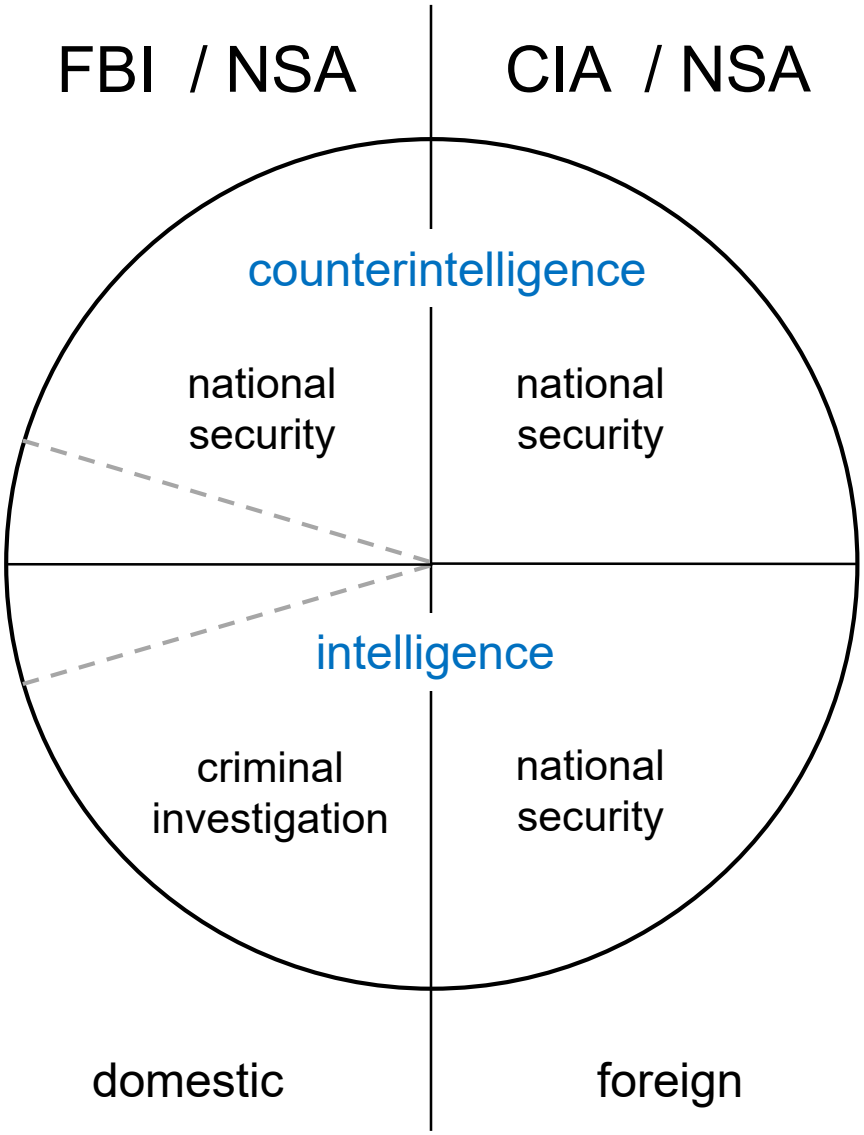
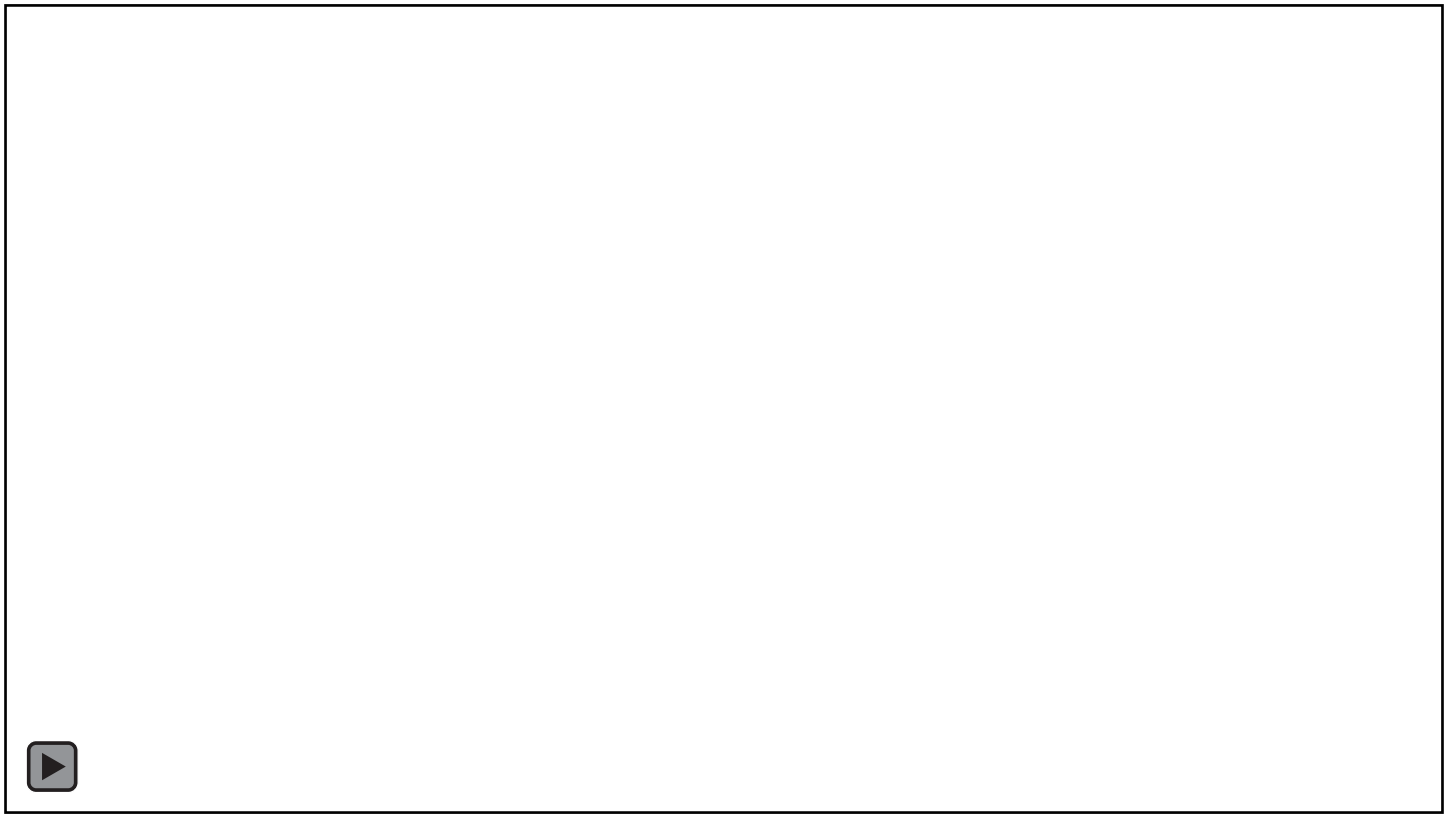
Scope of Surveillance



National Security and Privacy



Source: The Guardian

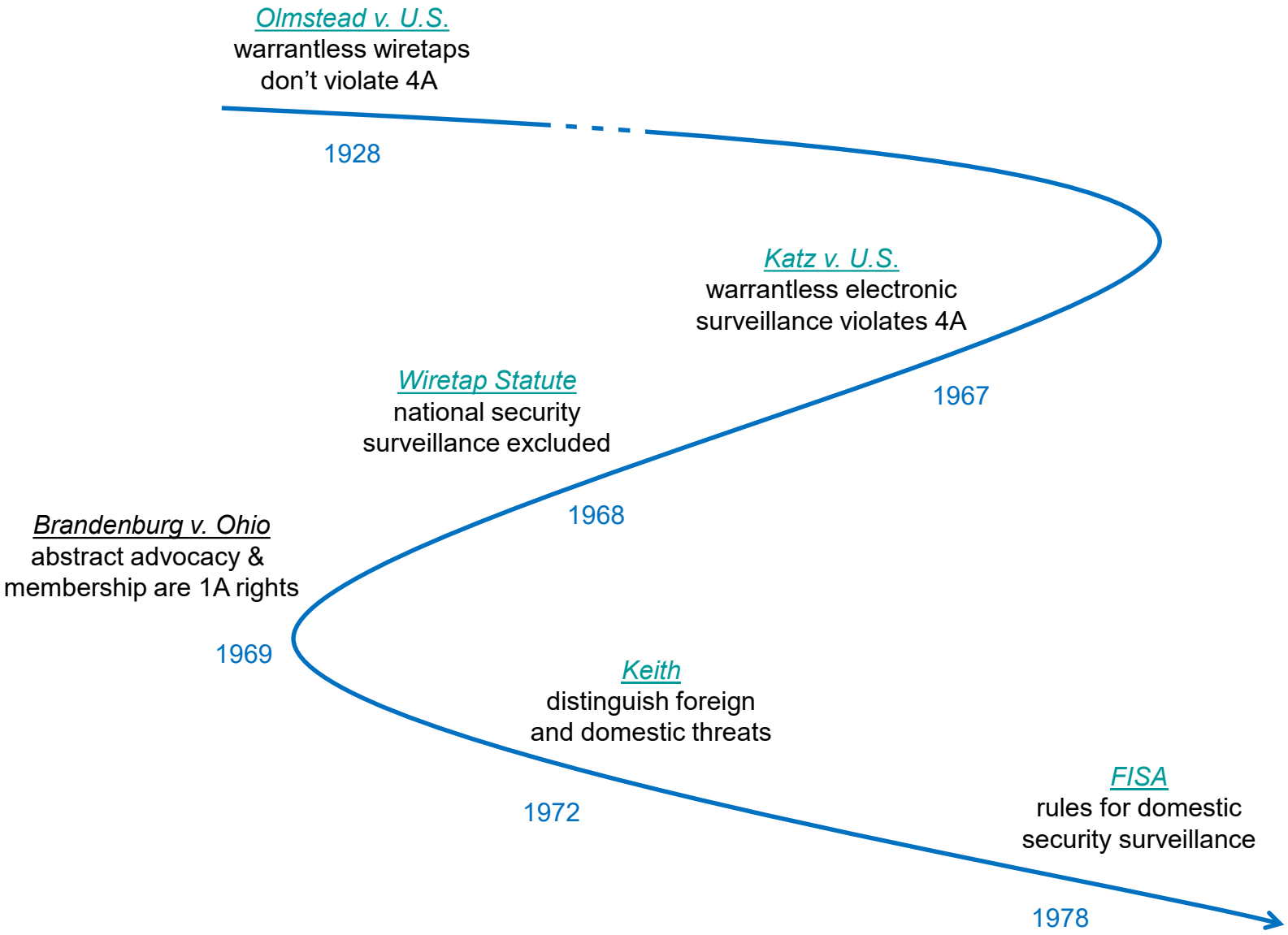
Constitutional Issues

First Amendment

Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press, or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.

Fourth Amendment

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.


Olmstead v. U.S.
warrantless wiretaps
don't violate 4A
1928
Katz v. U.S.
warrantless electronic
surveillance violates 4A
1967
Wiretap Statute
national security
surveillance excluded
1968
Brandenburg v. Ohio
abstract advocacy &
membership are 1A rights
1969
Keith
distinguish foreign
and domestic threats
1972
FISA
rules for domestic
security surveillance
1978

Olmstead v. United States (Supreme Court, 1928)

Majority (Taft)

> The amendment does not forbid what was done here. There was no searching. There was no seizure. The evidence was secured by the use of the sense of hearing and that only. There was no entry of the houses or offices of the defendants.

Dissent (Brandeis)

> The progress of science in furnishing the Government with means of espionage is not likely to stop with wire-tapping. Ways may someday be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home.

Katz v. United States (Supreme Court, 1967)

Majority (Harlan, concurring)

> [The majority holds] (a) that an enclosed telephone booth is an area where, like a home, and unlike a field, a person has a constitutionally protected reasonable expectation of privacy; (b) that electronic as well as physical intrusion into a place that is in this sense private may constitute a violation of the Fourth Amendment; and (c) that an invasion of a constitutionally protected area by federal authorities is, as the Court has long held, presumptively unreasonable in the absence of a search warrant.

Wiretap Statute, 1968

Nothing contained in this chapter… shall limit the constitutional power of the President to take such measures as he deems necessary to protect the Nation against actual or potential attack or other hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States, or to protect national security information against foreign intelligence activities.

Nor shall anything contained in this chapter be deemed to limit the constitutional power of the President to take such measures as he deems necessary to protect the United States against the overthrow of the Government by force or other unlawful means, or against any other clear and present danger to the structure or existence of the Government.

Keith case (Supreme Court, 1972)

Majority (Powell)

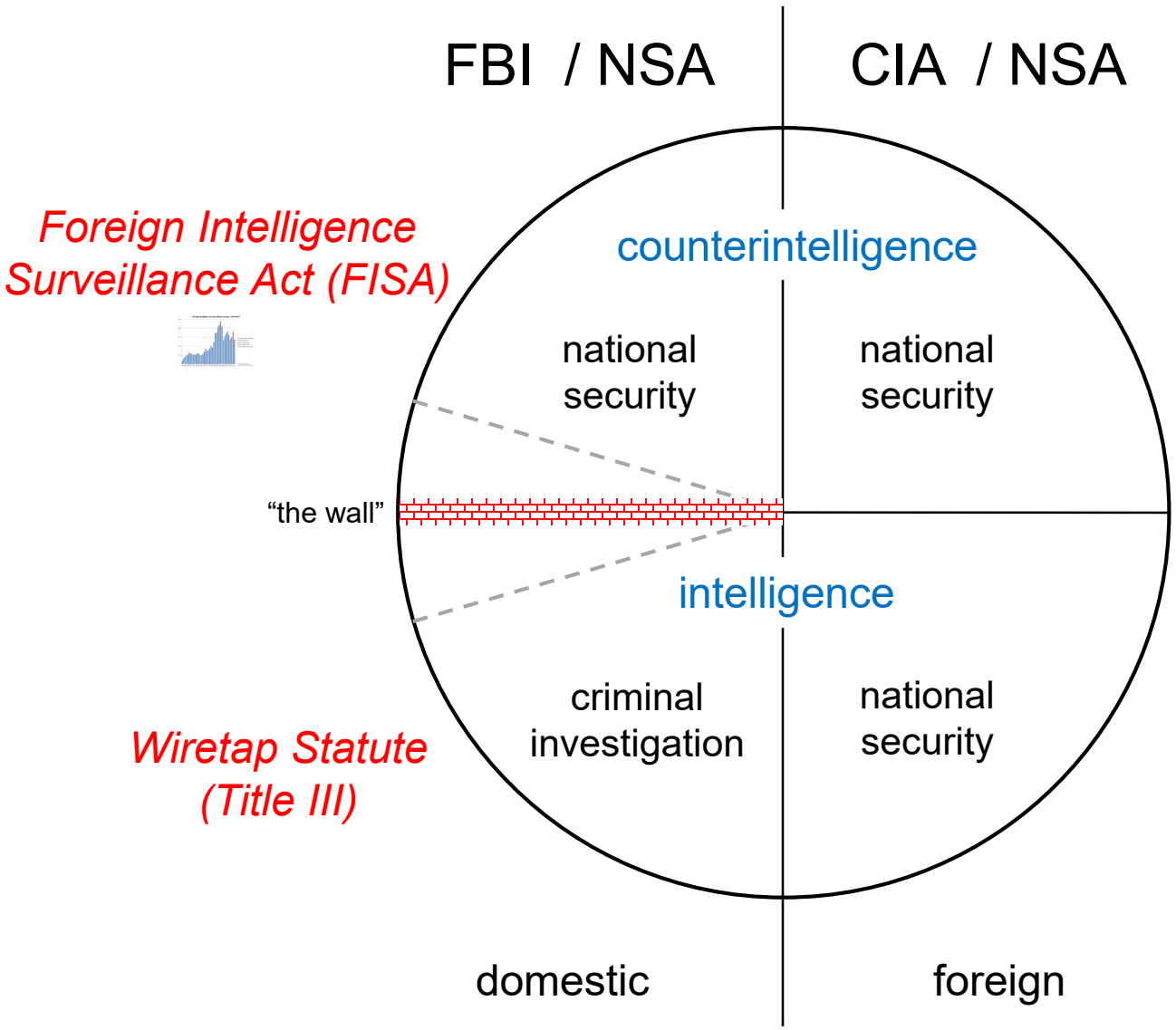
> The danger to political dissent is acute where the Government attempts to act under so vague a concept as the power to protect "domestic security." Given the difficulty of defining the domestic security interest, the danger of abuse in acting to protect that interest becomes apparent.

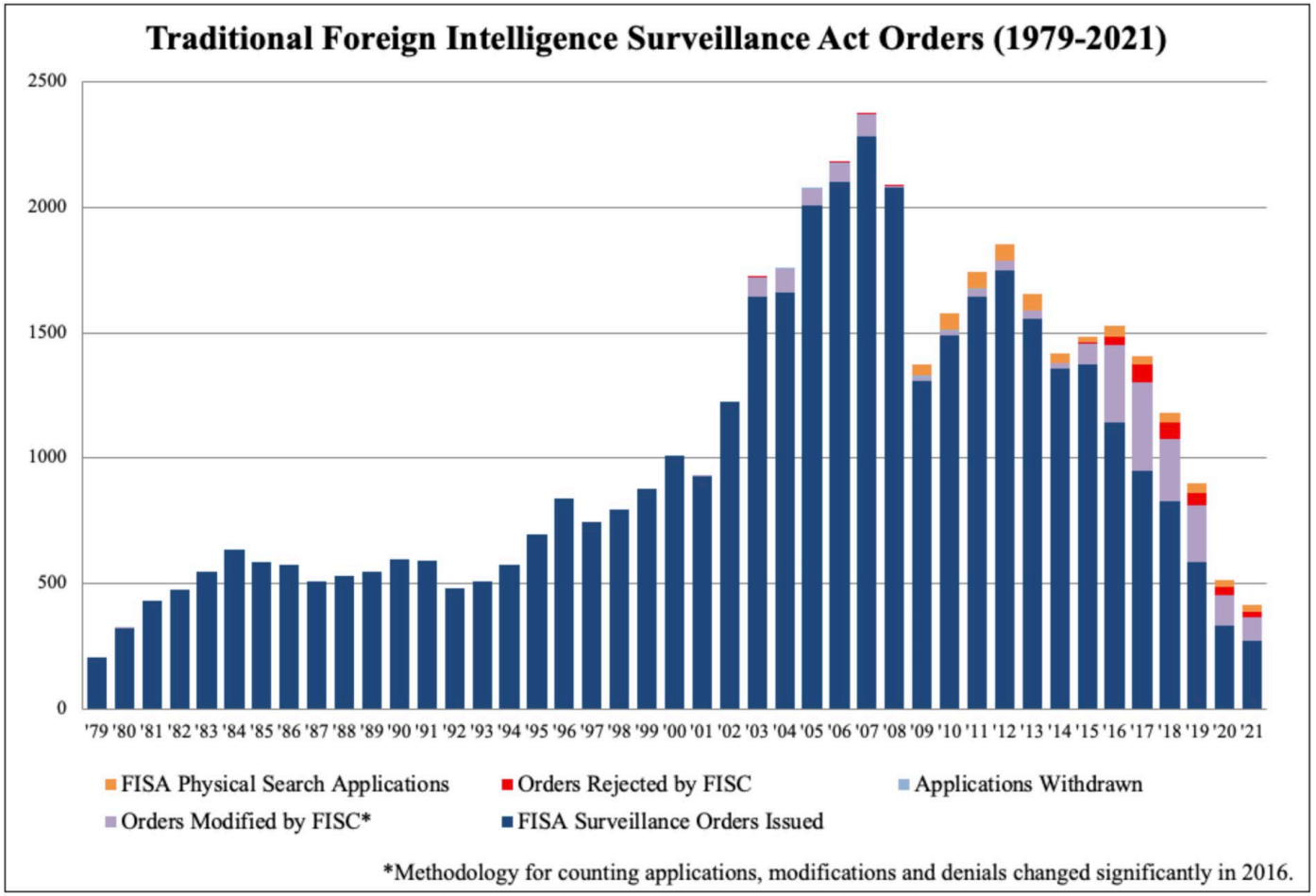
Foreign Intelligence Surveillance Act, 1978

Notwithstanding any other law, the President, through the Attorney General, may authorize electronic surveillance without a court order under this subchapter to acquire foreign intelligence information for periods of up to one year if the Attorney General certifies in writing under oath that:

A. the electronic surveillance is solely directed at
    i. the acquisition of the contents of communications transmitted by means of communications used exclusively between or among foreign powers, as defined in section 1801(a)(1), (2), or (3) of this title; or
    ii. the acquisition of technical intelligence, other than the spoken communications of individuals, from property or premises under the open and exclusive control of a foreign power, as defined in section 1801(a)(1), (2), or (3) of this title;
B. there is no substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is a party.

Scope of Surveillance




Traditional Foreign Intelligence Surveillance Act Orders (1979-2021)
2500
2000
1500
1000
500
0
'79 '80 '81 '82 '83 '84 '85 '86 '87 '88 '89 '90 '91 '92 '93 '94 '95 '96 '97 '98 '99 '00 '01 '02 '03 '04 '05 '06 '07 '08 '09 '10 '11 '12 '13 '14 '15 '16 '17 '18 '19 '20 '21
FISA Physical Search Applications
Orders Rejected by FISC
Applications Withdrawn
Orders Modified by FISC*
FISA Surveillance Orders Issued
*Methodology for counting applications, modifications and denials changed significantly in 2016.

Foreign Intelligence Surveillance Act, 1978 (cont.)

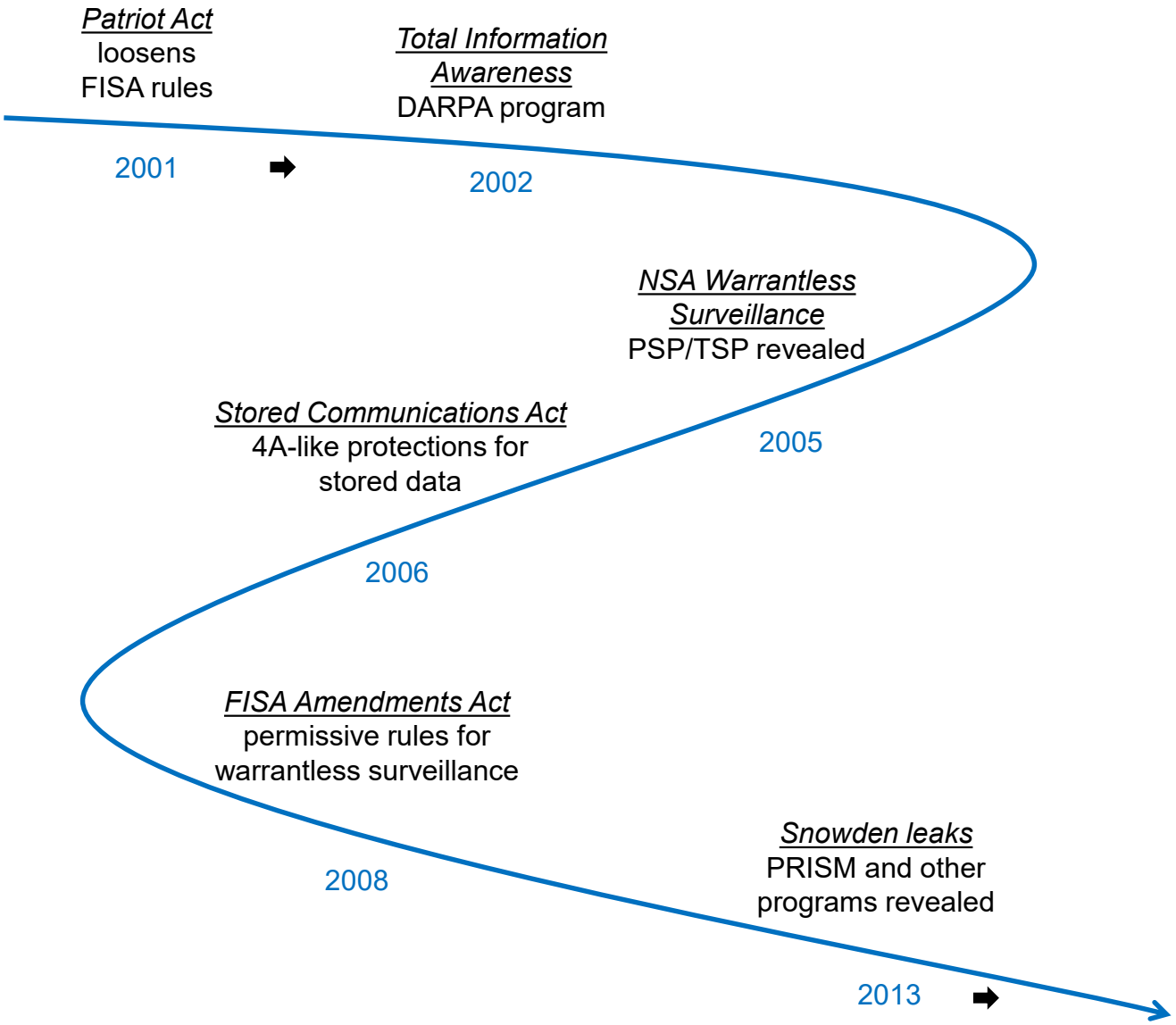
Upon an application made pursuant to section 1804 of this title, the judge shall enter an *ex parte* order as requested or as modified approving the electronic surveillance if he finds that

1. the application has been made by a Federal officer and approved by the Attorney General;

2. on the basis of the facts submitted by the applicant there is probable cause to believe that

    A. the target of the electronic surveillance is a foreign power or an agent of a foreign power: Provided, That no United States person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States; and

    B. each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power;


Patriot Act
loosens
FISA rules
2001
Total Information Awareness
DARPA program
2002
NSA Warrantless Surveillance
PSP/TSP revealed
2005
Stored Communications Act
4A-like protections for stored data
2006
FISA Amendments Act
permissive rules for warrantless surveillance
2008
Snowden leaks
PRISM and other programs revealed
2013

Sealed Case No. 02-001 (2002)

Foreign Intelligence Surveillance Court

> We find that these provisions…, particularly those which authorize criminal prosecutors to advise FBI intelligence officials on the initiation, operation, continuation or expansion of FISA's intrusive seizures, are designed to enhance the acquisition, retention and dissemination of *evidence for law enforcement purposes, instead* of being consistent with the need of the United States to "*obtain, produce, and disseminate foreign intelligence information*" (emphasis added)…. The 2002 procedures appear to be designed to amend the law and substitute the FISA for Title III electronic surveillances…. FISA's definition of minimization procedures has not changed, and these procedures cannot be used by the government to amend the Act in ways Congress has not.

In re Sealed Case No. 02-001 (2002)

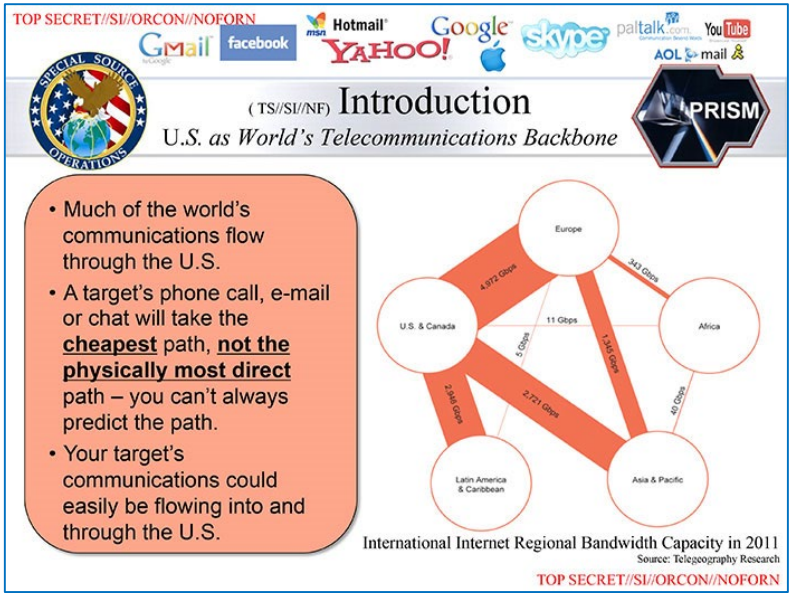
Foreign Intelligence Surveillance Court of Review

> Even without taking into account the President's inherent constitutional authority to conduct warrantless foreign intelligence surveillance, we think the procedures and government showings required under FISA, if they do not meet the minimum Fourth Amendment warrant standards, certainly come close. We, therefore, believe firmly, applying the balancing test drawn from *Keith*, that FISA as amended is constitutional because the surveillances it authorizes are reasonable.

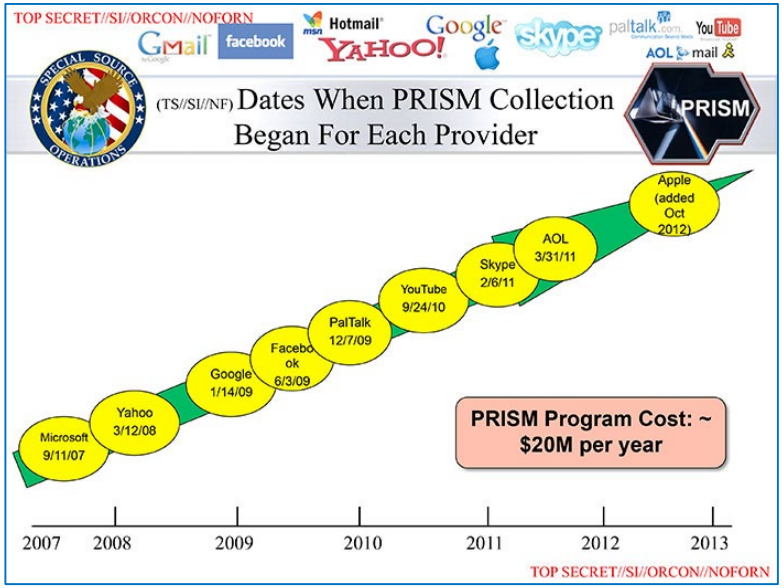
➡

PRISM

(Slides released by Edward Snowden)



Surveillance Concept



Provider Particpants

FISA, Section 702

DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC 20511

MAR 2 8 2014

The Honorable Ron Wyden
United States Senate
Washington, DC 20510

Dear Senator Wyden:

During the January 29, 2014, Worldwide Threat hearing, you cited declassified court documents from 2011 indicating that NSA sought and obtained the authority to query information collected under Section 702 of the Foreign Intelligence and Surveillance Act (FISA), using U.S. person identifiers, and asked whether any such queries had been conducted for the communications of specific Americans.

As reflected in the August 2013 Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702, which we declassified and released on August 21, 2013, there have been queries, using U.S. person identifiers, of communications lawfully acquired to obtain foreign intelligence by targeting non U.S. persons reasonably believed to be located outside the U.S. pursuant to Section 702 of FISA. These queries were performed pursuant to minimization procedures approved by the FISA Court as consistent with the statute and the Fourth Amendment. As you know, when Congress reauthorized Section 702, the proposal to restrict such queries was specifically raised and ultimately not adopted.

For further assistance, please do not hesitate to contact Deirdre M. Walsh in the Office of Legislative Affairs, at (703) 275-2474.

Sincerely,

James R. Clapper

➡

Mar-a-Lago Search and the Espionage Act

ATTACHMENT B

Property to be seized

All physical documents and records constituting evidence, contraband, fruits of crime, or other items illegally possessed in violation of 18 U.S.C. §§ 793, 2071, or 1519, including the following:

a. Any physical documents with classification markings, along with any containers/boxes (including any other contents) in which such documents are located, as well as any other containers/boxes that are collectively stored or found together with the aforementioned documents and containers/boxes;

b. Information, including communications in any form, regarding the retrieval, storage, or transmission of national defense information or classified material;

c. Any government and/or Presidential Records created between January 20, 2017, and January 20, 2021; or

d. Any evidence of the knowing alteration, destruction, or concealment of any government and/or Presidential Records, or of any documents with classification markings.