

刘涛◎译

Foreign Intelligence Surveillance Act of 1978 &
Foreign Intelligence Surveillance Court Rules of Procedure

美国涉外情报报监控法及 涉外情报报监控法院诉讼规则



中国人民公安大学出版社



美国涉外情报监控法及 涉外情报监控法院诉讼规则

刘 涛 译

中国人民公安大学出版社

· 北 京 ·

图书在版编目 (CIP) 数据

美国涉外情报监控法及涉外情报监控法院诉讼规则/刘涛译. —
北京: 中国人民公安大学出版社, 2011. 5

ISBN 978 - 7 - 5653 - 0440 - 8

I. ①美… II. ①刘… III. ①情报工作—法律—研究—美国
IV. ①D971. 221

中国版本图书馆 CIP 数据核字 (2011) 第 092644 号

美国涉外情报监控法及涉外情报监控法院诉讼规则

刘 涛 译

出版发行: 中国人民公安大学出版社

地 址: 北京市西城区木樨地南里

邮政编码: 100038

经 销: 新华书店

印 刷: 北京蓝空印刷厂

版 次: 2011 年 5 月第 1 版

印 次: 2011 年 5 月第 1 次

印 张: 5. 375

开 本: 880 毫米 × 1230 毫米 1/32

字 数: 141 千字

书 号: ISBN 978 - 7 - 5653 - 0440 - 8

定 价: 20. 00 元

网 址: www.cppsups.com.cn www.porclub.com.cn

电子邮箱: zbs@cppsup.com zbs@cppsu.edu.cn

营销中心电话: 010 - 83903254

读者服务部电话 (门市): 010 - 83903257

警官读者俱乐部电话 (网购、邮购): 010 - 83903253

法律图书分社电话: 010 - 83905745

本社图书出现印装质量问题, 由本社负责退换
版权所有 侵权必究

目 录

涉外情报监控法及涉外情报监控法院诉讼规则简介	1
涉外情报监控法	32
第一章 电子监控	32
第 1801 节 含义界定	32
第 1802 节 无法院授权命令的电子监控；司法部部长的 证明文件；向国会相关委员会提交报告； 加盖公章移送；公用电信营运商的职责和 补偿；申请书；法院的司法管辖权	39
第 1803 节 法官的选任	41
第 1804 节 向法院申请获得命令	45
第 1805 节 法院命令的签发	48
第 1805a 节至第 1805c 节 废除	55
第 1806 节 电子监控所得信息的使用要求	55
第 1807 节 向美国法院的行政管理办公室和国会 提交报告	59
第 1808 节 司法部部长向国会相关委员会提交报告；国会 相关委员会情报收集活动的职权或责任范围； 国会相关委员会向国会提交报告	60
第 1809 节 刑事制裁	61
第 1810 节 民事责任	62
第 1811 节 战争期间的授权	63

第 1812 节	对某些通信进行电子监控和窃听所使用的专用手段的说明	63
第二章	物理性搜查	64
第 1821 节	含义界定	64
第 1822 节	为获取涉外情报，物理性搜查的批准与授权	65
第 1823 节	申请获得法院的授权命令	68
第 1824 节	法院命令的签发	72
第 1825 节	物理性搜查所得信息的使用要求	76
第 1826 节	国会审查	80
第 1827 节	刑罚	81
第 1828 节	民事责任	82
第 1829 节	战争期间的授权	82
第三章	为获取涉外情报信息，安装和使用通信记录与通信追踪装置	83
第 1841 节	含义界定	83
第 1842 节	为获取涉外情报和调查国际恐怖主义活动，安装、使用通信记录器和通信追踪装置	84
第 1843 节	紧急情况下的授权	89
第 1844 节	战争期间的授权	90
第 1845 节	信息的使用要求	91
第 1846 节	国会监督	94
第四章	为获取涉外情报而使用某些商务记录	96
第 1861 节	为获取涉外情报和调查国际恐怖主义活动而使用某些商务记录	96
第 1862 节	国会监督	103
第 1863 节	废除	104

第五章 报告要求	105
第 1871 节 司法部部长的半年度报告	105
第六章 关于针对某些位于美国境外的人实施情报收集的 额外程序	108
第 1881 节 含义界定	108
第 1881a 节 针对某些位于美国境外的非美国人 收集情报的程序	110
第 1881b 节 在美国境内针对位于美国境外的美国人实 施某些情报收集行动	126
第 1881c 节 针对位于美国境外的美国人的 其他情报收集行动	135
第 1881d 节 联合申请与合并授权	141
第 1881e 节 依据本章之规定获得的信息的使用	142
第 1881f 节 国会审查	142
第 1881g 节 保留条款	144
第七章 对向政府提供协助的人的保护	145
第 1885 节 含义界定	145
第 1885a 节 实施法律规定辩护的程序	147
第 1885b 节 联邦法优先适用	150
第 1885c 节 报告	150
涉外情报监控法院诉讼规则	152
I. 规则的适用范围、参照适用及修改要求	152
II. 国家安全信息	152
III. 法院的组成和法官的职权	153
IV. 律师在本院出庭的授权	154
V. 书记官办公室	154
VI. 向法院提出申请的形式和方式	155
VII. 听审	157

VIII. 法院命令	158
IX. 相关资料的扣押或销毁	160
X. 上诉	161
附一：涉外情报监控法院法官名单	162
附二：涉外情报监控复审法院法官名单	163

涉外情报监控法及涉外情报 监控法院诉讼规则简介

一、立法简况

美国联邦宪法第四修正案（1791年）规定：“人民的人身、住宅、文件和财产有不受不合理搜查、扣押和拘捕的权利，不得侵犯。除依照合理根据，以宣誓或代誓宣言保证，并具体说明搜查的地点和扣押的人或物，不得发出搜查、扣押和拘捕令状。”这一修正案对公民的人身、住宅、文件、财产进行了保护，其实质要件为不受不合理的搜查、扣押和拘捕，形式要件是必须存在合理根据、要有宣誓或代誓宣言的保证，并且由独立的法院签发授权令状，令状中应当特别具体、详细地载明将要被搜查、扣押或拘捕的对象。但是，从文本上看，这一修正案的保护对象仅为人身、住宅、文件和财产，并没有明确提及对电话通信的保护。因为，这一修正案的通过时间是1791年，而电话通信的出现则是在1876年亚历山大·格雷厄姆·贝尔取得电话发明专利权之后。因此，电话通信是否受到美国联邦宪法的保护需要联邦最高法院通过判例确认。

一、1978年《涉外情报监控法》通过之前

在1928年的 *Olmstead v. United States* 一案^①中，美国联邦最高法院对联邦执法人员秘密窃听（wiretap）行为的合法性进行了激烈讨论，最后以5:4的表决结果通过了判决。首席大法官 Taft 主笔

^① 277 U. S. 438 (1928)。

撰写的判决意见认为，联邦执法人员的窃听行为不受联邦宪法第四修正案关于搜查和扣押的正当程序要求的约束，理由是第四修正案没有禁止该案中警察的行为，因为警察获取证据的方式是“听”，警察并未进入被告人的住宅，没有进行搜查，也没有物品被扣押，他认为国会应当通过单独的立法来保障公民个人通信的隐私权利，但是就该案而言，警察的行为并没有构成违反联邦宪法第四修正案，第四修正案所保护的客体只适用于有形财产。

1934年，美国国会通过了《联邦通信法》（Communications Act of 1934），这是第一部对美国国内州际通信和涉外通信活动进行规范和管理的联邦法律，其中也对窃听行为进行了首次规范。该法第705节（《美国法典》第47编第605节（47 U.S.C. 605））规定：“未经通信的发送者授权，任何人不得对通信进行窃听，不得将被窃听的通信的存在、内容、实质、主旨、结果或意义向任何人泄露或者公布。”在1937年的 *Nardone v. United States* 一案^①中，联邦最高法院依据《联邦通信法》的规定判定，联邦执法人员通过窃听或截听^②通信信息获得的证据在联邦地区法院的刑事审判中不具有可采性。在1939年，*Nardone v. United States* 一案中的另一个问题也得到解决，即被告人的辩护律师是否可以质疑控方使用了窃听所获得的信息，联邦最高法院最后裁定，法庭必须给被告方机会用以质疑控方的证据属于毒树之果。

进入20世纪60年代以后，厄尔·沃伦（Earl Warren）首席大法官领导的美国联邦最高法院推动了一场“正当程序革命”，联邦最高法院对窃听取证的态度发生了相应变化：允许窃听但受到严格

^① 1937. SCT. 1233, 302 U.S. 379, 58 S. Ct. 275, 82 L. Ed. 314 (1937).

^② 就技术角度而言，窃听（wiretap）与截听（intercept）的含义应当有所不同，目前国内学界所使用的术语也不尽一致，如窃听、截听、监听、侦听等，本书中没有明确区分。

限制。在 1967 年的 *Berger v. New York* 一案^①中，联邦最高法院认定，交谈属于联邦宪法第四修正案的保护范围，通过电子装置窃取交谈内容属于联邦宪法第四修正案中所规定的搜查和扣押，并提出了关于实施窃听的指导性意见：必须存在合理根据使人相信某一特定的犯罪已经或者正在实施；被窃听的交谈必须在令状中专门载明；窃听必须在特定、有限制的时间内进行；如果授权窃听的令状需要更新或延期，赖以签发授权令状的合理根据必须持续存在；一旦通话内容已经获得，窃听必须立即停止；窃听后必须告知，除非确实存在紧急情况；必须向法院提交关于授权令状执行情况的回执，以便法院能够进行监督和限制窃听所得资料的使用。在 1967 年的另一起案件即 *Katz v. United States* 一案^②中，联邦最高法院进一步扩展了联邦宪法第四修正案的适用范围，将不合理的搜查和扣押扩展适用到禁止在无法院令状授权的情况下对个人在公用电话亭的通话进行窃听，并进一步明确了关于窃听的指导性意见：宪法第四修正案保护的是个人的隐私权，将联邦宪法第四修正案的保护范围从有形物品扩展到了私人之间的交谈。

作为对上述两起案例的部分回应，1968 年美国国会通过了《综合犯罪控制与街道安全法》（*Omnibus Crime Control and Safe Street Act of 1968*），其中第三部分又称为“窃听与电子监控法”[*TITLE III - WIRETAPPING AND ELECTRONIC SURVEILLANCE*，在《美国法典》中的位置是第 18 编第 119 章第 2510 节至第 2522 节（18 USC 2510—18 USC 2522）]，该法是 1934 年《联邦通信法》之后关于窃听的又一部重要法律，澄清了关于进行窃听和电子监控的相关规定。该法明确规定：为了保护清白无辜的人的隐私，在未经通信任何一方当事人同意的情况下，窃听只能在拥有适格司法管辖权的法官授权批准，并且受到授权法官的监督和控制在情况下才

① 388 U. S. 41, 87. S. Ct. 1873, 18 L. Ed. 2d 1040 (1967).

② 389 U. S. 347, 88. S. Ct. 507, 19 L. Ed. 2d 576 (1967).

能实施。同时，为了捍卫美国的国家安全，该法赋予了总统额外的特殊权力，该法规定：美国总统有权采取他认为必要的措施以防范美国可能遭到的外国势力实施的、现实的或者潜在的或者其他的敌对活动，有权收集他认为与美国的国家安全相关的必要的外国情报信息，或者采取措施防范国家安全情报信息被外国情报活动收集；美国总统有权采取他认为必要的措施保护美国，阻止通过暴力或其他不合法的方式推翻政府，或者阻止其他意图明显且具有现实威胁的推翻现行政府组织或实体的行为。

1972年出现了关于窃听的具有里程碑式意义的案例：United States v. U. S. District Court,^① 也称为“Keith case”，在该案的判决中，联邦最高法院的大法官们以9:0的一致投票结果支持了以前案例中的裁决意见，认为：未经授权的窃听是对联邦宪法第四修正案的违反，窃听所得信息应当向被告方披露；如果针对国内的目标进行监控必须遵循联邦宪法第四修正案所要求的条件。

二、1978年《涉外情报监控法》的制定及之后的主要修改

（一）1978年《涉外情报监控法》的制定

1978年《涉外情报监控法》的立法背景是：尼克松总统“水门丑闻”事件曝光后从水门丑闻事件中的全面反思，尤其是针对总统容易滥用1968年《综合犯罪控制与街道安全法》中赋予的特殊权力，国会通过了《涉外情报监控法》（Foreign Intelligence Surveillance Act of 1978, FISA）。严格限制了情报机构对涉及美国公民以及在美国长期居住的居民的通信进行截听的权力。对于通信一方当事人是美国人时，要求司法部部长向特别组建的涉外情报监控法院（FISC）申请获得进行监控的授权命令。当然，FISA也规定了一些例外情形，为情报机构获取情报提供了相当大的回旋余地（leeway）：如在战争期间，总统可以实施为期15天的无法院授权命令的窃听；发生危机时，可以先进行窃听，有溯及力的授权窃听

^① 407 U. S. 297 (1972).

命令能够事后获得。

这一时期的重要判例是1979年的Smith v. Maryland一案,^①在该案中,在未取得法院授权令状的情况下,警察通过安装通信记录器(pen register)记录了从嫌疑人住宅拨出的电话号码,最后法院裁定,个人并不拥有将所拨打的电话号码视为其隐私的合理预期。

但1986年国会通过的《电子通信隐私法》(Electronic Communications Privacy Act of 1986, ECPA)对其作了修改,将其视为公民个人隐私权的一部分予以保护,具体内容规定在《电子通信隐私法》的第三部分“通信记录器和通信追踪装置”[TITLE III—PEN REGISTERS AND TRAP AND TRACE DEVICES,在《美国法典》中的位置是第18编第二部分第206章第3121节至第3127节(18 USC 3121—18 USC 3127)],这部分规定了对于拨打信号和输入信号的保护,对于安装和使用通信记录器与通信追踪装置进行了限制。

1986年《电子通信隐私法》除了上述修改之外,对于1968年《综合犯罪控制与街道安全法》中的窃听制度进行了重大修改,主要体现在:(1)《电子通信隐私法》的第一部分“对通信进行截听及相关事项”[TITLE I—INTERCEPTION OF COMMUNICATIONS AND RELATED MATTERS,在《美国法典》中的位置是第18编第119章第2510节至第2522节(18 USC 2510—18 USC 2522)],根据通信技术的进步和发展,将电子通信纳入了该法的保护范围,同时也扩展了窃听的适用对象,使窃听对象除了原来的有线和口头通信外,还包括电子通信;(2)《电子通信隐私法》的第二部分“使用存储的有线和电子通信业务记录”[TITLE II—STORED WIRE AND ELECTRONIC COMMUNICATIONS TRANSACTIONAL RECORDS ACCESS,在《美国法典》中的位置是第18编第121章第2701节至第2712节(18 USC 2701—18 USC 2712)],规定了对于存储的

^① 442 U. S. 735 (1979).

有线和电子通信信息的保护，同时也授权在一定情况下执法部门可以调取和使用存储的电子通信信息。截取存储的电子通信信息不同于一般的窃听，一般的窃听是与窃听对象的通信活动同步或同时进行的，但截取存储的电子通信信息则是在通信结束后在通信中转服务器中截取。

（二）2001年《爱国者法》对《涉外情报监控法》的修改

2001年“9·11”恐怖主义袭击事件发生以后，为有效预防和打击恐怖主义犯罪活动，美国国会迅速通过了2001年《爱国者法》（USA PATRIOT ACT OF 2001），《爱国者法》大幅度扩充了执法机构在美国境内和美国境外的执法权力。例如，扩充了执法机构搜查电话、电邮通信以及使用医疗、金融和其他记录的权力；取消了在美国境内获取外国情报的限制；扩展了财政部长管理金融交易的权力，尤其是针对外国人和外国实体的金融交易；扩展了执法与移民机构对涉嫌从事恐怖主义活动的人的扣留和驱逐的权力；扩展了对恐怖主义的界定，将国际恐怖主义活动扩展到国内恐怖主义，等等。其中，《爱国者法》的第二部分“加强监控措施”（TITLE II—ENHANCED SURVEILLANCE PROCEDURES）针对《涉外情报监控法》进行了诸多重要修改。例如，第206节扩展了涉外情报监控法中规定的“任意监控”（Roving Surveillance）职权；第207节扩展了依据涉外情报监控法针对非美国人的外国势力代理人的监控期限，包括电子监控和物理性搜查的实施期限；第208节扩大了选任涉外情报监控法院法官的范围并增加了涉外情报监控法院法官的数量；第214节扩展了依据涉外情报监控法使用通信记录器和通信追踪装置的职权；第215节对涉外情报监控法第四部分进行了全面修改，确立了为调查涉外情报和国际恐怖主义活动而使用某些商务记录，即“215调查命令”；第225节加强了对执行和协助涉外情报监控法相关命令和要求的执法人员、电子通信服务营运商、房东、保管人等个人的保护，执法人员的执法行为以及相关单位和个人对执法的协助行为免于承担民事责任，等等。

《2005年爱国者法修正与再授权法》(USA PATRIOT Improvement and Reauthorization Act of 2005, H. R. 3199)和《2006年爱国者法额外授权增补法》(the USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006, S. 2771)对《爱国者法》中的一些条款进行了适当的修正并对其中大多数临时性授权条款予以重新授权,使其永久化。

(三) 2007年《保护美国法》对《涉外情报监控法》的修改

《爱国者法》出台以后,政府权力得到空前扩张,在爱国者法的实施过程中,围绕爱国者法的争论也日趋尖锐,争论的核心是政府权力与公民权利保护之间的冲突和平衡,因为《爱国者法》赋予的政府在反恐行动中的权力,容易被政府以反恐为借口,假借法律规定之名滥用,进而侵犯公民个人享有的受联邦宪法保护的各项权利,尤其是言论自由权、隐私权和财产权利。例如,2007年在俄勒冈联邦地区法院审理的Mayfield v. United States一案^①中,被告方认为《爱国者法》赋予了FBI广泛的权力,并在具体案件中滥用,在审判时,联邦地区法官Ann Aiken裁定爱国者法违反宪法。

2007年《保护美国法》(Protect America Act of 2007)得到了参众两院中民主党和共和党的共同支持,其目的是使《涉外情报监控法》恢复到其当初的立法宗旨:保护美国公民的宪法权利,同时又力图使该法不会阻碍执法部门针对位于海外的外国目标获取涉外情报信息。该法主要从四个方面对涉外情报监控法进行了修改:(1)对位于外国领土上的目标,允许美国的情报专家更为有效地在没有事先获得法院授权的情况下收集其情报信息;(2)对于情报机构使用的用以确定监控活动针对的是位于海外的目标的规则和程序,涉外情报监控法院充当审查者的角色;(3)赋予了涉外情报监控法院可以要求第三方当事人为情报机构的情报收集活动

^① 504 F Supp. 2d 1023.

提供帮助的权力；（4）如果第三方当事人按照法院命令的要求向政府情报机构的情报收集活动提供了帮助，免于向权益受损人承担诉讼责任。

（四）《2008年FISA增补法》对《涉外情报监控法》的修改

作为国会审查和总统扩权需要之间妥协的结果，2008年7月10日，国会通过了《2008年涉外情报监控法增补法》（“Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008”或者“The FISA Amendments Act of 2008”），该法对涉外情报监控法中的一些内容进行了修改和调整，力图通过程序的优化设置实现政府情报收集活动的有效性与国会、法院对其进行审查和监督之间的平衡。该法主要修改了以下几点：一是加强了对在情报收集过程中向政府提供了协助的电信公司的保护，允许联邦法院驳回对这些提供了协助的电信公司的诉讼，只要他们能够证明其提供协助的行为是合法的；二是禁止州政府对电信公司和个人依据涉外情报监控法相关规定提供协助的行为展开调查和进行制裁；三是将执法部门可以实施的无令状的监控时间从48小时提高到7天；四是要求涉外情报监控法院批准对位于海外的美国人实施监控；五是要求所有参与了“总统监控计划”的情报机构的总监察长对本部门的监控活动实施全面审查并在一年之内提交报告，等等。

二、《涉外情报监控法》的主要内容

在美国国会编纂的《美国法典》2009年版中，《涉外情报监控法》共分为七章：第一章“电子监控”、第二章“物理性搜查”、第三章“为获取涉外情报信息，安装和使用通信记录与通信追踪装置”、第四章“为获取涉外情报而使用某些商务记录”、第五章“报告要求”、第六章“关于针对某些位于美国境外的人实施情报收集的额外程序”、第七章“对向政府提供协助的人的保护”。其主要包括以下内容：

一、涉外情报监控法的适用对象与范围

《涉外情报监控法》适用的主要对象为外国势力及外国势力的代理人，但是涉及美国人（包括美国公民和在美国取得永久居留权资格的人）的时候同样适用。《涉外情报监控法》第 1801 节（e）小节明确规定，在获取外国势力或外国势力的代理人的情报信息过程中，如果信息涉及某一美国人时同样适用。正是由于涉及美国人时同样适用，该法在美国国内受到广泛关注，尤其是 2001 年“9·11”恐怖袭击事件发生后，美国国会迅速通过的 2001 年《爱国者法》对该法进行了大幅度修改，极大地扩充了政府在反恐恐怖主义活动中的情报收集和调查取证权力，但与此同时，反恐扩权也引起了美国社会各界如美国民权联盟（ACLU）的担心和忧虑，担心政府假借反恐之名滥用权力，侵害美国人的隐私、财产和言论自由等宪法规定的权利。

二、涉外情报监控法院及《涉外情报监控法院诉讼规则》

1. 涉外情报监控法院

1978 年制定的《涉外情报监控法》在联邦司法系统中创设了一种新的法院，即涉外情报监控法院（Foreign Intelligence Surveillance Court，FISC）和涉外情报监控复审法院（Foreign Intelligence Surveillance Court of Review，Court of Review）。该法第 1803 节（a）小节规定：联邦最高法院首席大法官至少应当从美国的 7 个联邦司法巡回区中公开选任 11 名联邦地区法院法官组成一个法院。该法院中至少应当有 3 名法官居住在距离哥伦比亚特区 20 英里的范围之内。该法（b）小节规定：联邦最高法院首席大法官应当从美国联邦地区法院或联邦上诉法院中公开选任 3 名法官共同组成一个复审法院，其中一名法官应当被公开任命为首席法官。该法院依据本法之规定拥有对任何在涉外情报监控法院中被驳的申请进行复审的司法管辖权。

涉外情报监控法院及涉外情报监控复审法院中法官的任期为 7 年，任期届满后，即使符合条件也不得连任。该法第 1803 节（d）

小节规定：依据本节之规定选任的每一名法官的任期最长不得超过7年，7年期限届满之后，即使符合任职条件也不得被再次任命。例外的情形是，依据本节（a）小节之规定初次被选任的法官，其任期应当是1-7年，每一年即为一届任期，依据本节（b）小节之规定初次被选任的法官，其任期应当是3年、5年或7年，每一任期届满后在不超过7年的前提下还可以被任命。

涉外情报监控法院在联邦司法系统中的地位较为特殊：（1）地域司法管辖权很宽，“该法院拥有按照本法之规定发布的规则和程序审理电子监控申请和签发在美国境内任何地方进行电子监控的命令的司法管辖权。”（2）在级别上也相当高，对涉外情报监控复审法院的裁决不服的由联邦最高法院处理。联邦最高法院拥有对复审法院做出的裁决进行复审的司法管辖权。（3）关于涉外情报监控法院和涉外情报监控复审法院的成立及相关内容规定在涉外情报监控法第一章“电子监控”之中，但其司法管辖权覆盖了整个涉外情报监控法。（4）在《美国法典》中，涉外情报监控法院和涉外情报监控复审法院并没有出现在专门规范美国联邦司法系统的《美国法典》第28编“司法与司法程序”（JUDICIARY AND JUDICIAL PROCEDURE）之中，而是隐藏在《美国法典》第50编“战争与国防”（WAR AND NATIONAL DEFENSE）这一部分当中。

2. 《涉外情报监控法院诉讼规则》

《涉外情报监控法》第1803节（g）小节规定涉外情报监控法院可以从履行其职责的合理需要出发，制定相应的诉讼程序和规则并付诸实施。涉外情报监控法院依据此条款和《美国法典》第28编第2071节（28 U. S. C. 2071）关于法院规则制定权的规定（§2071. Rule - making power generally）制定了《涉外情报监控法院诉讼规则》，2006年2月17日生效。

《涉外情报监控法院诉讼规则》的内容比较简单，主要是从履行其职责需要尤其是从保密的角度对其诉讼程序做出了一些特殊规定，规则中没有相应规定的事项，参照适用联邦刑事诉讼规则或者