

A decorative graphic on the left side of the slide, consisting of white lines and circles on a blue background, resembling a circuit board or data flow diagram.

SENATE BILL 13: WARRANTLESS SEARCH OF ELECTRONIC DATA

SENATOR WIELECHOWSKI

STAFF: SARAH EVANS

WHAT IS THE NSA?

- NSA stands for National Security Agency
- NSA is a U.S. intelligence agency responsible for the global monitoring, collection, decoding, translation and analysis of information and data for foreign intelligence and counterintelligence purposes.
- The NSA was created in 1952

WHY SHOULD ALASKANS BE CONCERNED ABOUT THE NSA?

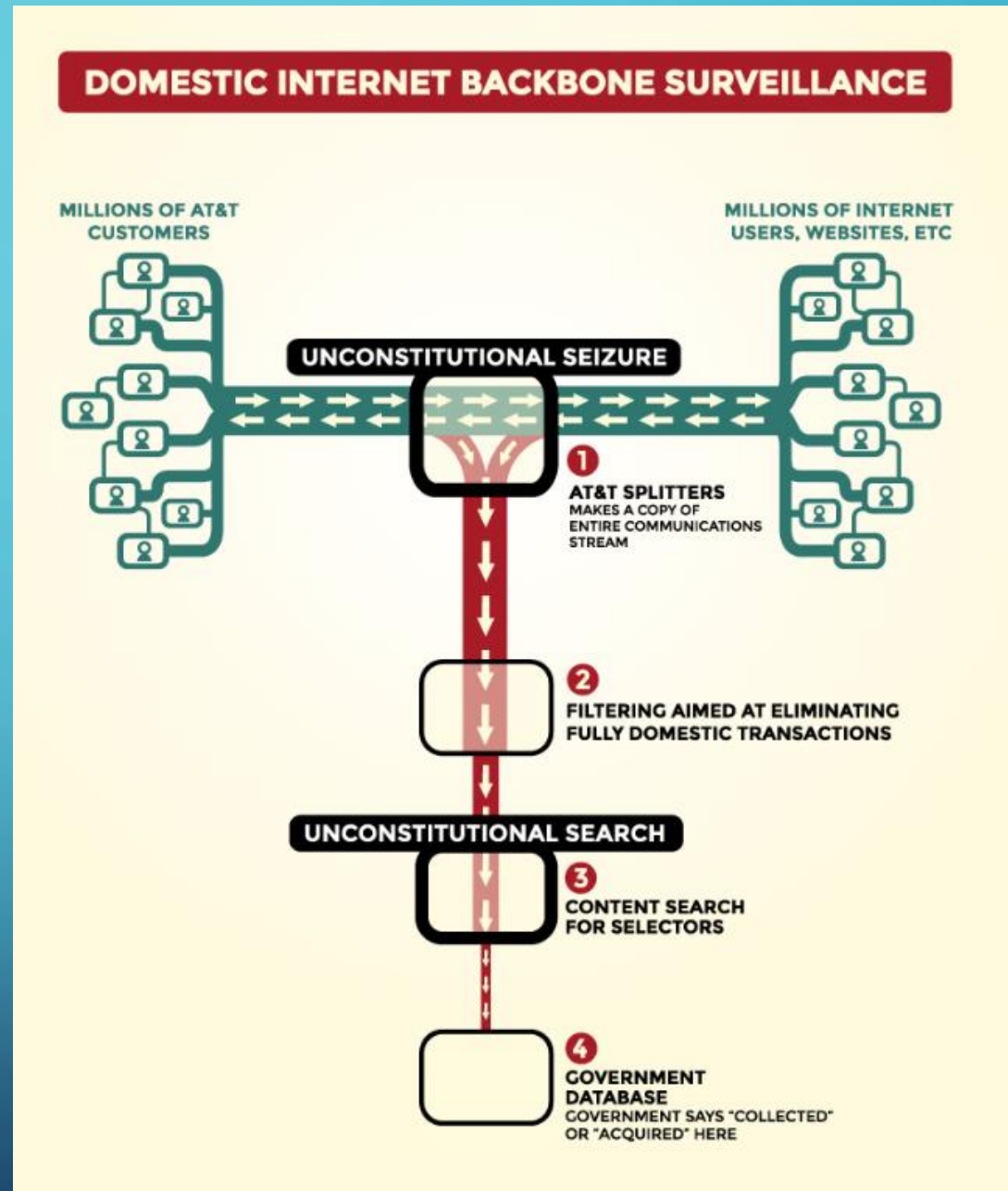
- The NSA has the ability to collect every American's phone records
- The PRISM Program lets the NSA access private user data on leading online services
- The NSA taps long-distance internet connection
- The NSA tracks cell phone locations around the world

HOW DID WE GET HERE?

- 2001 President Bush signed order beginning NSA's Domestic Spying Program after 9/11 attacks
- October 2001 the NSA had major telecommunication companies in the US hand over "call-detail records" which included customers names, street addresses and other personal information
- 2005 The NY Times exposed the NSA Spy Program for the first time.
- 2006 The NSA maxed out the Baltimore-area power grid
- 2008 President Bush signed into law the FISA Amendment Act

HOW PHONE SPYING WORKS

- In 2003 AT&T Tech. Mark Kline finds fiber-optic splitter installed by the NSA
- Thirty-Year NSA veteran, William Binney, estimates that the NSA installed between 10-20 intercept centers within the US.
- He also estimates NSA has collected between 15-20 trillion transactions over the past 11 years.



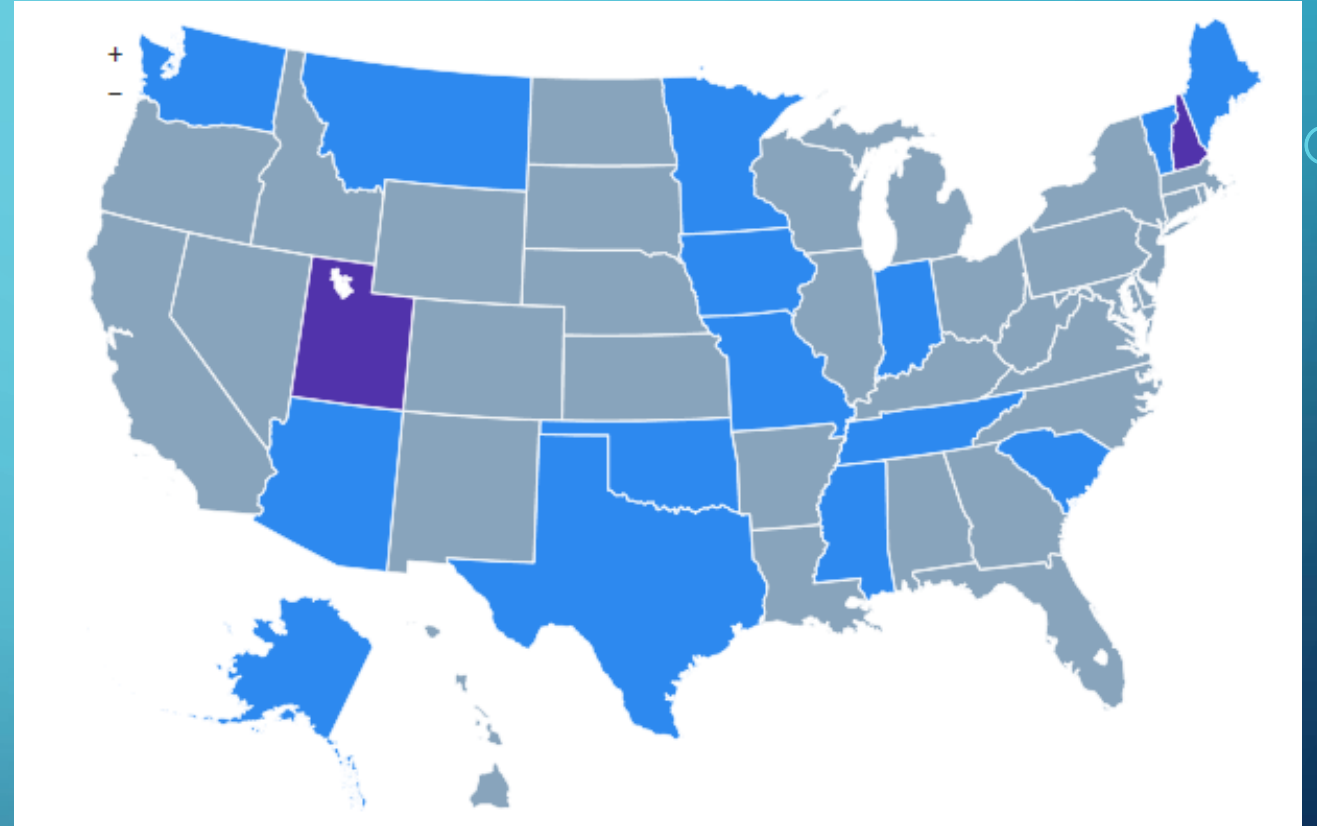
HOW DO WE KNOW THIS?

- The Guardian receives thousands of top secrets documents on American phone records and internet use that were leaked by an NSA employee
- In June of 2013 The Guardian begins to publish the documents revealing what information the NSA had been gathering



WHAT STATES ARE TAKING ACTION?

- The NSA sometimes relies on state and local government's resources to carry out their mass surveillance programs.
- 4th Amendment Protection Act bans all material support or resources to federal warrantless surveillance programs.
- Electronic Data Privacy Act prohibits states from obtaining data collected without a warrant



- Blue means legislation has been introduced in those states
- Purple means Electronic Data Privacy Law

WHAT DOES SB 13 DO?

- Section 1 provides that a home rule municipality may not adopt an ordinance inconsistent with the provisions of sec. 2 of the bill
- Section 2 prohibits a municipality or an agent of a municipality from cooperating with a federal data collection and surveillance agency in collecting electronic data without a search warrant or collecting telephone records without a warrant unless the collection is consistent with state law, and from using such records in a criminal investigation or prosecution
- Section 3 prohibits a state or municipal agency from using state or municipal assets to aid a federal data collection and surveillance agency in the collection of electronic data without a search warrant, or the collection of telephone records without a warrant unless the collection is consistent with state law

WHAT DOES SB 13 DO?

- Section 4 defines “electronic data” and “federal data collection and surveillance agency”
- Section 5 prohibits the state or an agent of the state from cooperating with a federal data collection and surveillance agency in collecting data without a search warrant, or collecting telephone records without a warrant unless the collection is consistent with state law, and from using such records in a criminal investigation or prosecution
- Section 6 provides that the bill has an immediate effective date



QUESTIONS?