THREATS TO YOUR PRIVACY RIGHTS: THE CHILLING EFFECTS OF ONLINE SURVEILLANCE

Legal Representation by Lawrence, G. Walters, Esq.
FIRSTAMENDMENT.com

WEB LAW NETWORK™
www.weblawnetwork.com

Presented by:

Lawrence G. Walters, Esq.

larry@firstamendment.com

www.FirstAmendment.com

www.WeblawNetwork.com

Walters Law Group™



Imagine a place…

Where the government recorded everything you said…

Stored every purchase you made…

Tracked your movements…

Knew what you looked for…

Could monitor every key stroke of your computer…

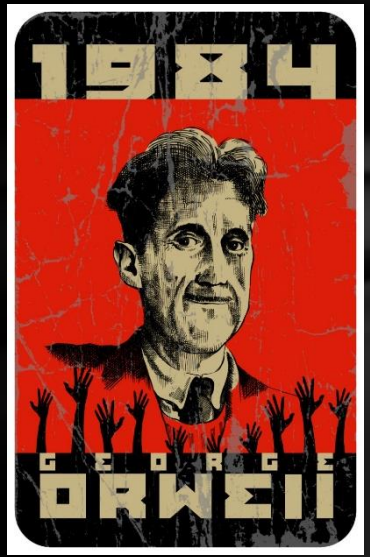
Created secret courts, that met in private, and made secret decisions impacting the privacy of ordinary citizens…

Spent your tax dollars to monitor social networking sites for ideas they found to be “misleading”…

Told the police to lie about how they got evidence…

…and was accountable to no one…

“BIG BROTHER IS WATCHING YOU”



Why Care?

Internet Usage Statistics 2013:
Total Population: 7.1 Billion
Total Internet Users: 4.3 Billion
Email Users: 3.8 Billion
Google Searches: 2 Trillion
Smartphone /Tablet Users: 1.9 Billion
Active Facebook Users: 1.6 Billion
Active Twitter Users: 234 Million



Source: FactsHunt

Cherry Picking

- If government controls all information about a person's past, their life's story can be told in such a way so as to make that person a villain or a hero.
- Such control permits government to dictate a person's future.
- Government now has that ability.

An Emerging Threat: The NSA



- Edward Snowden: Uncovered that the American government was spying on its own citizens and intercepting communications
- Although many companies deny “back door” access, others have opened systems to NSA Investigators: AT&T, Verizon
- Facebook, Microsoft & Google cooperate with NSA at some level

Dangers of Mass Data Collection

- Obtained without a warrant or any specific suspicion of criminal activity
- Stored indefinitely; Innocent citizens information stored along with those who pose potential threats
- Can reveal intimate information and details about our private activity, discussions, thoughts and relationships
- Encrypted information can be stored until computers are powerful enough to crack the security codes
- Investigators can go 'back in time' and cherry pick information to make anyone out to be a villain or a hero

“I’ve got nothing to hide”

"What are people worried about? What is the problem? Are you doing something you're not supposed to?”

- Trent Lott, when defending the NSA’s MAINWAY mass cell phone data collection practice.

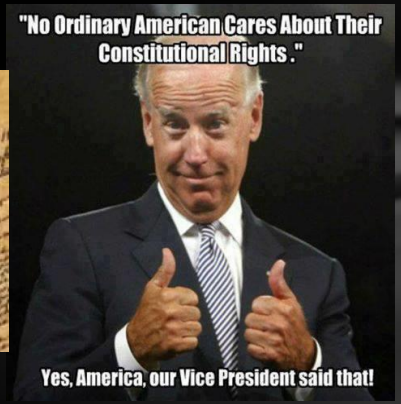
Common refrain in response to privacy concerns

Conflates individual concerns with overall public’s right to be free from governmental intrusion in a free society

Ultimately results in the loss of personal privacy

Constitutional Rights are Collective Not Personal





Snowden: Whistleblower or Traitor

NSA Former Chief Michael Hayden says Snowden is “morally Arrogant” and will end up an “Alcoholic”

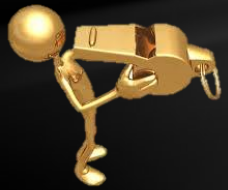


ACLU says Snowden is clearly a “whistleblower” under federal law



What's A Whistleblower?

- Federal law, with the Whistleblower Protection Act, protects "any disclosure" that a covered employee reasonably believes evidences "any violation of any law, rule, or regulation," or "gross mismanagement, a gross waste of funds, and abuse of authority, or a substantial and specific danger to public health or safety."



The NSA Tracks:



Social media



75% of all Internet traffic
(WSJ)

Alternatives Exist

Non-tracking search engines;

E.g., DuckDuckgo.com



TOR anonymous IP browser



Encrypted, Private Email Services;

E.g. Proton Mail protonmail.ch



Official Demands

- Yahoo received over 12,000 requests for user data from law enforcement agencies
- Apple received over 5000 requests
- Facebook received over 10,000 requests in a 6 month period

Source:
Money.CNN.com

Google Requests for User Data

2009 – 12,000
2010 – 14,000
2011 – 20,000
2012 – 25,000
2013 – 31,000



Responses that included user data: 75%

NSA's Social Media Policy

- Previously, "chaining" together of foreign person's contacts needed to stop when it reached American citizen or legal resident



- In 2010, policy changed
- Policy change was to help NSA "discover and track" connections from foreign intelligence subject to American citizen
- NSA uses social media, geo-location information, insurance and tax records, metadata of emails
- NSA analysts use software to create diagrams of a person's activity, including companions, social networks, and email contacts

Source: CNN

NSA May Even…

- Break into computers and infect them with malware “implants”

"In some cases the NSA has masqueraded as a fake Facebook server, using the social-media site as a launching pad to infect a target's computer and exfiltrate files from a hard drive […] In others, it has sent out spam emails laced with the malware, which can be tailored to covertly record audio from a computer's microphone and take snapshots with its webcam. The hacking systems have also enabled the NSA to launch cyberattacks by corrupting and disrupting file downloads or denying access to websites.”

- *First Look Media* report

- The NSA, of course, has denied this

Source: CNN

NSA Spy Shop: The ANT Catalog



NSA Ant Catalog: 48-page (classified) document containing a list of cyber surveillance technology available across the NSA

- Examples of "products" the NSA can provide to its divisions:
  - BULLDOZER: Technology that creates a hidden wireless bridge allowing NSA personnel to remotely control a system wirelessly.
  - DROPOUTJEEP: "A software implant for the Apple iPhone that utilizes modular mission applications to provide specific SIGINT functionality. This functionality includes the ability to remotely push/pull files from the device. SMS retrieval, contact list retrieval, voicemail, geolocation, hot mic, camera capture, cell tower location, etc. Command, control and data exfiltration can occur over SMS messaging or a GPRS data connection. All communications with the implant will be covert and encrypted."
  - Source: *The Independent* (July, 2014)

More Examples of NSA “Products”

- GINSU: Technology that uses a PCI bus device in a computer, and can reinstall itself upon system boot-up.
- GOPHERSET: GSM software that uses a phone's SIM card’s API (SIM Toolkit or STK) to control the phone through remotely sent commands.
- NIGHTSTAND: Portable system that wirelessly installs Microsoft Windows exploits from a distance of up to eight miles.
- PICASSO: Software that can collect mobile phone location date, call metadata, access the phone’s microphone to eavesdrop on nearby conversations.
- SURLYSPAWN: Keystroke monitor technology that can be used on remote computers that are not internet connected.
- TOTEGHOSTLY: Software that can be implanted on a Windows mobile phone allowing full remote control.

Spreading “Chosen” Messages?

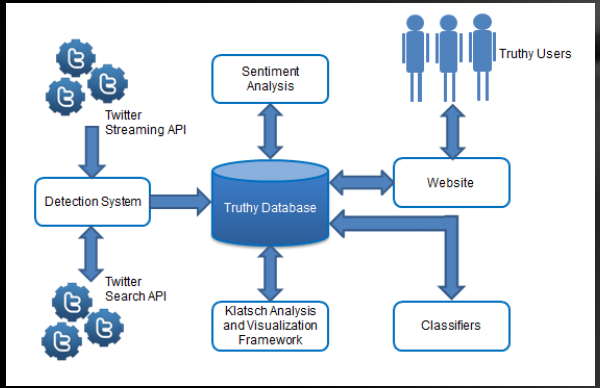
- UK’s intelligence gathering agency, GCHQ, doing something similar: has created a “toolkit” of software to “manipulate online traffic and information, infiltrate target computers” and spread “chosen messages on sites like Facebook and YouTube” (Snowden leak)



- Some examples:
  - SPRING BISHOP – “Find private photographs on Facebook”
  - CONCRETE DONKEY – “Repeatedly bomb a target number with the same message”
  - GATEWAY – “Ability to increase traffic to a website”
  - GESTATOR – “Amplification of a given message, normally video, on popular multimedia websites (Youtube)”
  - SUNBLOCK – “Ability to deny functionality to send/receive email”
  - UNDERPASS – “Change outcome of online polls”
  - CLEAN SWEEP - "masquerade[s] Facebook wall posts for individuals or entire countries"

Government Monitoring of Social Media

- "Truthy" program in development
- Online database and tool to track "misinformation," hate speech, and false/misleading **ideas**
- Truthy also monitors trends and memes
- Funded by your tax dollars to the tune of $1 million dollars



Where is all this data kept?

- In Bluffdale, Utah
- This data center will have the ability to collect ALL worldwide electronic communications and transactions
- Specs:
  - One million square feet in size
  - Power bill: $70 million per year
  - Storage estimates range from “yotabytes” (Wired) to 5 “zetabytes” of data, which can be stored indefinitely (NPR)
  - Conversion: yottabyte = 1,000 zettabytes = 1,000,000 exabytes = 1 billion pettabytes = 1 trillion terabytes.
  - The entire internet is only 1% of a yotabyte
  - Only 400 terabytes needed to hold all of the books ever written in any language.



And…It's Growing

- NSA Footprint will grow by 50% by the end of the decade. (Washington Post)



- NSA has enlarged all its major domestic sites — in Colorado, Georgia, Hawaii, Texas and Utah — as well as those in Australia and Britain.
- 60 percent of the president's daily intelligence briefing comes from the NSA. Percentage is growing.
- NSA capabilities now used to kill single individuals using geo-tracking of communications devices.
- Current NSA Motto:
  - "We Track 'Em, You Whack 'Em."

And…The Power Is Constantly Abused

- NSA Employees violated established policies over 3000 times. PRISM program designed to identify the 'foreigness' of a target with amazing 51% accuracy
- NSA Employees used surveillance information to spy on love interests (WSJ.com)
- Practice occurred often enough to earn its own spycraft name; "LOVEINT"

- Source; Snowden Documents

Denial



James Clapper, National Intelligence Director denies under oath that NSA is collecting information on millions of Americans.

At least not “wittingly.”

Parallel Construction

Law Enforcement's Dirty Little Secret:

- DOJ Officials allegedly obtain surveillance data from NSA, use the information to make a case, and create a false narrative to explain how the investigation occurred without reliance on NSA interception
- Domestic surveillance can be used in this way to prosecute garden variety crimes like drug offenses
- Silk Road case may blow the parallel construction issue wide open; motions challenge how the operator could possibly be identified without NSA help

"*Doublethink means the power of holding two contradictory beliefs in one's mind simultaneously, and accepting both of them.*"
— George Orwell, *1984*

Source: Techdirt.com (2014)

The Stingray Device

- Creates fake cell phone connection tower
- Allows law enforcement to sweep up all data to and from cell phones in the area
- Originally used only by NSA, then DOJ
- Now on loan to local police to investigate US citizens for ordinary crimes
- Emails suggest that U.S. Marshalls instructed police to lie about how they obtained the information from the Stingray device; Told to cite a 'confidential source'

Source: Techdirt.com (2014)

Opposition to Domestic Surveillance

- 66% of Americans Oppose NSA Domestic Spying Program
- Opposition Groups:
  - Stopwatching.us
  - Electronic Frontier Foundation – eff.org
  - Bill of Rights Defense Committee – bordc.org







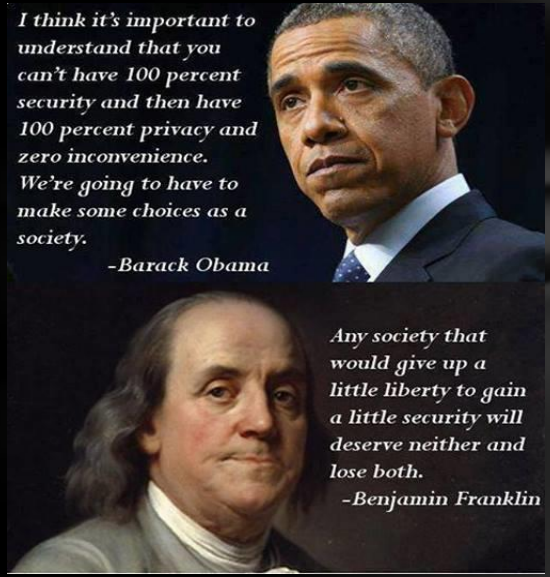
The Chilling Effect

- The First Amendment prohibits government actions that create a chilling effect on speech. *Lamont v. Postmaster General*, 381 U.S. 301 (1965)
- The "chilling effect" referred to in the case was a "deterrent effect" on freedom of expression—even when there is no law explicitly prohibiting it
- How much speech does not occur now that we know of the monitoring and storage of all electronic communications?

Unspoken Words



Liberty & Security



The Constitution, Spying & Terrorism

- How much intrusion on liberty are we willing to accept in the name of "safety" and "security"?
- Since 9/11, the Patriot Act & NSA domestic spying, the boundaries of personal liberty are shrinking dramatically
- New concerns re ISIS/ISIL may undermine NSA reform efforts.
- People are more likely to die from these other causes than from terrorism:
  - Killed by a Police Officer (8x more likely)
  - Choking on your own vomit (9x more likely)
  - Airline Travel (11,000x more likely)

Reforms – USA Freedom Act - House

- USA Freedom Act - House Version
  - Would have curbed mass collection of Internet data and phone records
  - Would have placed more limits on NSA
  - Also would have forced transparency requiring Foreign Intelligence Surveillance Act (FISA) Court to be more open regarding decision on government's use of data collection on individuals suspected of terrorist activity
- Gutted version passed in the House.
- While stuck in Senate, FISA Court reauthorized NSA's bulk collection of data

Reforms – USA Freedom Act - Senate

- Introduced by Sen. Pat Leahy, July 2014
- Substantial improvement over weakened House Version
- Would end bulk collection of cell phone data allowed under Section 215 of the Patriot Act
- Future collection efforts would be based on reasonable suspicion, and focused only on an "individual, account, or personal device"
- Creates "special advocate" position for FISA Court hearings; Special advocate will serve to protect civil liberties and privacy
- Requires the declassification of 'significant' FISA Court decisions
- Requires new reporting procedures relating to NSL letters and warrantless 'backdoor' searches

Source: Eff.org

Conclusions

- The First Amendment requires substantial 'breathing room' to allow robust discourse in a free society
- The mere existence of mass surveillance creates an intolerable chilling effect that stifles communication, creativity, and human interaction
- There is a role for the NSA and legitimate surveillance
- Balancing of interests must occur, in connection with substantial reform of the status quo
- Failure to reign in government intrusion on privacy will lead to a stifled populace that fears to speak its mind