THE N.S.A. COMES CLEAN

GREETINGS SUSPECTS!

D'OH! I MEAN, CITIZENS!

HOWEVER—WE UNDERSTAND THAT SOME AMERICANS FEEL THEIR PRIVACY HAS BEEN VIOLATED.

I HAVE A LIST OF THEIR NAMES RIGHT HERE.

HEH HEH, LITTLE SURVEILLANCE HUMOR THERE.

AND THERE'S NO NEED TO WORRY—YOUR DATA IS SAFE WITH US!

I MEAN, SURE, THERE WAS THAT TIME WE GOT CAUGHT EAVESDROPPING ON THE PHONE SEX CALLS OF AMERICAN TROOPS IN IRAQ—

--AND WELL, PASSING THEM AROUND THE AGENCY FOR LAUGHS—*

*ALL TRUE.

BUT SERIOUSLY—THE N.S.A. IS HERE TO HELP! THAT'S WHY WE'RE INTRODUCING OUR NEW OUTREACH PROGRAM--PRISM PLUS!

IT'S THE CLOUD BACKUP YOU NEVER EVEN KNEW YOU HAD!

- OR SO THEY HOPES.

BUT THAT WILL NEVER HAPPEN AGAIN! YOU HAVE OUR WORD!

HAVE WE EVER LIED TO YOU?

I MEAN, IN THE LAST WEEK OR TWO?

THAT YOU CAN PROVE?

OKAY THEN!

REMEMBER--WE'RE THE N.S.A.—

AND WE'RE WATCHING YOU!

D'OH! I MEAN WATCHING OUT FOR YOU!

I ALWAYS GET THAT MIXED UP.

AFTER ALL, YOU NEVER KNOW WHO MIGHT TURN OUT TO BE A SCARY TERRORIST!

(A DRAMATIZATION)
ALL MATERIALS ARE DECLASSIFIED AND IN THE PUBLIC DOMAIN
Surveillance of US Citizens
AND ITS IMPACTS ON OUR ECONOMY...

Robert L. Foster
September 2013
bfoster@apogee.us
512-550-2799
TO BE DISCUSSED: IMPACTS ON ECONOMY

- National Security Impacts
- International Relationships
- Peoples’ Trust of the Government
- Internet/Wireless Communications
- Innovation
- Politics
- Direct Impacts: e.g., “Surveillance concerns bring an end to crusading site Groklaw”
**SOME HISTORY**

- 1920’s – Army Gets “Black Chamber” & Western Union
- **SHAMROCK Formed 1945 NSA Formed 1952 – Took Over SHAMROCK**
- 1956 FBI Launched COINTEL PRO – to disrupt “Commies”
- **Law Changes in 1959 Unfettered NSA’s Powers**
  - Established Centers in New York, San Francisco and San Antonio
- By 1960’s COINTEL PRO was Lawless Dragnet (Nixon, JE Hoover)
- **1969 – MINARET REPLACES SHAMROCK**
- 1970 – 100’S Co’s Partner w/ NSA; FBI/CIA Feed Domestics
- **Church Commission Exposed Violations of 4th Amendment: 1975**
- 1978 – MINARET’S WRONGDOINGS LED TO FISA
- **2001 -- 9-1-1, PATRIOT ACT PASSED**
- 2006 – ROOM 641A in San Francisco Exposed
- **2007 – Protect America Act – PRISM TAKES ITS FIRST RASPY BREATH**
- 2008 – Requirement for Warrants Removed
- **2012 – AG, DNI, D-NCTC Update Domestic Spy Rules**
- 2012 – President Extends FAA for Five Years, Modifies COGCON 5
The Supreme Court in February 2013 dismissed a challenge to FAA’s constitutionality on the grounds that its bringers lacked standing, since they couldn’t prove that their communications with foreigners had been monitored under the act’s authority.
What Sequester?

- GWOT – Opened the Purse Strings for ISR
- NSA Budget 17% - 20% of National Intelligence Program
- Estimated conservatively at $58 Billion
- NIP Budget Estimated at $313 Billion +
- JUST THE TIP OF THE SPY-BERG...
Future Expenditures on Domestic Intelligence Data

- **Intelligence Advanced Research Projects Activity (IARPA)**
  - invest in high-risk, high-payoff classified programs for the Intelligence Community.

- **Aladdin Program**
  - to extract intelligence information from the high volume of videos uploaded to the internet.

- **Babel Program**
  - developing agile a speech recognition technology for massive amounts of real recorded speech.

- **Knowledge Discovery and Dissemination (KDD) program**
  - Developing advanced analytic algorithms
  - that can effectively draw inferences across multiple databases
  - to allow the Intelligence Community to create virtual fusion centers
  - enabling analysts to produce actionable intelligence.

- **Socio-cultural Content in Language (SCIL) Program**
  - developing novel algorithms and technologies to reveal/analyze group members
  - by examining the language used in relation to acceptable social and cultural norms.

- **Reynard Program**
  - seeks to identify behavioral indicators in online virtual worlds and "massively multiplayer online games" that are related to the real world characteristics of the users.
  - Attributes of interest include gender, age, economic status, educational level, occupation, ideology or "world view", and physical geographic location.
• Much of the world’s communications flow through the U.S.

• A target’s phone call, e-mail 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 U.S.

86% of the World’s Internet Traffic Traverses the USA

International Internet Regional Bandwidth Capacity in 2011
Source: Telegeography Research
IMMUNITY AND COERCION
No Warrant Required – Just E. Holder’s Directive

SOURCE OF 98% OF DATA

PRISM Program Cost: ~ $20M per year
Other Sources/Partners Publicly Disclosed

- **CIA’s CTO** – “We fundamentally try to collect everything and hang onto it forever.”
- **FBI** – DCSNet:
  - Google-Like Search of the...
  - FBI Law Enforcement National Data Exchange Program
  - Stingray IMSI Catchers (Smart Phone Intercepts)
- **DHS** – Passenger Data, Drones
- **US Treasury** -- SAR Reporting
- **USPO** – WILL MENTION LATER
- **US Congress** – FISA Amendments 2012 – “Back Doors”
- **State & Local** – Elec. Transit Cards, Tool Booths, License Plate Readers, Public Transportation Audio & Video Captures
- **US, AUS, CAN, GBR, NZL** – Share Info From Commercial Companies
All internet traffic (emails, web browsing, transactions)

U.S. Citizens

Telecommunication Company

Fiber-optic Splitter

NSA Data Intercept Station

NSA Utah Data Center (Fall 2013)
How the NSA collects your data

**SOURCES**

- **Telecommunications Cables**
  - AT&T
  - Verizon
  - Sprint
  - Facebook
  - Apple
  - Google
  - Microsoft
  - Yahoo
  - AOL

- **PATRIOT ACT**
  - Section 215

- **FISA AMENDMENTS ACT**
  - Section 702

**NSA**

- **DEPARTMENT OF JUSTICE**
  - **FBI**
  - **NSA**

- **CENTRAL INTELLIGENCE AGENCY**
  - **CIA**

- **NATIONAL SECURITY AGENCY**
  - **NSA**

- **GCHQ**

**PROJECTS**

- **FAIRVIEW, STORMBREW, BLARNEY, AND OAKSTAR**
  - ("Upstream" Data)

- **MAINWAY**
  - (Phone Metadata)

- **NUCLEON**
  - (Phone Content)

- **PRISM**
  - (Internet Content)

- **MARINA**
  - (Internet Metadata)

- **SHELLTRUMPET & EVILOLIVE**
  - (Internet Metadata)

- **MOONLIGHTPATH**
  - (Internet Metadata, planned Sept. 2013)

- **SPINNARET**
  - (Internet Metadata, planned Sept. 2013)
WHAT INFO IS COLLECTED BY PRISM/OTHERS

- Internet searches
- Websites visited
- emails sent and received
- Social media activity (Facebook, Twitter, etc.)
- Blogging activity including posts read, written, and commented on
- Videos watched and/or uploaded online
- Photos viewed and/or uploaded online
- Mobile phone GPS-location data
- Mobile phone apps downloaded
- Phone call records
- Text messages sent and received
- Skype video calls
- Digital “Pocket Litter”

- Online purchases and auction transactions
- Credit card/ debit card transactions
- Financial information
- Legal documents
- Travel documents
- Health records
- Cable television shows watched and recorded
- Commuter toll records
- Electronic bus and subway passes / Smartpasses
- Facial recognition data from surveillance cameras
- Educational records
- Arrest records
- Driver license information
- SIM Cards & CCTV via “Stingray” (IMSI)
- SMART Meters, WiFi Appliances
Our Undersea Cable Tapping Strategy
By tapping into the worldwide network of undersea cables, our OAKSTAR, STORMBREWS, BLARNEY and FAIRVIEW systems can process data as it flows across the internet. Each system is responsible for different types of intercepted data. For example, the BLARNEY system gathers metadata describing who is speaking to whom and through which networks and devices.
Two methods are employed for tapping into the undersea cable network:

- A modified nuclear submarine houses technicians and gear needed to place the physical taps on the undersea cables along strategic points in the network.
- Second method uses intercept probes at the point where cables connect to the landing stations in various countries. These probes capture and copy the data as it flows onward. “Jimmy Carter” Sub $3.2 Billion
"I, sitting at my desk," said Snowden, could "wiretap anyone, from you or your accountant, to a federal judge or even the president, if I had a personal email".
X-KEYSCORE – REAL TIME DATA MINING

• Near-comprehensive access to a target's activity, from email to chat, to accessed, to social media activity
• No authorization required
• Real-time surveillance of any target's internet activity
• Capacity to target "US persons for extensive electronic surveillance without a warrant..." the Guardian reports
• If an analyst wants to look back on a target's Google Maps search history, for example, he or she can: "XKEYSCORE extracts and databases these events including all web-based searches which can be retrospectively queried" (slide 20)
• Open access for analysts to the databases
• One PowerPoint slide titled, "What Can Be Stored?" boasts "Anything you wish to extract"
• In 2012, there were at least 41 billion total records collected and stored in XKeyscore for a single 30-day period," the Guardian reports
• Collects 20 Terabytes Daily
• Content remains on the system for only three to five days, while metadata is stored for 30 days.
The Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) is a collaborative effort led by the U.S. Department of Justice in partnership with the Department of Homeland Security, the FBI, and state and local law enforcement partners. This initiative establishes a national capacity for gathering, documenting, processing, analyzing, and sharing SAR information gathered by fusion centers across the county.
Visible Intermodal Prevention and Response (VIPR)

Office of Law Enforcement/Federal Air Marshal Service:
No Warrant Required.

TSA VIPR teams can be deployed at random locations and times in cooperation with local authorities to deter and defeat terrorist activity; or teams may be deployed to provide additional law enforcement or security presence at transportation venues during specific alert periods or in support of special events. **TSA routinely conducts thousands of VIPR operations each year in transportation systems nationwide.**
PRIORITY MAIL IS NOW EVEN BETTER.

Three major improvements are making Priority Mail an even easier way to ship in the U.S.

- IMPROVED USPS TRACKING™
- FREE INSURANCE UP TO $50
- DAY SPECIFIC DELIVERY

LEARN MORE ›

THE ADDRESS SIDE OF EVERY PIECE OF MAIL IS PHOTOGRAPHED AND STORED
Located in states and major urban areas,

Centers are uniquely situated to empower:

- front-line law enforcement
- public safety
- fire service
- emergency response
- public health, and
- private sector security personnel to gather and share domestic threat-related info
Tracking Our Surveillance Data: Boundless Informant

The "Boundless Informant" mapping tool provides analysts the means to track intelligence collection statistics worldwide. Using a color-coded map, they can quickly determine the volume of collection data by geographical location. This global heat map assigns each nation a color code based on its surveillance intensity ranging from green (least subjected to surveillance) through yellow and orange to red (most surveillance). With the monthly domestic intelligence collection volume at almost three billion pieces, the United States is assigned the color orange.
Main Core: Our Secret Database of Watchlisted Americans

The Main Core database tracks Americans who are considered potential threats in the event of a national emergency.

The NSA’s Domestic Surveillance Directorate is now the main source of intelligence feeding into the modern version of the Main Core system.

It was first developed in the 1980s using software called PROMIS, which was designed as a case management system by a private company, Inslaw, for federal prosecutors. It provided the ability to track people within the legal system across multiple databases. The PROMIS software was taken from Inslaw via allegedly “trickery, fraud and deceit” by the Department of Justice and modified by US intelligence agencies to monitor intelligence operations, agents and targets.

The software had users in multiple federal agencies including Lt. Col. Oliver North who created a secret dissident tracking system under the Reagan Administration’s Continuity of Government program. The database includes domestic e-mails, internet searches, bank transfers, credit card transactions, travel, phone, and other records allowing authorities to identify and locate those deemed 'enemies of the state' almost instantaneously in an emergency.
The TSC maintains the U.S. government's consolidated Terrorist Watch list, a single database of identifying information about those known or reasonably suspected of being involved in terrorist activity.

The FBI Terrorist Screening Center (TSC) was established in 2003 by Homeland Security Presidential Directive 6 which directed that a center be established to consolidate the government's approach to terrorism screening.
OLD “IRON” – DATA MINING
“TRUTHY” EXAMPLE: TWITTER DATA MINING TODAY...
APPLICATIONS PRESENTED TO COURT

Though the details of the applications are classified, the attorney general is required by law to report to Congress the total number of granted, modified or denied applications. The attorney general briefs select intelligence committees in the House and Senate about electronic surveillance on a semiannual basis.

Total number of electronic surveillance requests submitted to the court since 1979, by administration and year

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>CARTRG</td>
<td>518</td>
<td></td>
<td>115</td>
<td>204</td>
<td>124</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0 denied</td>
<td>0</td>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>REAGAN</td>
<td>4,294</td>
<td>2,284</td>
<td>1,154</td>
<td>645</td>
<td>338</td>
<td>160</td>
<td>83</td>
<td></td>
</tr>
<tr>
<td>0 denied</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>H.W. BUSH</td>
<td>2,218</td>
<td>1,154</td>
<td>645</td>
<td>338</td>
<td>160</td>
<td>83</td>
<td>83</td>
<td></td>
</tr>
<tr>
<td>0 denied</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>CLINTON</td>
<td>6,057</td>
<td>3,028</td>
<td>1,514</td>
<td>757</td>
<td>378</td>
<td>189</td>
<td>93</td>
<td></td>
</tr>
<tr>
<td>1 denied</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>BUSH</td>
<td>14,353</td>
<td>6,142</td>
<td>3,028</td>
<td>1,514</td>
<td>757</td>
<td>378</td>
<td>189</td>
<td>93</td>
</tr>
<tr>
<td>9 denied</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>OBAMA</td>
<td>6,556</td>
<td>2,672</td>
<td>1,336</td>
<td>668</td>
<td>334</td>
<td>167</td>
<td>83</td>
<td></td>
</tr>
<tr>
<td>1 denied</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

During the first 23 years of the Foreign Intelligence Surveillance Act, about 14,000 requests — or more than 600 per year on average — were submitted to the court.

Since Sept. 11, 2001, the average number of requests has nearly tripled to about 1,700 per year.

FISA
<table>
<thead>
<tr>
<th>Year</th>
<th># Requests Submitted</th>
<th># Requests Modified</th>
<th># Requests Denied</th>
<th>Cumulative # Warrants Issued</th>
</tr>
</thead>
<tbody>
<tr>
<td>1979–1999</td>
<td>12,082</td>
<td>0</td>
<td>0</td>
<td>12,090</td>
</tr>
<tr>
<td>1979</td>
<td>199</td>
<td>0</td>
<td>0</td>
<td>207[7]</td>
</tr>
<tr>
<td>2000</td>
<td>1,005</td>
<td>1</td>
<td>0</td>
<td>13,102 [c]</td>
</tr>
<tr>
<td>2001</td>
<td>932</td>
<td>2</td>
<td>0</td>
<td>14,036</td>
</tr>
<tr>
<td>2002</td>
<td>1,228</td>
<td>2 [d]</td>
<td>0</td>
<td>15,264</td>
</tr>
<tr>
<td>2003</td>
<td>1,724</td>
<td>79</td>
<td>4 [e]</td>
<td>16,988</td>
</tr>
<tr>
<td>2004</td>
<td>1,758</td>
<td>94</td>
<td>0</td>
<td>18,742</td>
</tr>
<tr>
<td>2005</td>
<td>2,074</td>
<td>63</td>
<td>0</td>
<td>20,814</td>
</tr>
<tr>
<td>2006</td>
<td>2,181</td>
<td>77</td>
<td>1</td>
<td>22,990</td>
</tr>
<tr>
<td>2007</td>
<td>2,371</td>
<td>86</td>
<td>4</td>
<td>25,360</td>
</tr>
<tr>
<td>2008</td>
<td>2,082</td>
<td>2</td>
<td>1</td>
<td>27,443</td>
</tr>
<tr>
<td>2009</td>
<td>1,329</td>
<td>14</td>
<td>1</td>
<td>28,763</td>
</tr>
<tr>
<td>2010</td>
<td>1,511</td>
<td>14</td>
<td>0</td>
<td>30,342</td>
</tr>
<tr>
<td>2011</td>
<td>1,676</td>
<td>30</td>
<td>0</td>
<td>32,087</td>
</tr>
<tr>
<td>2012</td>
<td>1,789</td>
<td>40</td>
<td>0</td>
<td>33,942</td>
</tr>
<tr>
<td>TOTALS</td>
<td>33,949</td>
<td>11 [f]</td>
<td></td>
<td>33,942</td>
</tr>
</tbody>
</table>
Privacy group takes NSA spying challenge straight to the Supreme Court

ROSARIAN AND “CATCH 22”
PRISM Checks and balances

• The program as a whole
  • Authorized once a year
  • In a secret order from the Foreign Intelligence Surveillance Court. (FISA Court)
• However, there are no individual warrants, even for access to full content.
• Before an analyst may conduct live surveillance using PRISM
  • A second analyst in his subject area must concur.
• In this “validation” process, the second analyst
  • Confirms that the surveillance has a valid foreign-intelligence purpose,
  • That there is a “reasonable belief” the target is neither American nor on U.S. soil
  • And that the surveillance complies with NSA regulations and the classified judicial order interpreting Section 702 of the FISA Amendments Act.
• For stored content, a similar review takes place in the NSA’s office of Standards and Compliance.
• There is a second review by the FBI
  • ensures the target does not match a U.S. citizen or U.S. resident in FBI files.
FEDERAL CONTINUITY RESPONSE

Federal executive branch government employees at their normal work locations. Maintain alternate facility and conduct periodic continuity readiness exercises.

Federal agencies and departments Advance Relocation Teams “warm up” their alternate sites and capabilities, which include testing communications and IT systems. Ensure that alternate facilities are prepared to receive continuity staff. Track agency leaders and successors daily.

Deployment of 50-75% of Emergency Relocation Group continuity staff to alternate locations. Establish their ability to conduct operations and prepare to perform their organization’s essential functions in the event of a catastrophic emergency.

Full deployment of designated leadership and continuity staffs to perform the organization’s essential functions from alternate facilities either as a result of, or in preparation for, a catastrophic emergency.

Activate classified CONPLAN 3600 evacuating the President and those in the line of presidential succession. Activate classified CONPLAN 3502 deploying the military to enforce law and order within the Civilian Control Districts. Seize all private communication facilities and assume control over all civilian voice and data communications. Activate internet kill switch. Commandeer all U.S. domestic resources including food and water. Seize all domestic energy and transportation infrastructure. Deploy the national citizen conscription plan to fulfill any labor required for the purpose of national defense and reconstitution.

THE UNITED STATES IS UNDER A STATE OF EMERGENCY
IMPACTS ON OUR ECONOMY

- INTERNATIONALLY SHARED INFRASTRUCTURE
- POLITICAL COMMUNICATIONS
- TERRORISM
- PRODUCT INNOVATION
- PRODUCT INNOVATION DISCOURAGEMENT
- BANDWIDTH CONSUMPTION: ENCRYPTION
- SECURITY BREACHES
- SOCIAL MEDIA IMPACTS
- ONLINE ENTERTAINMENT
- SEIGE MENTALITY
Impacts on US Economy

• Data Center Companies
• Cloud-based Companies
  – 10% of Non-US Co’s Cancel Contracts (Cloud Sec. Alliance report)
  – 56% of Non-Residents Hesitant to do Business w/US
  – Forrester Research says loss could be $180 Billion Annually
• Cities & States that are Telecom Centers
  – California Exposed
• Foreign Companies
• Complicit US Companies
• Unintended Consequences
  – Push for Personal Encryption
  – Encryption Impact on Bandwidth
  – Encryption Impact on Speed
  – Encryption Impact on Surveillance