, ethics, etc.
  - Increased surveillance, controls and accountability
  - Fewer people should have access to highly classified data
  - Two-man policies
- **Apply and use metrics**
- **Monitor! Monitor! Monitor!**
- **Continuously improve**
- **Train! Train! Train! (NIST SP 800-50 & NIST SP 800-16)**



Edward Snowden Routinely wore an EFF Hoodie and had an EFF Sticker on his laptop

Source: http://www.dailydot.com/news/snowden-eff-hoodie/

ILLINOIS INSTITUTE OF TECHNOLOGY

THE LATEST DEVELOPMENTS ON EDWARD SNOWDEN

ILLINOIS INSTITUTE OF TECHNOLOGY

Snowden's Advice from Exile

- The NSA whistleblower, Edward Snowden, has urged lawyers, journalists,doctors, accountants, priests and others with a duty to protect confidentiality to upgrade security in the wake of the spy surveillance revelations.
- Snowden said professionals were failing in their obligations to their clients, sources, patients and parishioners in what he described as a new and challenging world.
- "What last year's revelations showed us was irrefutable evidence that unencrypted communications on the internet are no longer safe. Any communications should be encrypted by default," he said.

Edward Snowden
Former NSA Contractor

Rusbridger, A. and MacAskill, E. (2014). The Guardian Exclusive: Whistleblower says NSA revelations mean those with duty to protect confidentiality must urgently upgrade security. Retrieved from http://www.theguardian.com/world/2014/jul/17/edward-snowden-professionals-encrypt-client-communications-nsa-spy on July 20, 2014.

ILLINOIS INSTITUTE OF TECHNOLOGY

Edward Snowden's Revelations at the ACLU Conference

1. Has promised to release MANY more revealing documents
2. Has set up a "Doomsday" release arrangements of all documents in case he is assassinated

Edward Snowden

ILLINOIS INSTITUTE OF TECHNOLOGY

Edward Snowden's 6 Revelations at the SXSW Conference

1. **Bulk Data Collection Doesn't Work**
2. **There Isn't Much Consumers Can Do to Avoid It**
3. **The Most Dangerous Men in America Are Michael Hayden and Keith Alexander**
4. **The Government Still Doesn't Know What Snowden Has**
5. **The Tech Industry Is Upset**
6. **Snowden Has No Regrets**

"The NSA is setting fire to the Internet. You people in the room at SXSW are the firefighters." – Edward Snowden

Edward Snowden
Live via Secure Webcast
at the SXSW Conference
March 11, 2014

6 Things Edward Snowden Revealed at SXSW
http://www.pcmag.com/article2/0,2817,2454827,00.asp

ILLINOIS INSTITUTE OF TECHNOLOGY

Edward Snowden's 7 Revelations During the May 2014 NBC News Interview

1. Says the U.S. "stranded" him is Russia by revoking his U.S. Passport
2. Says he was trained as a "Spy"
3. Feels justified as a "whistleblower" and that it was his duty to report the "illegal surveillance of Americans".
4. Says he cannot possibly receive a "fair trial" because what he has done would have to be tried in a secret court under the Espionage Act
5. **Is Outraged at the Russian Government requiring registration of bloggers**
6. Snowden Has No Regrets
7. Says he misses the U.S. and wishes he could return

Edward Snowden:
NBC News Interview
With Brian Williams on
May 28, 2014

Inside the Mind of Edward Snowden: NBC News Interview in Russia with Brian Williams
http://www.nbcnews.com/feature/edward-snowden-interview/exclusive-edward-snowden-tells-brian-williams-u-s-stranded-him-n116096

The EU Parliament in a show of Solidarity for Edward Snowden and his disclosures votes in support of anti-spying measures

ILLINOIS INSTITUTE OF TECHNOLOGY

I, spy: Edward Snowden in exile

He doesn't drink, he's reading Dostoevsky and, no, he doesn't wear a disguise. A year after blowing the whistle on the NSA, America's most wanted talks frankly about his life as a hero-pariah – and why the world remains 'more dangerous than Orwell imagined'.

- Read a transcript of the interview

Rusbridger, A. and MacAskill, E. (2014). I, spy: Edward Snowden in exile. http://www.theguardian.com/world/2014/jul/18/-sp-edward-snowden-interview-rusbridger-macaskill on July 19, 2014.

Photograph: Alan Rusbridger for the Guardian

Edward Snowden Granted a Three-Year Extension in Russia

- **August 7, 2014** - Snowden's lawyer, Analtoly Kucherena, was quoted by Russian news agencies as saying Snowden now has been granted residency for three more years, **but that he had not been granted political asylum.**

Edward Snowden

Russians on the street occasionally recognize him. "Shh," Snowden tells them, smiling, putting a finger to his lips.

Source: Edward Snowden Gets Permission To Stay In Russia For 3 More Years: Lawyer, Jim Heintz
http://www.huffingtonpost.com/2014/08/07/edward-snowden-russia_n_5657481.html

Edward Snowden on the Cover of Wired Magazine (Weekly) – August 13, 2014

- August 13, 2014 – Wired Magazine online article: Snowden: The Untold Story: The Most Wanted Man in the World

Bamford, J. (2014). Edward Snowden: The Most Wanted Man in the World. Retrieved from http://www.wired.com/2014/08/edward-snowden/.

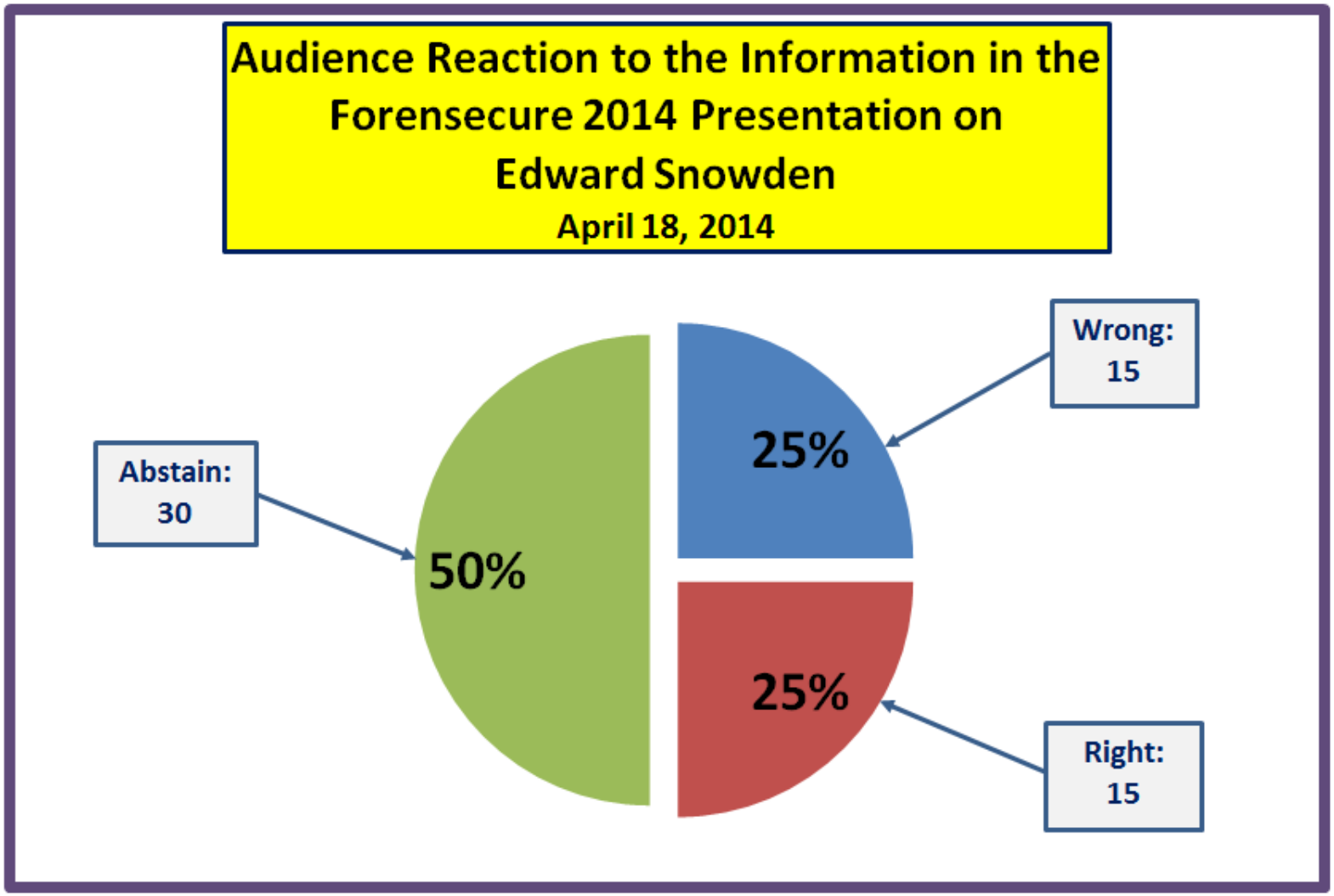
Opinion: Do You Think Edward Snowden Was Correct in Doing What He Did?

- Let's take a vote using a show of hands

Snowden was WRONG	Snowden was RIGHT

ILLINOIS INSTITUTE OF TECHNOLOGY

Poll Results: Do You Think Edward Snowden Was Correct in Doing What He Did?



ILLINOIS INSTITUTE OF TECHNOLOGY

Anecdotal Advice to Prevent an Edward Snowden Event in your Organization:

1. Vet your staff members carefully with background checks.
2. Monitor your members' work and behaviors
3. *Never* hire a high school drop-out.
4. Train your system administrators on a Code of Ethics: http://1drv.ms/QjMcjw
5. Train your entire staff about what Social Engineering is, how it works, and how to protect against it.
6. Read this paper about Hacking Humans: http://www.billslater.com/writing/Hacking_Humans_from_W_F_Slater_v1_2013_0219_.pdf

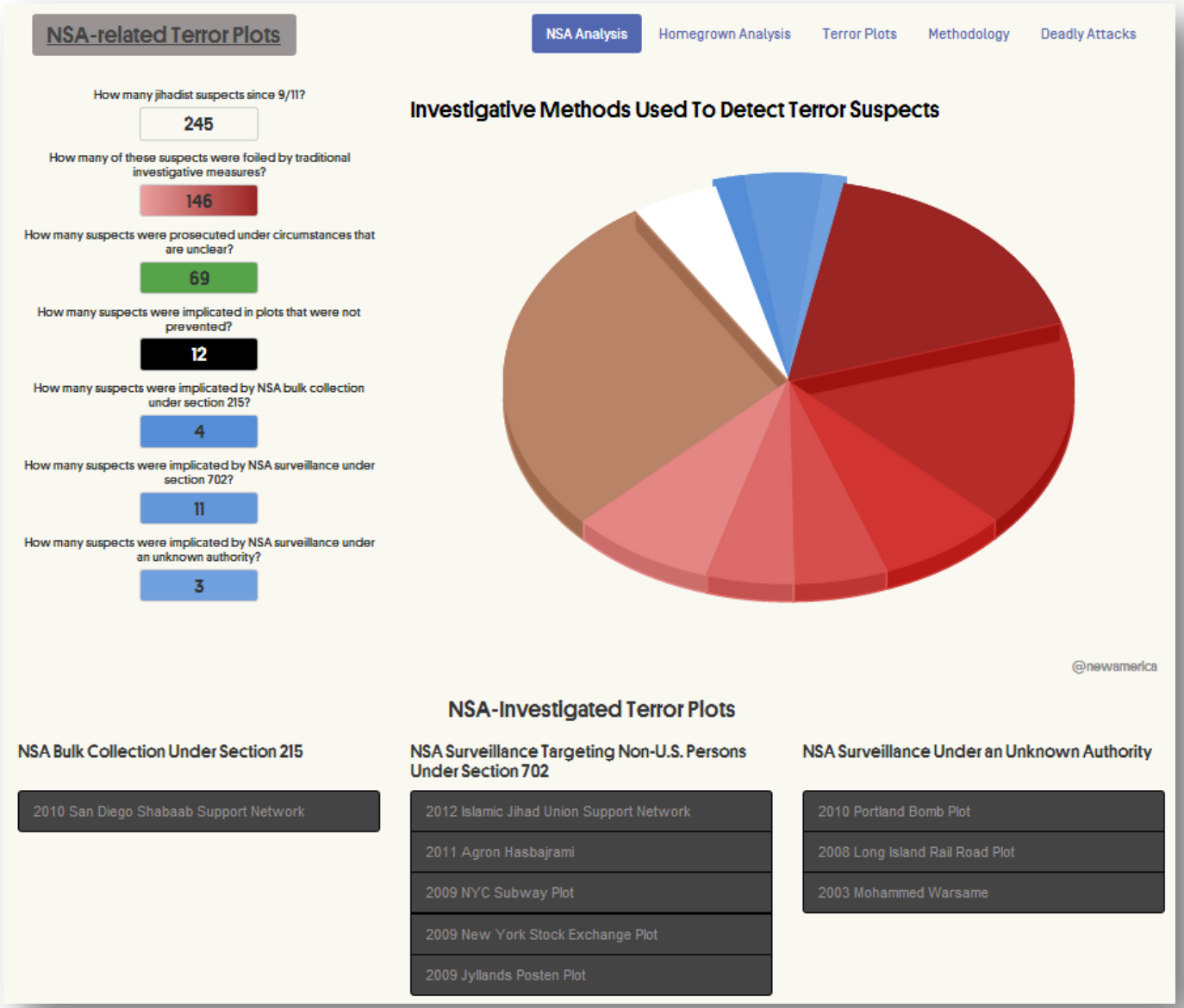
ILLINOIS INSTITUTE OF TECHNOLOGY

My Own Assessments

- Snowden has mental issues. Inferiority complex and a megalomaniac
- Snowden is a major TRAITOR, and he has hurt the U.S. Its security and dishonored himself and his profession
- Snowden is still in grave danger
- Snowden gravitates toward the limelight to remind the World that he is still alive
- If Snowden really wants to live, he would be better off if he would learn the Russian language, history, & culture, and ultimately apply for Russian Citizenship

ILLINOIS INSTITUTE OF TECHNOLOGY

NSA Bulk Data Surveillance Programs



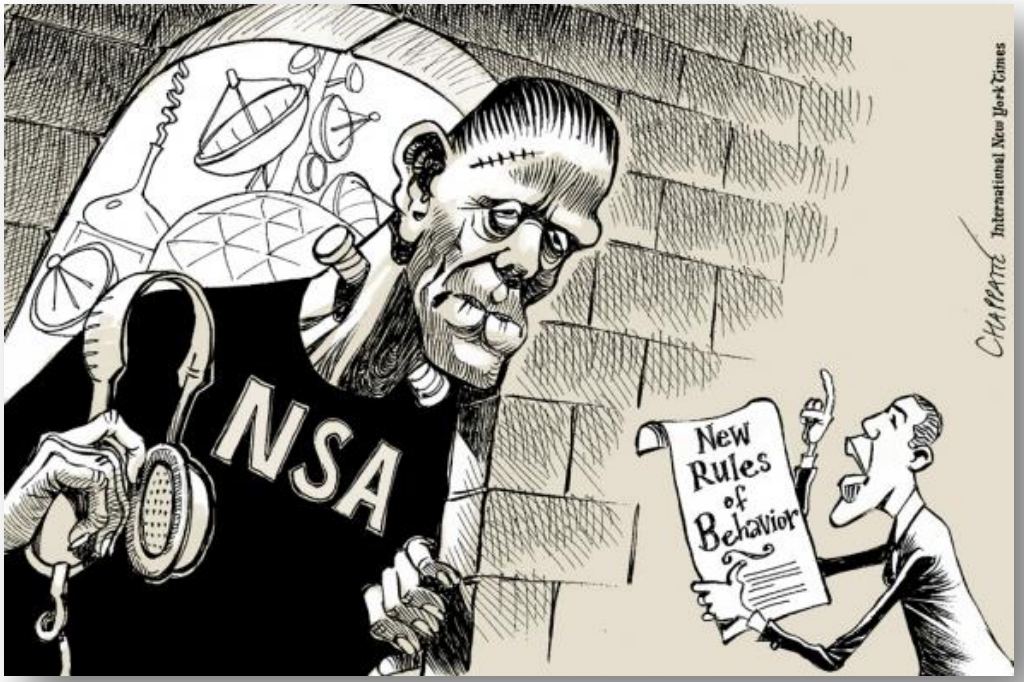
International Security. (2014). Do NSA's Bulk Surveillance Programs Stop Terrorism? Retrieved from http://securitydata.newamerica.net/nsa/analysis on August 7, 2014.

NSA Fallout

- US' National Security Agency, Struggling to Recruit Top Talent, Turns to Silicon Valley

- Snowden reveals that NSA personnel distributed nude pictures of American citizens

- NSA now hated and mistrusted in the U.S. and around the world



U.S. Embassy in Berlin, Germany

Conclusions

- ✓ **Despite billions of dollars of planning, engineering and administration, the human element proved to be the weakest link**
- ✓ **A lot of security REENGINEERING will need to take place**
- ✓ **A lot of money, time, and energy will be required to get it corrected**
- ✓ **Things will get more complicated for Management and Cybersecurity professionals**
- ✓ **Greater vetting efforts and compartmentalization of data**
- ✓ **Expect that highly-trained, high-skilled, trustworthy cybersecurity professionals and managers will be more valuable and in demand**

ILLINOIS INSTITUTE OF TECHNOLOGY

Parting Thoughts

- To understand the Genesis of U.S. Government Surveillance and the Power that has now accumulated in the **Executive Branch of the U.S. Federal Government**, please view this very brief **August 17, 1975** video with prescient comments about powerful and growing surveillance capabilities, **"Government Tyranny" and "the Abyss" by Senator Frank Church**, Chairman of the Senate Committee on Intelligence Activities on NBC's Meet the Press.

Senator Frank Church

- **My advice: Save this information.**

Source: NBC NEWS Meet the press Interview with Senator Frank Church Retrieved from https://www.youtube.com/watch?v=YAG1N4a84Dk

ILLINOIS INSTITUTE OF TECHNOLOGY

The End… of The Beginning

The Brand New 1 million square foot NSA Data Center in Bluffdale, Utah
This 100 MW Facility will hold 12 Exabytes of Data

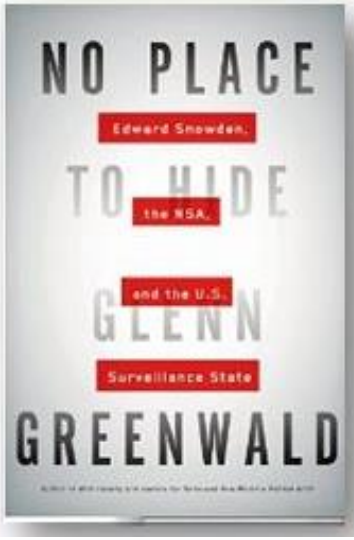
It houses EVERYONE's Data

Questions?

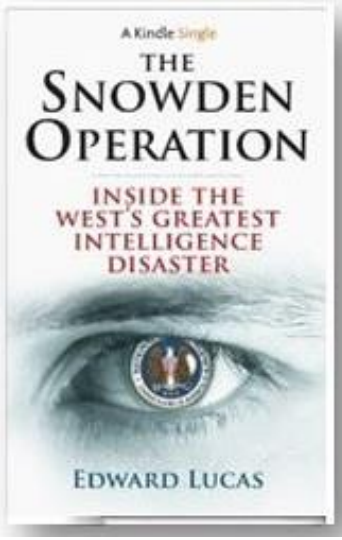
References

- New Books on Edward Snowden

No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State



The Snowden Operation: Inside the West's Greatest Intelligence Disaster



No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State

ILLINOIS INSTITUTE OF TECHNOLOGY

References

- ACLU. (2014). President Obama: Grant Edward Snowden Immunity Now. Retrieved from https://www.aclu.org/secure/grant_snowden_immunity on March 18, 2014.
- ANI. (2014). White House cyber security chief says damage done by Edward Snowden will take decades to repair. Retrieved from http://www.dnaindia.com/world/report-white-house-cyber-security-chief-says-damage-done-by-edward-snowden-will-take-decades-to-repair-1973325 on April 5, 2014,
- Anonymous, (2104). Edward Snowden, A Truth Unveiled (Documentary). Retrieved from http://www.youtube.com/watch?v=dSXlKdWF5HE on March 20, 2014.
- Associated Press. (2014). Everyone is under surveillance now, says whistleblower Edward Snowden. Retrieved from http://www.theguardian.com/world/2014/may/03/everyone-is-under-surveillance-now-says-whistleblower-edward-snowden on May 3, 2014.
- Bamford, J. (2014). Edward Snowden: The Most Wanted Man in the World. Retrieved from http://www.wired.com/2014/08/edward-snowden/ on August 13, 2014.
- Batley, M. (2014). Clapper: Snowden Took Advantage of 'Perfect Storm' of Security Lapses. Retrieved from http://www.newsmax.com/US/Edward-Snowden-James-Clapper-NSA-intelligence/2014/02/12/id/552327 on February 12, 2014.
- Boyle, D. (2014). Edward Snowden was in Moscow's sights six years before leaking U.S. secrets claims former KGB agent. Retrieved from http://www.dailymail.co.uk/news/article-2651973/Edward-Snowden-Moscows-sights-six-years-leaking-U-S-secrets-claims-former-KGB-agent.html on June 12, 2014.
- Campbell, B. (2014). The story of Edward Snowden is so unbelievable, sometimes you forget it's nonfiction Retrieved from http://www.pri.org/stories/2014-02-14/story-edward-snowden-so-unbelievable-sometimes-you-forget-its-nonfiction on February 15, 2014.

ILLINOIS INSTITUTE OF TECHNOLOGY

References

- Cohen, T. Military spy chief: Have to assume Russia knows U.S. secrets. Retrieved from http://www.cnn.com/2014/03/07/politics/snowden-leaks-russia/index.html on March 9, 2014.
- Coleman, G. (2014). The Latest Snowden Revelation Is Dangerous for Anonymous — And for All of Us. Retrieved from http://www.wired.com/opinion/2014/02/comes-around-goes-around-latest-snowden-revelation-isnt-just-dangerous-anonymous-us/ on February 4, 2014.
- Cook, J. (2014). Cryptome: Remaining Snowden docs will be released to avert 'unspecified US war' in July 2014. retrieved from http://benswann.com/cryptome-remaining-snowden-docs-will-be-released-to-avert-unspecified-us-war-in-july/ on July 3, 2014.
- Decrypted Matrix. (2014). An NSA Coworker Remembers The Real Edward Snowden: 'A Genius Among Geniuses'. Retrieved from https://decryptedmatrix.com/live/an-nsa-coworker-remembers-the-real-edward-snowden-a-genius-among-geniuses/ on March 31, 2014.
- Farrell, H. (2014). The political science of cybersecurity IV: How Edward Snowden helps U.S. deterrence. Retrieved from http://www.washingtonpost.com/blogs/monkey-cage/wp/2014/03/12/the-political-science-of-cybersecurity-iv-how-edward-snowden-helps-u-s-deterrence/ on March 12, 2014.
- Forrest, H. (2014). Monday, March 10: Edward Snowden to Speak at SXSW Interactive Via Videoconference. Retrieved from http://sxsw.com/interactive/news/2014/monday-march-10-edward-snowden-speak-sxsw-interactive-videoconference on March 10, 2014.
- Free Man's Perspective. (2014). YES, YOU ARE BEING MANIPULATED BY YOUR GOVERNMENT. Retrieved from http://www.freemansperspective.com/governments-manipulate/ on March 20, 2014.
- Friedersdorf, C. (2014). The Latest Snowden Leak Is Devastating to NSA Defenders. Retrieved from http://www.theatlantic.com/politics/archive/2014/07/a-devastating-leak-for-edward-snowdens-critics/373991/ on July 7, 2014.

ILLINOIS INSTITUTE OF TECHNOLOGY

References

- Gallagher, R. and Greenwald, G. (2104). How the NSA Plans to Infect 'Millions' of Computers with Malware. Retrieved from https://firstlook.org/theintercept/article/2014/03/12/nsa-plans-infect-millions-computers-malware/ on March 12, 2014.
- Greenwald, G. (2014). No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State Metropolitan Books.
- Gross, G. (2014). House approves effort to limit NSA searches of US data. Retrieved from
- http://www.itworld.com/internet/423824/house-approves-effort-limit-nsa-searches-us-data on June 19, 2014.
- Gurnow, M. (2014). The Edward Snowden Affair: Exposing the Politics and Media Behind the NSA Scandal. Blue River Press, Inc.
- Harding, L. (2014). The Snowden Files: The Inside Story of the World's Most Wanted Man. Random House, LLC.
- Heintz, J. (2014). Edward Snowden Gets Permission To Stay In Russia For 3 More Years: Lawyer. Retrieved from http://www.huffingtonpost.com/2014/08/07/edward-snowden-russia_n_5657481.html on August 7, 2014.
- Huffington Post. (2014). Bill Gates: Edward Snowden Is No Hero. Retrieved from http://live.huffingtonpost.com/r/archive/segment/bill-gates-edward-snowden-is-no-hero/5323697e78c90a1ede00033b on March 16, 2014.
- International Security. (2014). Do NSA's Bulk Surveillance Programs Stop Terrorism? Retrieved from http://securitydata.newamerica.net/nsa/analysis on August 7, 2014.
- Kelly, M. B. (2014). A Former Obama Cabinet Official Made The Strongest Snowden Allegation Yet. Retrieved from http://www.businessinsider.com/former-obama-official-snowden-is-a-spy-2014-5 on May 5, 2014.

ILLINOIS INSTITUTE OF TECHNOLOGY

References

- Leopold, J. (2014). EXCLUSIVE: EMAILS REVEAL CLOSE GOOGLE RELATIONSHIP WITH NSA. Retrieved from http://america.aljazeera.com/articles/2014/5/6/nsa-chief-google.html on May 6, 2014.
- Lucas, E. (2014). The Snowden Operation: Inside the West's Greatest Intelligence Disaster. Amazon Digital Services.
- Maass, P. (2013). How Laura Poitras Helped Snowden Spill His Secrets. Retrieved from http://www.nytimes.com/2013/08/18/magazine/laura-poitras-snowden.html on April 3, 2014.
- Mirkinson, J. (2014). Brian Williams Scores Edward Snowden's First American Television Interview. Retrieved from http://www.huffingtonpost.com/2014/05/22/brian-williams-edward-snowden-interview_n_5374024.html on May 22, 2014.
- Meyer, D. (2014). Edward Snowden tells European Parliament how local spies aid NSA surveillance. Retrieved from http://gigaom.com/2014/03/07/edward-snowden-gives-testimony-to-european-parliament-surveillance-inquiry/ on March 7, 2014.
- Moyers, B. (2014). Anatomy of the Deep State. http://billmoyers.com/2014/02/21/anatomy-of-the-deep-state/ on March 31, 2014.
- NBC News. (2014). Citizens' Racy Photos Shared Among NSA Workers, Snowden Says. http://www.nbcnews.com/storyline/nsa-snooping/citizens-racy-photos-shared-among-nsa-workers-snowden-says-n160916, retrieved on July 23, 2014.
- Newsmax. (2013). NSA, Military Beef-Up Cybersecurity Measures in Wake of Leaks. Retrieved from http://www.newsmax.com/US/NSA-Military-cybersecurity-leaks/2013/07/19/id/515984 on July 19, 2013.
- Reuters. (2014). Edward Snowden, Glenn Greenwald urge caution of wider government monitoring at Amnesty event. Retrieved from http://www.dnaindia.com/world/report-edward-snowden-glenn-greenwald-urge-caution-of-wider-government-monitoring-at-amnesty-event-1975659 on April 6, 2014.

ILLINOIS INSTITUTE OF TECHNOLOGY

References

- Reuters. (2014) US' National Security Agency, Struggling to Recruit Top Talent, Turns to Silicon Valley. Retrieved from http://www.ndtv.com/article/world/us-national-security-agency-struggling-to-recruit-top-talent-turns-to-silicon-valley-572704 on August 8, 2014.
- Rodriguez, S. (2014). NSA posed as Facebook to infect computers with malware, report says. Retrieved from http://www.latimes.com/business/technology/la-fi-tn-nsa-posing-facebook-malware-20140312,0,3491724.story#ixzz2yGiHhZJa on March 12, 2014.
- RT. (2014). Spooking the spooks: US surveillance system to muzzle rogue agents and leakers. Retrieved from http://rt.com/usa/us-government-internal-monitoring-870/ on March 10, 2014.
- RT. (2014). 'NSA in da house': German artist lights up US Embassy Retrieved from http://rt.com/news/174196-berlin-artist-obama-embassy/ on July 20, 2014.
- RT. (2014). Former CIA director: 'We kill people based on metadata'. Retrieved from http://rt.com/usa/158460-cia-director-metadata-kill-people/ on May 12, 2014.
- Rusbridger, A. and MacAskill, E. (2014). The Guardian Exclusive: Whistleblower says NSA revelations mean those with duty to protect confidentiality must urgently upgrade security. Retrieved from http://www.theguardian.com/world/2014/jul/17/edward-snowden-professionals-encrypt-client-communications-nsa-spy on July 20, 2014.
- Rusbridger, A. and MacAskill, E. (2014). I, spy: Edward Snowden in exile. Retrieved from http://www.theguardian.com/world/2014/jul/18/-sp-edward-snowden-interview-rusbridger-macaskill on July 19, 2014.
- Sanger, D. and Schmidtt, E. (2014). Spy Chief Says Snowden Took Advantage of 'Perfect Storm' of Security Lapses. Retrieved from http://www.nytimes.com/2014/02/12/us/politics/spy-chief-says-snowden-took-advantage-of-perfect-storm-of-security-lapses.html on February 12, 2014.

ILLINOIS INSTITUTE OF TECHNOLOGY

References

- Sardesai, N. (2014). NSA is Working on an Encryption-Cracking Quantum Computer. Retrieved from http://www.cryptocoinsnews.com/2014/01/03/nsa-working-encryption-cracking-quantum-computer/ on March 1, 2014.
- Schneier, B. (2013). Snowden's Cryptographer on the NSA & Defending the Internet. Retrieved from https://www.youtube.com/watch?feature=player_embedded&v=kWNk9irv1e8 on March 10, 2014.
- Snowden, E. (2014. Edward Snowden's Testimony to the European Union Parliament. Retrieved from http://www.europarl.europa.eu/document/activities/cont/201403/20140307ATT80674/20140307ATT80674EN.pdf on March 7, 2014.
- Snowden, E. (2104). TED Talk: Here's how we take back the Internet. Retrieved from http://www.youtube.com/watch?v=EomroTpkaYI on March 20, 2014.
- Vanity Fair. (2014). Snowden Speaks: A Vanity Fair Exclusive. Retrieved from http://www.vanityfair.com/online/daily/2014/04/edward-snowden-interview on April 9, 2014.
- NSA WHISTLEBLOWER: SNOWDEN NEVER HAD ACCESS TO THE JUICIEST DOCUMENTS
- Washington's Blog. (2014). NSA WHISTLEBLOWER: SNOWDEN NEVER HAD ACCESS TO THE JUICIEST DOCUMENTS Retrieved from http://www.infowars.com/nsa-whistleblower-snowden-never-had-access-to-the-juiciest-documents/ on June 8, 2014.

ILLINOIS INSTITUTE OF TECHNOLOGY

Career Opportunities?

- Yes – The U.S. Government is hiring Cybersecurity Professionals
- Private Industry will be picking up more and more Cybersecurity experts

Career Development Opportunities?

Illinois Institute of Technology

- M.S. in Cyber Forensics and Security (land campus)

Information Technology and Management » Master of Cyber Forensics and Security »

Master of Cyber Forensics and Security

There is a critical need in both the government and private sectors for professionals equipped to prevent, counteract and investigate cybercrimes and information security breaches. According to Bloomberg the average cost of security breaches in the U.S. is 7.2 million dollars per incident. Gartner studies show that the average enterprise spends 5.6% of their it budget on information security, making this a nearly one trillion dollar a year industry. The need for educated professionals in this field is clearly spelled out in documents such as the U.S. Committee on National Security Systems Directive No. 500 Information Assurance (IA) Education, Training, and Awareness which mandates information assurance education for the professionals necessary to ensure the development and implementation of a comprehensive approach for the protection of U.S. Government national security systems and the information they store, process, or transmit.

The *Master of Cyber Forensics and Security* degree is designed to equip experienced information technology professionals with the necessary knowledge and tools to fill the need for educated cyber security and forensics practitioners, investigators and managers. Built around a strong core of courses originally developed for IIT's Information Technology and Management degrees, the program also draws on courses from the IIT Chicago-Kent College of Law curriculum to give cyber security and forensics practitioners the necessary thorough grounding in legal issues and compliance. Courses are taught by experts in the field who not only have academic knowledge but years of experience in the information security realm in both industry and government service.

http://www.itm.iit.edu/cybersecurity/index.php

ILLINOIS INSTITUTE OF TECHNOLOGY

Bellevue University

Bellevue, NE (land campus and online)

- M.S. in Cybersecurity
- B.S. in Cybersecurity

M.S. Cybersecurity

- 01 - CIS 608 Information Security Management
- 02 - CYBR 515 - Security Architecture and Design
- 03 - CYBR 510 Physical, Operations, and Personnel Security
- 04 - CIS 537 Introduction to Cyber Ethics
- 05 - CIS 607 Computer Forensics
- 06 - CYBR 520 Human Aspects of Cybersecurity
- 07 - CYBR 610 Risk Management Studies
- 08 - CYBR 525 Ethical Hacking and Response
- 09 - DET 630 Cyber Warfare & Deterrence
- 10 - CYBR 625 Business Continuity Planning and Recovery
- 11 - CYBR 615 Cybersecurity Governance and Compliance
- 12 - CYBR 650 Current Trends in Cybersecurity

http://www.bellevue.edu/degrees/graduate/cybersecurity-ms/

BELLEVUE UNIVERSITY

Presenter Bio:
William Favre Slater, III

- IT professional since July 1977
- Owner of Slater Technologies, Inc.
- Currently a Senior IT Consultant in IT Security, Information Security, IT Infrastructure Management, Data Center Operations & Development, IT Change Management, Application System Development, Technical Service Development, and Service Management
- An Adjunct Professor at the Illinois Institute of Technology – for over six years
- first Data Center Manager of Microsoft's Flagship Cloud Data Center, the Microsoft Chicago Data Center in 2008
- Managed Data Centers at BP from August 2001 – November 2006, was also a Change Management Manager and a System Administrator during that time.
- Have achieved 80 IT-related certifications, including PMP, CDCP, CISSP, SSCP, CISA, MCITP, MS Project, Visio, MCSE 2003 Security & Messaging, MCSD, MCAD, MCDST, and MCT
- Data Center Technology Program – Marist College & and the Institute of Data Center Professionals, February 2008 – Received the Certified Data Center Professional Certification
- M.S. in Cybersecurity – Bellevue University, Bellevue, NE. 2013
- MBA, University of Phoenix, 2010
- MS in Computer Information Systems, University of Phoenix, 2004
- BS in Engineering Technology with a major in Computer Systems Technology, University of Memphis
- Published author & editor: Magazines, books, courseware
- Subject Matter Expert in Cybersecurity for Caveon Courseware and Testing
- Happily married (since December 2000) to Joanna K. Roguska, who is a professional web developer
- A former U.S. Air Force computer systems staff officer at Strategic Air Command Headquarters supporting the SAC Underground and SAC Battle Staff Command Control Communications Systems, July 1977 – October 1980
- Native of Memphis, Tennessee
- Resident of Chicago
- A Black belt in Kodokan Judo, since 1990
- Active Judo Player and Former member of Chicago Police Judo Club (http://billslater.com/judo)

ILLINOIS INSTITUTE OF TECHNOLOGY

Presenter Bio: William Favre Slater, III

- **Current Position – Project Manager / Sr. IT Consultant at Slater Technologies, Inc.** Working on projects related to
  - Security reviews and auditing
  - ISO 27001 Project Implementations
  - Subject Matter Expert for preparing Risk Management and Security Exams at Western Governor's State University in UT
  - Created an eBook with articles about Security, Risk Management, Cyberwarfare, Project Management and Data Center Operations
  - Providing subject matter expert services to Data Center product vendors and other local businesses.
  - Developing and presenting technical training materials for undergraduate and graduate students at the Illinois Institute of Technology in the areas of Data Center Operations, Data Center Architecture, Cyber Security Management, and Information Technology hardware and software.

ILLINOIS INSTITUTE OF TECHNOLOGY

William Favre Slater, III
Contact Information:

- William Favre Slater, III
  - MBA, M.S., PMP, CISSP, SSCP, CISA, ISO 27002, ISO 20000, ITIL v3, IP v6 Project Manager / Program Manager
  - slater@billslater.com
  - williamslater@gmail.com
  - Career Page: http://billslater.com/career
  - LinkedIn: http://www.linkedin.com/in/billslater
  - Twitter: http://twitter.com/billslater (@billslater)
  - Skype: billslater
  - 773 - 235 - 3080 - Home Office
  - 312 - 758 - 0307 - Mobile
  - 312 - 275 - 5757 – FAX
  - 1337 N. Ashland Ave. No. 2
  - Chicago, IL 60622
  - United States of America

ILLINOIS INSTITUTE OF TECHNOLOGY