ЕВРОПЕЙСКИ ПАРЛАМЕНТ PARLAMENTO EUROPEO EVROPSKÝ PARLAMENT EUROPA-PARLAMENTET
EUROPÄISCHES PARLAMENT EUROOPA PARLAMENT ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ EUROPEAN PARLIAMENT
PARLEMENT EUROPÉEN PARLAIMINT NA hEORPA PARLAMENTO EUROPEO EIROPAS PARLAMENTS
EUROPOS PARLAMENTAS EURÓPAI PARLAMENT IL-PARLAMENT EWROPEW EUROPEES PARLEMENT
PARLAMENT EUROPEJSKI PARLAMENTO EUROPEU PARLAMENTUL EUROPEAN
EURÓPSKY PARLAMENT EVROPSKI PARLAMENT EUROOPAN PARLAMENTTI EUROPAPARLAMENTET

Committee on Civil Liberties, Justice and Home Affairs
- The Secretariat -

Background Note on

US Legal Instruments for Access and Electronic Surveillance of EU Citizens

Introduction

This note presents a general description of US legal provisions that would arguably be used for the access of and targeting of electronic communications of EU citizens: namely Section 702 of US Foreign Intelligence Surveillance Act (FISA); Section 215 of the USA Patriot Act, Executive Order 1233 and Electronic Communications Privacy Act (ECPA).

The legal instruments on surveillance of electronic communications in place in the Member States will be be the object of another document that will be presented at a later stage.

The US Patriot Act 2001

1. Following the attacks on the World Trade Center in September of 2001, Congress enacted the USA PATRIOT Act of 2001 (Patriot Act)1. The Patriot Act modified portions of numerous electronic communications laws, including the Electronic Communications Privacy Act (ECPA) and Foreign Intelligence Surveillance Act (FISA), expanding the authority of federal law enforcement authorities to combat terrorism. The Act expands federal agencies' powers in intercepting, sharing, and using private telecommunications, especially electronic communications, along with a focus on criminal investigations by updating the rules that govern computer crime investigations.

2. Sections 201-216 refer to interception of communications. It seems that they would be the legal basis for the collection of domestic (US) communication data, namely Section 215. Section 215, amended FISA to allow the FBI to apply for an order that compel any person or entity to turn over "*any tangible* things," so long as the FBI "specifies "*that the order is "for an authorized investigation . . . to protect against international terrorism or clandestine intelligence activities.*"

3. **Section 215** expands the FBI's power to spy on ordinary people living in the United States, including United States citizens and permanent residents. The FBI need not show probable

[1] http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf

cause, nor even reasonable grounds to believe, that the person whose records it seeks is engaged in criminal activity. The FBI need not have any suspicion that the subject of the investigation is a foreign power or agent of a foreign power. Those persons or organisations served with Section 215 orders are prohibited from disclosing the fact to anyone else. Those who are the subjects of the surveillance are never notified that their privacy has been compromised. If the government had been keeping track of what books a person had been reading, or what web sites she had been visiting, the person would never know.

4. Section 206 of the Patriot Act, also known as "roving John Doe wiretap" provision, permits the government to obtain intelligence surveillance orders that identify neither the person nor the facility to be tapped. This provision is contrary to traditional notions of search and seizure, which require government to state with particularity what it seeks to search or seize.

The US Foreign Intelligence Surveillance Act (FISA) 1978

5. FISA provides a statutory framework by which government agencies may, when gathering foreign intelligence information, obtain authorisation to conduct wiretapping or physical searches. It was adopted in 1978 and repeatedly amended, namely by the US Patriot Act and more recently in 2008 and 2012.

6. Following the disclosure by the New York Times in 2005 of the National Security Agency's 'warrantless wiretapping' activities conducted in violation of constitutional and statutory protections afforded to US citizens and legal residents, the US Congress enacted in 2007 the Protect America Act. The Act provided retroactive immunity to the telecommunications companies involved and allowed wiretapping to continue without individual warrants, conditional upon the approval of NSA procedures by the secret Foreign Intelligence Surveillance Court (FISC).

7. A subsequent test case at the Foreign Intelligence Surveillance Court of Review (tasked with reviewing FISC decisions to deny applications for electronic surveillance warrants) confirmed that the Fourth Amendment of the US Constitution which requires any warrant for surveillance operations to be judicially sanctioned and supported by probable cause, only applied to surveillance directed at US persons. In other terms, non-US citizens or legally resident are not protected by the Fourth Amendment and other US statutory safeguards.[2]

8. After this decision the US Congress enacted **FISAA (FISA Amendments Act of 2008) in 2008, to amend FISA, adopted in 1978. New Section 702 (50 U.S.C. § 1881a)** authorises the mass surveillance of non-US foreigners outside US territory but whose data are in the range of US jurisdiction. FISA extends the scope of surveillance beyond interception of communications, to include any data in public cloud computing as well. This change occurred

[2] Later on the US Supreme Court in February 2013 (Clapper v. Amnesty International***)*** **ruled that US organisations and civil liberties groups lack standing to challenge the constitutionality of 1881a of FISAA.**

merely by incorporating "*remote computing services*" into the definition of an "electronic communication service provider".

9. After the modifications of FISA, Section 702 empowers the Attorney General (AG) and the Director of National Intelligence ("DNI") to authorize, for up to one year, the acquisition of communications concerning "*persons reasonably believed to be outside the United States*" by means of an order issued by the FISA Court on the basis of a certification by the Attorney General and the DNI that must be certified in writing, under oath, and supported by appropriate affidavit(s). The certification is not required to identify the individuals at whom such acquisitions would be directed, but must attest, in part, that targeting procedures are in place that have been approved, have been submitted for approval, or will be submitted with the certification for approval by the FISA Court. In order words, **Section 702 does not require an individualized court order.** The applicable targeting and minimization procedures are subject to judicial review by the FISA Court[3].

10. Generally, if the certification and targeting and minimization procedures meet the statutory requirements and are consistent with the Fourth Amendment, a FISC order approving them will be issued prior to implementation of the acquisition of the communications at issue

11. However, in "*exigent circumstances*", the AG and DNI may also authorise the targeting of **persons reasonable believed to be outside the US, without a FISC order when they determine that intelligence important to the national security of the US may be lost or not timely acquired.** A "certification supporting such "determination" shall be submitted to the FISC as soon as practicable but not later than days after the determination was made (FISAAA Section 702, subsection (c)(2)).

12. If a provider fails to comply with the order (directive), the US Attorney General may seek an order from the FISA Court compelling compliance with the directive. Failure to obey an order of the FISA Court may be punished as a contempt of court. A person receiving a directive may challenge the legality of that directive by filing a petition with the FISA Court. Determinations of the FISA Court may be appealed to the Foreign Intelligence Court of Appeals.

13. FISAAA prohibits the party that receives a FISA Order from disclosing that fact. This typically would prevent a cloud service provider or a communication or on line services provider from informing its customers that the service provider had shared their data with a law enforcement agency in response to a FISA Order. The Act provides explicit immunity from civil suit in any federal or state court for providing any information, facilities, or assistance in accordance with a directive under the Act.

14. The powers granted by FISAAA to NSA expired in December 2012. The US Senate agreed on 28 December 2012 to extend them for a new period of five years ending December 2017 (*Public Law 112-238*).

---

[3] Congressional Research Service. Reauthorization of the FISA Amendments Act/ April 8, 2013: "the court is not required to look behind the assertions made in the certification".

The Electronic Communications Privacy Act (ECPA) 1986

15. This instrument covers: (1) the interception of wire, oral, or electronic communications (wiretapping) (2) access to the content of stored electronic communications and to communications transaction records and (3) the use of trap and trace devices and pen registers. Court authorisation is required for such activities. It covers basically law enforcement investigations. Does not cover international or foreign communications. ECPA has been amended several times, particularly by the Patriot Act and the FISA Amendments 2008 (FISAA).

16. Surveillance activities for foreign intelligence purposes might fall within the scope of ECPA, but if the activity falls within the definition of electronic surveillance under FISA, then it may be conducted under FISA procedures. If it is not electronic surveillance as defined in FISA, but involves the acquisition of foreign intelligence information from international or foreign communications, then it is not subject to ECPA. For example, the interception of an international telephone call would not be considered electronic surveillance for purposes of FISA if the target were the person on the non-domestic end of the conversation and the acquisition would not occur on United States soil. Using the procedures under FISA is compulsory for those activities that qualify as electronic surveillance but are exempt from ECPA. Prior to the FISA Amendments Act, FISA's procedures were generally never needed for wiretapping activities that did not qualify as electronic surveillance, and which were also exempt from ECPA because they involved international or foreign communications. However, the recently added § 704 of FISA does make FISA's procedures compulsory when the target of such surveillance is a United States person.

Executive Order 12333 United States Intelligence Activities

17. This Instrument was adopted on 4 December 19814. It intends to extend powers and responsibilities of US intelligence agencies and direct the U.S. federal agencies to co-operate fully with CIA requests for information. It was lately amended by in 2008, to strengthen the role of the DNI.

18. It seems to cover collection of information within the United States or directed against United States persons abroad, relating to foreign powers, organisations or persons and theirs agents5. Agencies are not authorized to use such techniques as electronic surveillance, unconsented physical search, mail surveillance, physical surveillance, or monitoring devices unless they are in accordance with procedures established by the head of the agency concerned and approved by the Attorney General. If a warrant would be required for law enforcement purposes, the executive order requires the Attorney General to determine in each case that there is probable cause to believe that the technique is directed against a foreign power or an agent of a foreign

[4] http://www.archives.gov/federal-register/codification/executive-order/12333.html

[5] Under specific conditions and circumstances, US intelligence agencies could also collect, retain or disseminate information concerning US persons. (Section 2.3)

power. The authority delegated by Executive Order 12333 must be exercised in accordance with in accordance with FISA, but also extends to activities beyond FISA's reach (electronic surveillance).

The Intelligence Reform and Terrorism Prevention Act 2004

19. Section 6001 of the Intelligence Reform and Terrorism Prevention Act of 2004, or the so-called "Lone Wolf" provision, permits secret intelligence surveillance of non-US persons who are not affiliated with a foreign organization. Such an authorization is granted only in secret courts. This provision would have never been used and should be allowed to expire outright.