Privacy & the NSA

"In the world we're living in, increasingly by choice and by chance, we are forfeiting privacy at levels that, as individuals, I don't think we truly understand..."

Adm. Michael Rogers, Director NSA
6/3/2014

Michael Robinson
Chair, Intellectual Freedom Committee
Alaska Library Association

Fourth Admendment

"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

Timeline

https://www.eff.org/nsa-spying/timeline

- 1791 – Bill of Rights, Fourth amendent
- 1952 – Truman establishes NSA
- 1972 – Supreme Court rules warrants are required for domestic intelligence surveillance
- 1975 – Senate committee uncovers illegal domestic spying by NSA, recommends reforms
- 1978 – Foreign Intelligence Surveillance Act to govern domestic surveillence creates a secret court to issue warrants

Timeline

https://www.eff.org/nsa-spying/timeline

- Sep 2001 – Terrorist attacks in America
- Oct 2001 – Presidential order authorizing NSA to create program to spy on domestic emails & phone calls without warrants
- Nov 2001 – DOJ opinion that the order is legal
- May 2002 – Chief justice of FISA court briefed
- Summer 2002 - AT&T technician discovers NSA is working inside AT&T facilities

Timeline

https://www.eff.org/nsa-spying/timeline

- Sep 2003 - Congress cancels military's Total Info Awareness program due to privacy concerns
- Mar 2004 – President suspends NSA internet data collection after growing concerns from DOJ
- Jul 2004 – FISA court signs order authorizing NSA internet data collection
- Dec 2005 – NYT exposes NSA domestic spying to public for first time
- Jan 2006 - USA Today reveals telecom companies which voluntarily helped in NSA domestic spying

Timeline

https://www.eff.org/nsa-spying/timeline

- May 2006 – Phone companies end voluntary agreement to hand over bulk metadata
- May 2006 – FISA court okays dragnet surveillance of telephony metadata
- Jul 2008 – Congress passes FISA Admendments Act giving telcom's immunity & expanding wiretaps
- Dec 2008 – US Attorney general declares ISPs immune from liability
- 2010 – Number of court cases dismissed either because of FISA Admendments or state secrecy

Timeline

https://www.eff.org/nsa-spying/timeline

- Jan 2011 - NSA starts construction on massive data center to house intercepted communications
- Late 2012 – Snowden begins to contact journalists
- May 2013 – Snowden delivers estimated 1.7 million documents to journalists and flees the United States
- Jun 2013 – Newspapers begin publishing articles based on the NSA documents
- Apr 2014 – Washington Post & The Guardian recieve Pulitzer Prize for its NSA reporting

Revelations So Far

- NSA collects metadata on all domestic phone calls. It also collects 5 billion records per day on location of cellphones and mobile devices around the world.
- Under a FISA authorized program called PRISM, NSA has targeted access to content from major online services including Google,Yahoo, Facebook, Apple & Microsoft.
- NSA has also infiltrated the link between data centers for Google & Yahoo which provides them with unfettered access to millions of accounts.

Revelations So Far

- NSA has access to a vast amount of intelligence data from other agencies including the CIA as well as foreign allies. This data includes tapping fiber optic cables, satellites, & cell phone signals.
- NSA works to subvert encryption through super computers, malware, court orders, and behind the scenes persuasion.
- NSA can target individual computers to install monitoring software and other malware.
- Numerous violations of NSA's own rules and a lack of oversight by FISA and Congress.

Revelations So Far

- XKeyscore is an NSA data-retrieval system which consists of a series of user interfaces, backend databases, servers and software that selects certain types of data and metadata that the NSA has already collected using other methods.

According to Snowden:

"You could read anyone's email in the world, anybody you've got an email address for. Any website: You can watch traffic to and from it. Any computer that an individual sits at: You can watch it. Any laptop that you're tracking: you can follow it as it moves from place to place throughout the world. It's a one-stop-shop for access to the NSA's information."

"…You can tag individuals… I can track your username on a website on a form somewhere, I can track your real name, I can track associations with your friends and I can build what's called a fingerprint, which is network activity unique to you, which means anywhere you go in the world, anywhere you try to sort of hide your online presence, your identity."

What's Next

- Only about 1% of documents that Snowden leaked have been published as of Nov 2013.
- Journalists continue to work their way through the material and make decisions on what to publish.
- Officials warn that the worst is yet to come.
- Several court cases pending on legality of some aspects of the NSA programs.
- New legislation – US Freedom Act to reduce scope, length of retention.

Privacy & the NSA

"They who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety."

Benjamin Franklin
1755

Michael Robinson
Chair, Intellectual Freedom Committe
Alaska Library Association