MEIGUO

SHEWAI QINGBAO JIANKONG YU TONGXIN JIEQU FALÜ ZHIDU

美国涉外情报监控与通信截取法律制度

刘　涛◎译

中国政法大学出版社

美国涉外情报监控与通信截取法律制度

刘　涛◎译

中国政法大学出版社

图书在版编目（CIP）数据

美国涉外情报监控与通信截取法律制度/刘涛译. —北京:中国政法大学出版社，2014.4
ISBN 978-7-5620-5320-0

Ⅰ.①美… Ⅱ.①刘… Ⅲ.①情报－监视控制－涉外行政法－美国 ②电信－经济法－美国 Ⅳ.①D971.221 ②D971.222.9

中国版本图书馆CIP数据核字(2014)第050944号

出 版 者　中国政法大学出版社
地　　址　北京市海淀区西土城路25号
邮寄地址　北京100088信箱8034分箱　邮编100088
网　　址　http://www.cuplpress.com（网络实名：中国政法大学出版社）
电　　话　010-58908285(总编室)　58908334(邮购部)
承　　印　固安华明印业有限公司
开　　本　880mm×1230mm　1/32
印　　张　9.125
字　　数　220千字
版　　次　2014年4月第1版
印　　次　2014年4月第1次印刷
定　　价　30.00元

本书为教育部2012年度人文社会科学研究项目
——《秘密侦查与技术侦查措施规范化研究》
（编号：12YJA820043）的成果之一

美国涉外情报监控与通信截取法律制度简介

一、与涉外情报监控和通信截取相关的立法及判例简况

美国联邦宪法第四修正案（1791）规定：人民的人身、住宅、文件和财产不受不合理搜查和扣押的权利，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，不得发出搜查和扣押令状。[1] 这一修正案对公民的人身、住宅、文件和财产权益提供了宪法保护，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，并且由独立的法官签发授权令状，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公民个人的人身、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，而电话通信的正式出现则是1876年亚历山大·格雷厄姆·贝尔（Alexander Graham Bell）取得电话发明专利权之后。因此，电

〔1〕 "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."

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。随着时代发展的需要，美国国会逐步制定了相关法律，结合判例，其立法与判例发展简要过程如下：

（一）1934 年《联邦通信法》及相关判例

在 1928 年的奥姆斯特德诉合众国（Olmstead v. United States）一案[2]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的讨论，最后以 5:4 通过了判决。首席大法官塔夫托（Taft）主笔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中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实施的行为，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，警察的行为并没有违反联邦宪法第四修正案，第四条修正案所保护的对象只适用于有形财产。

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之间的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［在《美国法典》中的编号是第 47 编第 605 节（a）小节（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截听，不得将被截听的通信的存在、内容、实质、主旨、结果或意义向任何人泄露或者公布。[3]在 1937 年的纳登诉合众国（Nardone v. United States）一

[2] 277 U. S. 438 (1928).

[3] “...no person not being authorized by the sender shall intercept any communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communications to any person.”

案〔4〕中，联邦最高法院认为，《联邦通信法》第705节中规定的“任何人”不仅包括公民个人，也包括联邦探员。因此，联邦执法人员通过窃听或截听〔5〕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，纳登诉合众国一案中的另外一个问题也得到了解决，即被告人的辩护律师是否可以质疑控方使用了截听所获得的信息，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”。然而，1934年《联邦通信法》的实质效力只是认定受到窃听的谈话在法庭上不具有证据资格（可采性），在《联邦通信法》通过之后，基于其他目的的截听仍然在持续。在1942年的戈德曼诉合众国（Goldman v. United States）一案〔6〕中，联邦最高法院重审，只要不存在物理性（有形的）入侵，通过紧贴墙壁安装某种窃听装置偷听隔壁房间的谈话（即“隔墙有耳”式窃听）并不违反联邦宪法第四修正案。相反，如果窃听装置穿透了墙壁，这种窃听行为则构成了对联邦宪法第四修正案的违反，在1961年的西尔弗曼诉合众国（Silverman v. United States）

〔4〕 1937. SCT. 1233, 302 U. S. 379, 58 S. Ct. 275, 82 L. Ed. 314 (1937).

〔5〕 在美国，关于窃听的英语单词主要有：eavesdrop、wiretap、wire tapping、bug、intercept等。笔者认为，尽管都有窃听、偷听的含义，但其侧重点有所不同：wiretap、wire tapping主要指搭线窃听；bug主要指通过装窃听器进行窃听；eavesdrop主要指偷听，如“隔墙有耳”式的偷听；intercept的内涵要宽泛一些，不仅包括“窃听”或“偷听”等秘密“听”的方式，也包括秘密查看、复制电子信息等，如互联网通信中存贮在服务器里的各种信息，既有语音信息，也有非语音信息，因而，intercept翻译为“截取”应该是最为准确的。目前国内学界所使用的术语也不尽一致，如有窃听、截听、监听、侦听等。本书中将intercept翻译为截听，保留了“听”这个意思。《涉外情报监控法》（Foreign Intelligence Surveillance Act of 1978）中主要使用的是surveillance，surveillance包括的内容更为广泛，既有监听、监视也有通信截取，以及通信追踪等，笔者将其翻译为监控。

〔6〕 316 U. S. 129 (1942).

一案[7]中，联邦最高法院做出了此种认定。

进入20世纪60年代以后，厄尔·沃伦·伯格（Earl Warren Burger）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限制。在1967年的伯杰诉纽约（Berger v. New York）一案[8]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实施或者正在实施；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；窃听事后必须告知，除非确实存在着紧急情况；必须向法院提交关于窃听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年的另外一起案件，即卡茨诉合众国（Kats v. United States）一案[9]中，联邦最高法院斯图尔特（Stewart）大法官主笔撰写的多数判决意见认定：即使没有某种物理性的（有形的）入侵证据，窃听和其他形式的电子窃听也构成了对联邦宪法第四修正案的违反，因为联邦宪法第四修正案保护的是“人民”而不是“地方”；一个人故意暴露给社会公众的部分，即使是在他的家里或者办公室，并不是联邦宪法第四修正案关注的对象；但是，如果一个人谋求将其作为隐私保护的一部分，即使是在社会公众可以接近的场所，也可以得到宪法性保护。对于FBI在公用电话亭对公民个人电话谈话的

〔7〕 365 U. S. 505 (1961).

〔8〕 388 U. S. 41, 87. S. Ct. 1873, 18 L. Ed. 2d 1040 (1967).

〔9〕 389 U. S. 347, 88. S. Ct. 507, 19 L. Ed. 2d 576 (1967).

窃听，Stewart 大法官认为，尽管公用电话亭具有公共性质，但是，“Kats”案力图排除的并不是入侵的“眼睛”，而是未受邀请的“耳朵”，因而也是不允许的。

总体而言，“Kats”案的判决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：联邦宪法第四修正案保护的是公民个人的隐私权，将联邦宪法第四修正案的保护范围从有形物品、地点扩展到了私人之间的交谈。但是，该案的判决意见并未解决在涉及国家安全的案件中进行截听时，联邦宪法第四修正案所要求的法院令状是否适用。

（二）1968 年《综合犯罪控制与街道安全法》及相关判例

作为对上述两起案例的部分回应和支持，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），该法中的第三部分又称之为“窃听法”（TITLE III - WIRETAPPING AND ELECTRONIC SURVEILLANCE）[10]，在《美国法典》中的位置是第 18 编第 119 章第 2510 ~ 2522 节（18 U. S. C. 2510 - 18 U. S. C. 2522），该法是继 1934 年《联邦通信法》之后关于窃听的一部专门法律，对窃听的条件、程序、方式及被告人的权利保护等问题作出了详细规定，目的是实现有效执行法律与公民个人权利保护之间的平衡。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的情况下才能实施。同时，为了捍卫美国的国家安全，该法赋予了总统额

〔10〕 此部分的标题较为准确的翻译应当是“窃听和电子监控”，通俗译为“窃听法”。

外的特殊权力，即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攻击或者其他敌对活动，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。但是，在1968年《综合犯罪控制与街道安全法》的第三部分“窃听法”中，对于美国总统权力的立法表述不甚明确，该法第2511（3）节规定：“本章或者1934年《联邦通信法》第605节中的任何规定不得限制美国总统在他认为必要的时候采取此类措施保护美国的宪法性权力”。[11] 此规定在表面上看来似乎是赋予了美国总统在国家安全受到威胁时可以授权实施无司法令状的电子监控行动。显然，对于含义不甚明确的这一规定仍然需要联邦最高法院通过判例来澄清和界定其具体含义。

1972年出现了关于窃听的具有里程碑式意义的案例是合众国政府诉美国地区法院（United States v. U. S. District Court）[12]，也称之为“Keith case”，在该案中，被告人挑战了美国政府依据上述1968年《综合犯罪控制与街道安全法》第2511（3）节这一例外规定在美国国内实施无令状的电子监控的合法性。在该案的判决中，联邦最高法院的大法官们以9:0的一致投票结果做出的裁决意见认为：美国政府误解了1968年《综合犯罪控制与街道安全法》第2511（3）节之规定，这一规定实质上并未授权美国总统可以授权实施无令状的电子监控，即使在美国国内

〔11〕 “Nothing contained in this chapter or in section 605 of the Federal Communications Act of 1934 shall limit the constitutional power of the President to take such measures as he feels necessary to protect the United States.”

〔12〕 407 U. S. 297（1972）.

存在着威胁国家安全的情况。因此，该案中政府实施的无令状窃听违反了联邦宪法第四修正案。在判例的基础上，对于这一含义不明、容易引起误解的立法用语，1978 年 10 月 25 日该法的修正案将其删除了。总体而言，“Keith”案明确了一个关键性问题：如果针对国内的目标进行监控必须遵循美国宪法第四修正案所要求的条件，未经授权的窃听是对美国宪法第四修正案的违反。

（三）1978 年《涉外情报监控法》

美国关于通信截听或监控的另外一部重要法律是 1978 年制定的《涉外情报监控法》（Foreign Intelligence Surveillance Act of 1978，FISA），该法在《美国法典》（U. S. C.）中的位置是第 50 编“战争与国防”（TITLE 50 — WAR AND NATIONAL DEFENSE）第 36 章（50 USC CHAPTER 36）。该法主要的立法背景之一是：尼克松总统“水门丑闻”事件（Watergate scandal）曝光后，美国社会各界对“水门丑闻”事件进行全面反思，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》中赋予其的特殊权力。该法适用的主要对象为外国势力及外国势力的代理人，但是在涉及美国人（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。该法规范了政府部门监控和收集情报的权力和程序，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，要求司法部长向依据《涉外情报监控法》第 1803 条特别组建的涉外情报监控法院（FISC）申请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截听；发生危机时，可以先进行截听，有溯及力的授权截听命令能够

事后获得。[13]

（四）1986 年《电子通信隐私法》

随着通信技术的发展，尤其是电子通信技术的发展，1968 年的《综合犯罪控制与街道安全法》中的“窃听法”部分已不能适应侦查和司法实践的需要，1986 年国会通过了《电子通信隐私法》（Electronic Communications Privacy Act of 1986，ECPA）。1986 年的《电子通信隐私法》共三个部分，不仅对 1968 年《综合犯罪控制与街道安全法》中的窃听法部分进行了重大修改，全面替代了该部分，而且增加了两部分新内容。

1.《电子通信隐私法》中的第一部分“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 2510～2522 节），替代了 1968 年的《综合犯罪控制与街道安全法》中的“窃听法”部分（即《综合犯罪控制与街道安全法》中的第三部分），并且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，同时也就扩展了截听的适用对象，使截听对象除了原来的有线和口头通信外，还包括了电子通信。

2.《电子通信隐私法》的第二部分“使用存贮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 2701～2712 条），规定了对于存储的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。截取存贮的电子通信信息不同于一般的截听，一般的截听是与截

〔13〕 关于《涉外情报监控法》制定和修改的详细内容的介绍参见译者翻译的另外一部法律：《美国涉外情报监控法及涉外情报监控法院诉讼规则》，中国人民公安大学出版社 2011 年版。

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的中转服务器中截取的。

3.《电子通信隐私法》的第三部分是“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3121～3127条）。在1979年的史密斯诉马里兰州（Smith v. Maryland）一案[14]中，警察在未取得法院授权令状的情况下，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，其不受隐私权的保护。但是，1986年《电子通信隐私法》的第三部分对这一判例意见做出了修改，将通信拨号信息和拨入信息视为公民个人隐私权的一部分予以保护，对于安装和使用通信记录器和通信追踪装置进行了限制。

（五）1994年《通信协助执法法》

通信截听的实施方式主要有两种：一种是执法机构自己的侦探和相关人员借助相关技术设备实施；另一种是执法机构在电信营运商的协助配合下实施。在美国，后者应当是主要的，因为通信截听、截取需要的人员和技术设备执法机构往往并不具备，而由电信营运商按照执法机构的需要实施能够更为有效的收集情报信息。为加强情报信息收集，明确在通信截听过程中电信营运商的协助能力、协助义务和相关法律责任，1994年10月25日美国国会通过了《通信协助执法法》（Communications Assistance for Law Enforcement Act of 1994）。该法分为三个部分（titles）：第一部分为“对数字和其他通信进行截听”（TITLE I—INTERCEPTION OF DIGITAL AND OTHER COMMUNICA-

[14] 442 U. S. 735 (1979).

TIONS)；第二部分主要对《美国法典》第18编中收录的《电子通信隐私法》的部分条款进行了修改（TITLE II—AMENDMENTS TO TITLE 18, UNITED STATES CODE)；第三部分是对1934年《联邦通信法》中一些条文的修改（TITLE III—AMENDMENTS TO THE COMMUNICATIONS ACT OF 1934)。其中，与通信截听密切相关的是第一部分，其简称为《通信协助执法法》，在《美国法典》中的位置是第47编第9章第1001～1021节，第二部分中对《电子通信隐私法》的修改已并入了《美国法典》中的《电子通信隐私法》，第三部分与通信截听关系不密切，因此本书中没有收录。

总之，美国现行关于情报收集和通信截听的法律制度主要包括：1934年《联邦通信法》第605节和第606节，1978年《涉外情报监控法》、1986年《电子通信隐私法》（该法全面取代了1968年《综合犯罪控制与街道安全法》中的第三部分“窃听法”）和1994年《通信协助执法法》。本书中是以《美国法典》2010年2月1日的版本为依据收录翻译了这几部法律。

二、《爱国者法》以来的主要修改情况

（一）《爱国者法》对《涉外情报监控法》和《电子通信隐私法》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境外的执法权力。例如，扩充了执法机构搜查电话、电邮通信的权力，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活动的权力，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）对《联邦刑事诉讼规则》、《涉外情报监控法》以及《电子通信隐私法》中的诸多条款进行了重大修改，一些条款甚至创设了以前立法中政府执法部门不曾拥有的手段和权力。

1.《爱国者法》对《涉外情报监控法》的修改主要有：

（1）对《涉外情报监控法》中的任意窃听（“roving” surveillance）权限进行了修改，扩大了可以进行任意窃听的范围。《爱国者法》第206节针对《涉外情报监控法》第105节[15]所规定的可以进行任意窃听的范围，增加规定“在某些情况下，即法院认为申请对象的行为可能对查证某特别个人或类似其他人的身份造成阻碍”时适用这种窃听。

（2）延长了《涉外情报监控法》中截听和搜查令状的有效期限。《爱国者法》第207节规定FISA中对外国势力及其代理人（非美国公民）进行窃听和物理性搜查令状的有效期限最长可以延长至一年。

（3）扩大了涉外情报监控法庭（FISC）法官的遴选范围。为更好地执行《涉外情报监控法》，《爱国者法》第208节放宽了可以担任涉外情报监控法庭法官的筛选范围和条件。

（4）《爱国者法》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权力，规定了可以将其运用到电子通信（如互联网）上。

（5）《爱国者法》第215节增补了《涉外情报监控法》，授权依据《涉外情报监控法》使用某些商务记录或其他物品，确

---

〔15〕 此处的第105条是指1978年《涉外情报监控法》制定时的编排体例，在《美国法典》中则是指第50编第36章第1805条。

立了“215 调查命令”。

（6）《爱国者法》第 218 节要求依据《涉外情报监控法》实施截听和搜查应当附具执法目的，取消了普通刑事犯罪和间谍犯罪之间搜查令和截听命令之间的界限。

（7）《爱国者法》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。

（8）《爱国者法》第 203 节（d）对涉外情报信息的含义进行了更为明确的界定。

2.《爱国者法》对《电子通信隐私法》的修改主要有：

（1）将与恐怖主义犯罪行为有关的通信信息纳入截听的范围（《爱国者法》第 201 节：授权截听有线、言谈和电子通信中与恐怖主义犯罪相关的信息）。

（2）授权在计算机诈骗与计算机滥用犯罪的调查中进行截听（《爱国者法》第 202 节：授权截听有线、言谈和电子通信中与计算机诈骗和滥用犯罪相关的信息）。

（3）《爱国者法》第 203 节授权执法部门共享犯罪调查情报信息：①《爱国者法》第 203 节（b）授权执法部门共享通过截听获得的任何电子的、有线的或者言谈的信息。任何调查官员、执法官员、政府检察官，依据本条款的授权，对通过截听有线、言谈和电子通信中所知悉的任何涉及涉外情报、恐怖主义、敌对势力等的信息以及由此衍生的证据，可以向任何其他的联邦执法机构、情报机构、保卫机构、移民局、国防部和国家安全机构的官员披露其内容，以便帮助这些官员利用相关信息履行其职责。②《爱国者法》第 203 节（c）要求司法部长制定专门的程序规则来规范和保障依据《联邦刑事诉讼规则》、《电子通信隐私法》以及《涉外情报监控法》进行的这类信息披露。

(4) 从立法技巧上澄清了截听立法上的一些规定。《爱国者法》第204节从立法技术上澄清了在涉外情报监控中使用通信记录器（pen register）和通信追踪装置（trap and trace device）属于对通信保护的例外，从实体法上明确了可以进行截听。

(5)《爱国者法》第209节扩展了依据法院司法令状截听和扣押有线和电子通信语音邮件信息的范围。

(6) 扩展了针对电子通信记录的传票的适用范围。《爱国者法》第210节扩展了依据《电子通信隐私法》对电子通信记录使用的传票的涵盖范围。

(7)《爱国者法》第212节修改了《电子通信隐私法》的紧急披露制度，授权电信营运商在紧急情况下，如可能造成生命危险或身体伤害时可以向执法部门披露客户的通信内容或相关记录，并免于承担相关法律责任。

(8)《爱国者法》第216节扩展了《电子通信隐私法》中与使用通信记录器和通信追踪装置相关的职权。

(9)《爱国者法》第217节修改了《电子通信隐私法》的截听权限，授权执法部门截取计算机非法侵入者的通信。

(10)《爱国者法》第220节扩展了《电子通信隐私法》中相关司法令状的效力范围，联邦法院针对电子通信证据签发的搜查令状在全国范围具有效力，不受地域限制。

(11)《爱国者法》第222节规定了相关人员为执法机构提供截听协助后有权获得补偿。该条规定：《爱国者法》没有对有线和电子通信服务的营运商或其他提供设备和技术支持的人施加任何额外的技术支持义务与要求。任何有线和电子通信服务的营运商、房东、管理者和其他依据《爱国者法》第216节之规定提供设备和技术支持的人，对于发生在提供设备和技术支持过程中的合理花费，有权获得合理的补偿。