解读美国电子监控制度的演变

周学峰
(北京航空航天大学 法学院, 北京 100191)

摘 要: 美国联邦最高法院通过判例确认政府从事电子监控应受联邦宪法"第4修正案"制约,政府从第三方获取当事人自愿提供的信息除外。美国国会通过《电子通讯隐私法》和《涉外情报监控法》,对美国政府基于执法需要而进行的监控与基于国家安全目的而进行的监控进行了进一步的规范。"911"事件发生后,美国国会颁布了《爱国者法案》,进一步扩大政府收集信息的权力范围,国家安全与个人隐私保护之间的关系被重新调整,并引发了诸多的争议。

关键词: 电子监控; 政府监控; 个人隐私
中图分类号: DF84 **文献标识码**: A **文章编号**: 1009-3370(2014)06-0110-09

一、从时间维度观察美国电子监控制度的演变

美国政府基于国家安全的目的而采取的秘密监控行动,最早可追溯至1775年,当时的大陆会议(Continental Congress)组建了"秘密通讯委员会",并授权其从事官方情报活动。美国独立之后,华盛顿、杰弗逊等都曾基于总统职权直接授权有关机构从事情报收集和反间谍活动[1]。

在电报发明后不久,对电报的窃听亦随之出现,在美国内战时期,南北双方的军队都互相窃听对方的电报以了解对方的军事部署;内战结束后,美国国会在进行一些调查活动时曾试图从西联公司获取电报记录,这一事件被披露后激起了美国民众的强烈反对。在民众的压力下,美国国会1880年曾考虑颁布一部保护电报通讯秘密的法案,虽然该法案最终未能在联邦国会获得通过,但许多州立法机关对此积极响应,纷纷制定禁止电报公司披露电报内容的法规[2]。在电话发明后不久,亦出现了窃听,许多州亦对此积极回应,到1928年时,有一半以上的州都制定有禁止搭线窃听的刑事法律。

20世纪初,美图和德国的关系紧张,威尔逊总统曾下令对德国外交官进行秘密监听。1917年俄国布尔什维克革命爆发后,美国"军事情报局"(MID)和司法部开始大量收集激进人士的情报,并开展大规模监听活动,以配合"反赤化"运动。在这种背景下,美国司法部成立以胡佛为首的秘密调查机构,后来被正式命名为"联邦调查局"(FBI)。

在20世纪30年代富兰克林·罗斯福总统执政期间,曾秘密授权联邦调查局从事与国家安全有关的情报收集工作,准许其从事监听、监视等活动。从此,总统直接授权,成为美国国家安全机构从事监控活动的重要法律依据①。

除了情报机构,政府执法部门在调查刑事犯罪时也经常采用监听措施。联邦最高法院在1928年的"欧姆斯蒂德诉美国政府"案中认定,政府执法机构搭线窃听他人电话的行为,不属于宪法"第4修正案"意义上的搜查或扣押,不受"第4修正案"的约束②。

联邦最高法院在"欧姆斯蒂德"案中宣称,如果国会认为应该禁止窃听电话行为,可以通过立法做出规定。基于此,国会1934年颁布《联邦通讯法》第605条款明确宣告:未经发送者授权,任何人不得截取无线电通讯或将截取的通讯内容泄露给第三人。联邦最高法院在1937年的"那顿诉美国政府"案

收稿日期: 2013-12-20
基金项目: 中央高校基本科研业务费项目(YWF-13-W01-003)
作者简介: 周学峰(1973—),男,法学博士,副教授,E-mail:zhouvx@sina.com

①在罗斯福总统执政期间,联邦调查局得到快速的扩张。在1933年罗斯福就任总统时,联邦调查局仅有353名特工和422名辅助职员;1945年罗斯福去世时,联邦调查局已有特工4 380名,辅助职员7 422名。联邦调查局不仅在人员方面得到扩张,其借助第二次世界大战的需要,在职权方面亦得到很大扩张。参见 Daniel J. Solove, Reconstructing Electronic Surveillance Law, 72 Geo. Wash. L. Rev. 1264, 1272(2004)。

②Olmstead v. United States, 277 U.S. 438(1928)。

中，宣布联邦执法机构通过窃听犯罪嫌疑人的电话而获得的证据不得作为刑事诉讼中的证据[①]。但是，联邦调查局之类的情报机构进行窃听的主要目的在于收集情报，如果无意将窃听的结果用于法庭审理，就可不必理会《联邦通讯法》。

第二次世界大战结束后，美国先后成立了中央情报局和国家安全局，专门从事对外情报收集活动，联邦调查局继续从事国内的情报收集，并借助冷战时期的反共浪潮从事了大量的监听活动。1967 年，美国联邦最高法院先后通过两个判决，推翻了先前的“欧姆斯蒂德”案的判决意见，认定政府机构的电子监听行为应适用联邦宪法第 4 修正案有关搜查和扣押的规定[②]。1968 年，美国国会制定了《全面控制犯罪与街道安全法》，该法案第 3 章对电子监听行为进行了全面规制[③]。

联邦最高法院在 1972 年的“美国诉美国地区法院”案中进一步指出，对于国内的国家安全案件，政府在进行监听时，仍应事先获得司法许可，但是，许可条件可与普通刑事案件不同，因为两者所适用的政策考虑因素不同[④]。

1975 年“水门事件”之后，美国国会组建专门委员会对政府的情报工作展开大规模调查，并重点调查政府的情报工作是否侵犯了美国公民的权利，1976 年 4 月对外发布内容详尽的调查报告（“Church”报告）[⑤]。其披露的政府机构进行情报收集时滥用职权行为令人震惊。有大量的个人和组织都遭到了情报机构的秘密调查，他们并没有从事任何暴力、违法行为或充当外国敌对势力代理人的行为，而仅仅是因为其政治信仰的缘故。情报机构对这些个人或组织的调查时间会长达数十年，尽管这些个人或机构并未从事过任何违法行为[⑥]。调查报告还披露，自富兰克林·罗斯福到尼克松的历任美国总统，都曾允许甚至鼓励政府机构从事与政治斗争有关的情报收集工作，例如，收集与总统的政敌有关的情报，这些情报往往与国家安全并无关系[⑦]。

美国司法部长 1976 年签发《国内监控指南》（Guidelines on Domestic Surveillance），明确要求政府实施国内监控应仅限于严重违反联邦法律的调查活动，而不得参与政治斗争。“指南”还规定实施政府监控的程序，规定联邦调查局在实施监控时应接受司法部的领导和监督，从而终结了联邦调查局自行其是的历史[⑧]。美国国会于 1978 年颁布《涉外情报监控法》（FISA），创设“涉外情报监控法院”（FISC）专门受理对政府机构提出的为收集涉外情报的需要而进行电子监控的申请，法院在审查后可向政府机构颁发监控许可命令[⑨]。

美国联邦最高法院在 1976 年的“美国诉米勒”案和 1979 年的“史密斯诉马里兰”案中，确立以下“第三方规则”：当事人对于向第三方自愿提供的信息不享有合理的隐私期待，政府机构在获取此类信息时，可以不受宪法第 4 修正案的约束[⑩]。作为对“米勒”案判决的回应，美国国会于 1978 年制定《金融隐私权法》（Right to Financial Privacy Act.），对联邦政府机构从金融机构获取客户的金融信息记录进行规制。作为对“史密斯”案判决的回应，美国国会于 1986 年制定《电子通讯隐私法》（ECPA），并对《全面控制犯罪与街道安全法》中的有关内容进行了修订[⑪]。

2001 年 9 月 11 日，美国遭遇了历史上最严重的恐怖袭击。美国国会在对“911”事件进行调查后认为，政府机构的情报工作不力，特别是多个政府机构之间缺乏信息方面的沟通与合作，是导致未能防范“911”事件的重要原因。10 月 26 日，布什签署

①Nardone v.United States，302 U.S. 379（1937）。

②Berger v. New York，388 U.S. 41（1967）；Katz v. United States，389 U.S. 347（1967）。

③Omnibus Crime Control and Safe Streets Act of 1968，Pub .L. 90-351。

④United States v. United States District Court，407 U.S. 297（1972）。

⑤United States Senate，“Final Report of the Select Committee to Study Governmental Operations With Respect to Intelligence Activities”（April 26，1976）。因为主持此次调查委员会的参议员为 Frank Church，所以，该调查委员会又被为“Church”委员会，其调查报告又被称为“Church”报告。

⑥例如，美国联邦调查局曾怀疑美国民权运动领袖马丁·路德·金是共产党的同情者而对其进行秘密监听和调查，在得出否定性结论后仍坚持对其进行调查。又如，联邦调查局怀疑 NAACP 组织与共产党有联系而对其展开秘密调查，该调查持续了 25 年，尽管调查机构一直都未获得任何有力证据。

⑦例如，肯尼迪政府曾让联邦调查局对一名国会议员进行窃听；约翰逊总统曾让联邦调查局对其批评者和反对者展开秘密调查；尼克松总统曾授权一项纯粹为白宫服务而与国家安全无关的秘密窃听项目。

⑧在此之前，特别是在胡佛主持联邦调查局期间，联邦调查局经常以总统直接授权为由，越过司法部，独立实施监控行为，几乎不受任何制约。

⑨Foreign Intelligence Surveillance Act of 1978，Pub. L. No. 95-511。

⑩United States v. Miller，425 U.S. 435（1976）；Smith v. Maryland，442 U.S. 735（1979）。

⑪Electronic Communications Privacy Act of 1986，Pub. L. No. 99-508。

《爱国者法案》[①]。该法案对先前制定的《电子通讯隐私法》和《涉外情报监控法》做出许多重要修订,放松对政府机构从事监控行为的许可审查标准,扩大了可收集信息的范围。

2007 年《今日美国》报刊披露美国国家安全局通过美国电话电报公司、Verizon 公司等电信公司收集了数百万美国人的电话记录信息,从而引发了公众对个人隐私受侵害的担忧,许多公民和组织纷纷对参与该项目的电信公司提起索赔诉讼。2013 年夏,"斯诺登"事件发生后,再次引发美国民众对隐私的担忧,美国总统公开宣布,将对政府的监控项目进行改革,增加监督的力度和透明度,以缓解公众焦虑[②]。

二、从宪法判例的视角观察美国电子监控制度的演变

(一)联邦宪法第 4 修正案

美国联邦宪法第 4 修正案规定:"人民有权使其人身、住宅、文件与财产受到保障,不受不合理的搜查与扣押,此种权利不可被侵犯,并且,只有当存在可信的理由,并有宣誓或郑重声明做支持,且具体指明了搜查地点、拘捕之人或扣押之物时,才可签发搜查或扣押许可证。"该条款强调:一是公民的人身与财产不受不合理的搜查与扣押;二是法院不得颁发内容宽泛的搜查与扣押许可证。制定这一宪法条款,与美国人在殖民地时期所遭受的痛苦经历分不开。在英国殖民统治时期,统治者经常借助英国国王颁发的"协助令"(writ of assistance)闯入私人住宅查抄违禁物品或走私物品,此种令状属于典型的内容宽泛的令状,一经签发,便可在国王终身及身后 6 个月内长期有效,美国人曾深受此类搜查与扣押令状之苦。

(二)"欧姆斯蒂德诉美国"案:窃听不属于搜查与扣押

联邦宪法第 4 修正案规制政府的"搜查"与"扣押"行为,可以推测的是,立法者是在当时的生活情景下理解"搜查"与"扣押"含义的,设想的主要场景是入室检查、对有形财物进行检查和扣押。然而,随着科学技术的发展,产生了一个新的问题,即窃听他人通话,是否亦属于一种"搜查"或"扣押"。

在 1928 年的"欧姆斯蒂德诉美国"案中,联邦政府指控以欧姆斯蒂德为首的一伙人违法图谋进口、运输和贩卖酒类,控方的主要证据是通过搭线窃听欧姆斯蒂德等人的电话内容而获得的。政府执法人员并没有进入犯罪嫌疑人的办公室或住宅内,而是在其房屋外通过将导线植入犯罪嫌疑人的电话线中进行窃听的。以首席大法官塔夫特为首的最高法院的多数法官都认为,这种搭线窃听行为并不属于联邦宪法第 4 修正案意义上的"搜查"或"扣押",因为,只有对人身、文件或其他有形的物质财产的搜查或扣押,或者实际物理性侵入他人房屋,才可构成"搜查"或"扣押"[③]。

在该案中,布兰迪斯大法官发表了著名的异议意见。他认为:"在适用宪法时,不能仅考虑我们已经知道的,还要考虑到未来有可能发生的情形。科技的进步为政府刺探信息提供了许多手段,不可能止步于搭线窃听。也许有一天会发展出一种新的方式,政府无需将文件从保险柜中取出,便可在法庭上再现其内容,并能够向陪审团展示家中所发生的最隐密的事情。"他还将电话通讯与邮寄相类比,一封投入邮箱中的密封的信件应受宪法修正案的保护,电话通讯亦应受到相同的保护[④]。他进一步解释道:"电话隐私遭受侵害而带来的危害要远远大于私拆信件。当一条电话线被窃听时,电话线两端的当事人的隐私都会受到侵害,并且,他们之间的谈话,无论内容为何,都可能被窃听,即使谈话内容是正当的、保密的、享受特权保护的。而且,对一个人的电话线进行窃听,会导致与其通话的每一个人都被窃听。"

布兰迪斯主张,对于宪法第 4 修正案上的"搜查"或"扣押"的解释,不能拘泥于字面含义,应从立法精神出发,做出与时俱进的解释,进行电话窃听时,是否进入被告的房屋并不重要,是否是出于执法的需要亦不重要,均应被看作"搜查"与"扣押"[⑤]。

(三)"伯格"案与"凯茨"案:窃听属搜查与扣押

在"欧姆斯蒂德"案约 40 年后,联邦最高法院通过两个判例改变了原先的态度。

1. "伯格诉纽约州"案

在"伯格诉纽约州"案中,政府执法人员依据纽

①该法案的全称为"United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001",其英文简称为(USA PATRIOT ACT),因此,又被称为《爱国者法案》。

②Obama Announces Proposals to Reform NSA Surveillance,Washington Post,August 10,2013。

③Olmstead v. United States,277 U.S. 438(1928)。

④布兰迪斯在判决意见中引用 Rudkin 法官的意见来说明信件与电话的关系:"的确,一个是看得见的,另一个是看不见的;一个是有形的,另一个是无形的;一个是密封的,另一个是未密封的,但是,这些差异并不是真正的不同。"

⑤Olmstead v. United States,277 U.S. 438(1928),Brandeis dissenting。

约州的法律，通过在墙壁上安装窃听器和录音装置，窃听到被告伯格的谈话，并将其作为指控伯格犯罪的证据。伯格却提出纽约州的相关法律违反了联邦宪法“第 4 修正案”，基于窃听所获得的证据应当予以排除。纽约州的法律规定，在执法人员“有合理的依据相信有可能获得犯罪证据”的情况下，可以请求法院颁发窃听许可证。联邦最高法院认为：“谈话”属于“第 4 修正案”的保护范围，使用电子装置窃取他人谈话属于“搜查与扣押”行为；纽约州的法规虽然规定了执法人员在进行窃听之前须征获法院的许可，但是，法规所规定的授权条件过于宽泛，仅要求有合理的依据相信有可能获得犯罪证据，而不要求相信犯罪行为已经发生或正在发生，并且，也不要求指明“搜查的地点”或“扣押的具体人或物”，不对所要窃听的谈话进行具体描述，而且，授权窃听的时间可长达两个月，这些都是与宪法第 4 修正案的要求所不符的①。

道格拉斯大法官在判决的附和意见中表达了对电子监听的强烈厌恶，在他看来，发放监听许可证相当于发放一份内容宽泛的搜查许可证，即使对时间进行限定，亦是对当事人隐私的严重侵犯，“这等于在卧室、会议室、社会场所、律师事务所，以及任何可以安置窃听器的地方，安放了一名政府职员。”他指出：“如果一部法规允许在每个有可信理由认为有可能获得犯罪证据的住宅或办公室内安置一名警察，毫无疑问，该法规将被认为严重侵害隐私而被推翻。我看不出此类法规与授权许可电子监听的法规有何不同，后者实际上是在家中放置了一名看不见的警察。如果有何不同，那就是后者对隐私的侵害更为严重，因为家庭主人对于自己隐私受侵犯完全不知晓。搭线窃听或电子窃听装置就像一个超级大网，它会将监听范围内的所有谈话全部吞噬进去，而不考虑参与谈话的人是谁或谈话的性质是什么。”②

2. “凯茨诉美国”案

在“凯茨”案中，凯茨被指控在州际间传递赌博信息而违反联邦法律，用于指控的一项重要证据是联邦调查局通过在公用电话亭外侧安装窃听录音装置而记录下来的凯茨的电话谈话内容。该案的争执焦点是，联邦调查局通过窃听获取证据的行为是否违反宪法第 4 修正案。最高法院在该案判决中明确宣称：当一个人进入电话亭，关上门打电话时，他有理由相信自己说的每一句话都是私密的，而不让全世界听到；政府对上诉人谈话的电子监听和记录侵犯了上诉人合理地认为其所享有所信赖享有的的隐私，并属于“第 4 修正案”意义上的“搜查与扣押”，至于政府所使用的电子装置是否穿透了电话亭的墙壁，则是无关紧要的③。因此，“凯茨”案的判决明确推翻了“欧姆斯蒂德”案的判决意见。

哈兰大法官在此案中发表了附和意见，他认为宪法第 4 修正案所保护的是当事人的“合理的隐私期待”，具体地讲“有两项标准，一是当事人存在事实上的（主观的）对隐私的期待；二是这种期待在社会看来是‘合理的’。”④该意见被后来的判例所采纳并得到进一步阐释。

值得注意的是，本案并不涉及国家安全，但是，怀特大法官在附和意见中提出：对于国家安全案件，无需像普通案件那样要求政府部门事先获得司法许可，只要总统或司法部长认为进行电子监听是合理的即可⑤。对此，道格拉斯大法官发表了不同意见：决不可为行政机关大开绿灯，不能因行政机关自己为某些案件签上了“国家安全”的标签，就可以豁免宪法所要求的司法许可；“第 4 修正案”之所以要求政府事先获得司法许可，是因为法官是与案件无利害关系的中立的第三方，而总统、司法部长或行政部门则不是，他们代表的是案件的一方当事人，甚至是监听对象的敌对方；放任行政机关自行决定监听将破坏宪法所规定的权力制衡原则⑥。

（四）“美国诉美国地区法院”案：国内国家安全监控规则

在“美国诉美国地区法院”案（“Keith”案）⑦中，被告 Plamondon 等人被指控阴谋破坏政府财产，他们在庭前动议中要求政府披露其通过电子监听获得的信息。政府提出：对被告进行电子监听，虽未获得法院的许可，但仍是合法的，因为获得了司法部长许可，进行监听是为了保护国家安全而进行情报收集所必需的；总统基于宪法享有为保护国家安全

①Berger v. New York，388 U.S. 41（1967）。

②Berger v. New York，388 U.S. 41（1967），Douglas concurring。

③Katz v. United States，389 U.S. 347（1967）。

④Katz v. United States，389 U.S. 347（1967），Harlan concurring。

⑤Katz v. United States，389 U.S. 347（1967），White concurring。

⑥Katz v. United States，389 U.S. 347（1967），Douglas concurring。

⑦United States v. United States District Court，407 U.S. 297（1972）。由于审理该案的美国联邦地区法院的法官的姓名为 Keith，所以，该判例又被称为“Keith”案。

而采取必要行动的权力,司法部长可代为行使此种权力,而无需事先获得法院许可。

联邦最高法院认为:即使是国内的国家安全案件,亦应遵守宪法"第 4 修正案",政府在进行监听之前应获得法院许可;国家安全案件,往往会涉及第 4 修正案,亦会涉及第 1 修正案,从历史上看,人们主张言论自由与出版自由的斗争与反对无证搜查与扣押的斗争是紧密联系在一起的,当政府监控的对象是那些在政治上持非正统观念的人时,为此提供宪法第 4 修正案的保护尤其重要。

最高法院指出应权衡两种价值:一是政府负有保障国家安全的职责;二是保障个人的隐私与言论自由不受不合理的监控的威胁。一方面,如果将国内的安全监控完全交由行政机构自主决定,那么,个人的隐私与自由将无法得到保障;另一方面,要求政府在实施监控前获得许可,并不会使得政府保障国家安全的职责受到严重的干扰①。与此同时,最高法院承认,国内国家安全案件与普通刑事案件存在许多不同,两者面临着不同的政策考量因素,因此,获得司法许可的条件与程序可以有所不同,具体应由国会来决定。另外,最高法院强调,该判决意见仅适用于国内的国家安全监控案件,而不适用于涉及外国势力或其代理人的有关国家安全的监控案件②。该案的判决意见对于后来的国会立法有着重要影响。

(五)"米勒"案与"史密斯"案:"第三方例外"规则

在"凯茨"案中,最高法院提出"第 4 修正案"保护的是"对隐私的合理期待",而在"米勒"案与"史密斯"案中,最高法院进一步指出,当事人对于其自愿向第三方提供的信息并不享有法律上的隐私期待,这意味着政府机构在从第三方获取此类信息时,可以不受"第 4 修正案"的约束。

在"美国诉米勒"案中,米勒被指控犯有联邦罪行,但其主张应将从银行获取的支票、存款凭条等银行记录的复印件从证据中排除,理由是执法机关获取这些证据的程序不合法,违反了联邦宪法第 4 修正案,属于非法扣押。最高法院驳回了米勒的主张,认定当事人对于支票、存款凭条等银行记录文件所记载的内容不享有法律上的"隐私期待",不受"第 4 修正案"的保护,因为支票并不属于秘密通讯,而是商业交易工具,其所包含的信息是当事人自愿传送给银行的,当事人在使用支票时可以预见到其已将相关信息揭示给银行的雇员③。

在"史密斯诉马里兰"案中,上诉人是犯罪嫌疑人,电话公司应警察局的要求在办公室安置了一个"笔式记录器"(Pen Register),记录从上诉人家中的电话机所拨出的电话号码,但警察局事先并未获得司法许可证。上诉人提出应将警察通过笔式记录器所获得的证据予以排除,因为其违反了宪法第 4 修正案。最高法院认为:首先,人们在拨打电话时通常都知道他们必须要向电话公司传输要拨打的号码并且电话公司会有设备能够将这些信息记录下来,而且电话公司确实会因多种商业目的(如核对帐单、防欺诈等)而进行记录,因此,人们通常不会对拨打电话的号码记录具有隐私期待;其次,即使上诉人的确对拨打的号码具有隐私期待,那么这种期待在社会看来也是不具有"合理性"的,当上诉人通过拨打电话而自愿地将号码信息传递给电话公司,并使其在日常营业中对此知晓,他就承担了电话公司有可能向警察局披露此信息的风险。因此,安装和使用笔式记录器的行为不属于宪法第 4 修正案意义上的"搜查"或"扣押"④。

三、从成文法规的视角观察美国电子监控制度的演变

在电子监控领域,美国国会制定的各种成文法规的中心内容要求政府机构在实施监控之前应申请获得某种类型的许可,如传票、法院命令或搜查许可证⑤。具有框架支撑作用的基础性法规当属《电子通讯隐私法》和《涉外情报监控法》。

---

①政府在本案中提出国家安全案件的复杂性和保密性等理由来反对事先获得许可,但遭到了最高法院的驳斥。

②United States v. United States District Court,407 U.S. 297(1972)。

③United States v. Miller,425 U.S. 435(1976)。

④Smith v. Maryland,442 U.S. 735(1979)。

⑤实践中主要有以下几种许可类型:第一类是传票(Subpoena),如大陪审团的传票或行政机关签发的传票,政府机构可凭借此类传票要求通讯服务商向政府机构提供客户的通讯信息或记录。第二类是法院命令(Court Order),又包括两种,一种仅要求政府机构在申请时能证明其可能获得的信息与执法调查具有相关性即可,而另一种则要求政府机构在申请时必须提供具体的、清晰的事实以证明其有合理的理由相信所要获得的信息与正在进行的犯罪调查既具有相关性亦具有重要性。第三类是搜查许可证(Warrant),又包括两种,一种存在"可信理由"(Probable Cause)的搜查许可证,例如,在刑事诉讼中,要求政府机构举出事实以证明存在相当大的可能性:犯罪已经发生并且在搜查地点有可能找到犯罪证据;另一种被称为"超级"(Super)搜查许可证,意味着其不仅要满足普通搜查许可证的申请条件,还要满足一些特殊条件,如要求政府机构在提出申请之前应穷尽其他所有可获取信息的方法等。参见 Orin S. Kerr,Internet Surveillance Law after the USA PATRIOT Act:the Big Brother that Isn't,97 Nw. U. L. Rev. 607,620-621(2003)。

(一)《电子通讯隐私法》

《电子通讯隐私法》共 3 章，分别被习惯称为“窃听法”(Wiretap Act)“存储通讯法”(Stored Communications Act)和“笔式记录器法”(Pen Register Act)。简单地讲，“窃听法”所保护的是当事人正在进行的通讯内容；“存储通讯法”保护的是临时存储的信息；“笔式记录器法”保护的则是不含通讯内容的电话号码之类的信息。

1. 窃听法

“窃听法”规制的对象是对他人正在通过线路进行传输的通讯的截取，如搭线窃听他人电话，但不适用于无声音的图像传输。政府执法机构在进行窃听之前，必须先申请获得法院的“超级搜查许可证”，法案为其设定了很高的许可条件，执法机构除了要提供“可信的理由”外，还要对截取通讯进行详细描述，要确保对非相关信息的截取做到最小化，要保证一经达到目的便立即终止。如果执法机构人员违反上述要求，将受到最低一万美元的罚款。

2. 存储通讯法

“存储通讯法”规制的对象是电子存储，即为了满足当事人进行电子通讯的需要而附带的和临时性的存储，它所保护的对象是那些非处于传输状态而是被临时存储起来的通讯信息，但不包含那些被固定存储起来的信息。例如，在接发电子邮件时，电子邮件首先到收件人的 ISP 的服务器中被临时存储起来，收件人将邮件打开下载后，可选择删除或保存。若该邮件未被删除，它将依然被存储在 ISP 的服务器中，此时的存储已不再属于“临时”存储，因此，当政府执法机构获取已被收件人打开过的电子邮件时，将不受存储通讯法的制约。

对于网络服务商所存储的有关客户的个人信息记录，如姓名、住址、电话号码、银行账号等，如果执法机构能提供具体的事实以证明有合理依据相信其与正在进行的刑事调查有关联并且重要，亦可申请获取。

就对个人信息的保护程度而言，法案对于电子存储通讯信息的保护力度要低于窃听法。对于存储时间等于或少于 180 天的通讯信息，政府机构只需满足普通搜查许可证的条件即可获得，而对于存储时间已超出 180 天的通讯信息，政府机构只需获得一份行政传票、大陪审团传票、审理传票或法院命令即可获得，其无需提供“可信理由”，只需举出具体的、清晰的事实以证明所欲获得的通讯与犯罪调查有相关性即可。

对于执法机关违反法定程序所获取的公民的电子存储通讯信息，并不适用于证据排除规则，该信息仍可作为刑事诉讼证据①。另外，执法机构人员违反上述规定所受罚款数也比较低，为最低一千美元。

3. 笔式记录器法

“笔式记录器法”规制的对象是执法机关利用笔式记录器或类似的追踪记录设备，记录被监控对象打入或打出电话的号码、拨打时间、通话时长等信息，但不涉及电话的具体内容。《爱国者法案》对笔式记录器法规制对象进行了扩展，从而将电子邮件的收发地址、时间等信息、访问网络时的 IP 地址和网址(URL)之类的网络信息涵盖了进去。“笔式记录器法”与前两章最大的区别在于，它所保护的并不是当事人通讯的“内容信息”，而是电话号码之类的不含通讯内容的“外在信息”。

就对个人信息的保护程度而言，“笔式记录器法”较之前两章法律要低，主要表现为执法机构获取许可安置笔式记录器等监控设备所需条件较低，虽然必须事先获得“法院命令”，但只需证明使用此类装置有可能获取相关信息并且这些信息与正在进行调查活动具有相关性即可，执法人员违反此类规定而获取相关信息，不会适用证据排除规则，对于受害人而言几乎无任何救济措施。

(二)《涉外情报监控法》

1.《1978 年涉外情报监控法》的主要内容

《1978 年涉外情报监控法》(FISA)适用于政府机构以收集涉外情报为目的对美国境内的“外国势力”(foreign power)或其代理人之间的通讯进行的监控。所谓“外国势力”，既包括外国国家，也包括外国政治组织；所谓“外国势力的代理人”，既包括外国政府的情报人员，也包括故意从事颠覆活动、国际恐怖主义，或代表外国势力为从事上述活动而进行准备的人。法案还对“美国人”(U.S. persons)和“非美国人”进行了区分，前者包括美国公民和永久居民(permanent residents)。无论是美国人还是非美国人，都有可能构成“外国势力的代理人”，但适用标准不同。对于美国人当其在明知状态下为外国势力从事情报活动并触犯美国刑法，才被认定为外国势力的代理人；对于非美国人，只要其成为外国势力的工作人员或国际恐怖组织的成员，便可被认定为外国势力的代理人。

①依照《电子通讯隐私法》，执法机关违反法定程序获取公民的电子存储通讯信息，会招致罚款的后果。但是，这对于保护当事人的个人信息而言，其作用非常有限，远不如证据排除规则更为有力。

由于涉外情报监控具有秘密性，不宜向外界公开①,如果放任情报部门暗箱操作,很容易导致权力滥用,因此,法案规定了行政、立法和司法三种监督措施。首先,法案要求司法部建立起一套确保政府机构在实施监控时对非公开信息的收集和传播做到最小化的程序(简称“最小化程序”),行政机构提出监控申请前应征得司法部长批准，并应遵循司法部所制定的各项要求。其次，法案还规定国会的监督机制，要求司法部长定期向国会报告涉外监控的实施情况。第三,建立司法制衡机制,要求政府机构在实施监控行动之前获得法院的许可，并接受法院的监督。鉴于情报工作的特殊性,法案创设了专门法院,即“涉外情报监控法院”。

涉外情报监控法院由最高法院首席大法官任命的 7 名(现行法规定为 12 名)联邦地区法院的法官组成。审理时通常是秘密的、不公开的,采用单方审理程序,即仅由政府机构提出单方申请,而没有任何敌对方出庭参与庭审。如果政府机构初审败诉,还可向由 3 名联邦法官组成的上诉法庭上诉。

《涉外情报监控法》所规定的监控许可条件要比《电子通讯隐私法》更为宽松,政府机构仅需证明其有“可信理由”相信电子监控的对象是外国势力或外国势力的代理人,必须同时表明其从事监控的目的是收集涉外情报。

(三)《爱国者法案》及其影响

2001 年的“911”事件发生后,美国国会通过了《爱国者法案》,对《涉外情报监控法》进行了多处修订,有两点重要变化尤其值得关注。

首先,《爱国者法案》扩大了《涉外情报监控法》的适用范围。《1978 年涉外情报监控法》明确规定其适用于以收集涉外情报为“目的”(the Purpose)的政府监控行为,在司法实践中,法院进行了扩张解释,将其适用范围扩充为以收集涉外情报为 “主要目的”(Primary Purpose)的政府监控行为。然而,在《爱国者法案》通过后,《涉外情报监控法》的适用范围变为以收集涉外情报为 “重要目的”(significant purpose)的监控行为。这意味着,只要政府机构的行动目的中有一项为收集涉外情报,即使不是主要目的,亦可依据《涉外情报监控法》实施。美国司法部 2002 年重新修订了监控指南规则,废除了先前的情报监控与刑事侦查之间的隔离机制,允许刑事侦查机构和情报收集机构互换信息②。

《电子通讯隐私法》和《涉外情报监控法》的分工原本明确，前者主要适用于普通的政府执法行动,如刑事侦查;后者适用于以涉外情报收集为目的的监控。《电子通讯隐私法》所规定的监控许可条件要比《涉外情报监控法》严格得多。依照《电子通讯隐私法》的规定,法院在签发监控许可命令时享有自由裁量权,即使政府的申请符合条件,法官依然可拒绝签发③。依据《涉外情报监控法》,在政府申请符合法律规定的条件时，法官必须签发命令,政府获得监控许可的比率非常高④。然而,在《爱国者法案》通过后,两种不同性质监控的边界开始模糊,政府机构基于《涉外情报监控法》的授权而获得的证据,亦可被用于刑事诉讼中,因此,有可能产生一个问题,即政府机构有可能在国内执法活动中依据《涉外情报监控法》提出监控请求,而绕开《电子通讯隐私法》,事实上,在《爱国者法案》通过后,政府机构通过《涉外情报监控法》获取法院的监控许可命令大幅激增,并在 2003 年首次超过了依据《电子通讯隐私法》取得的法院监控许可命令⑤。

其次,《爱国者法案》扩大了政府机构收集信息的权力范围。《1978 年涉外情报监控法》规定的监控仅限于电子监听之类的电子监控,1998 年法案进行修订时,将监控范围扩展,规定政府机构可以请求涉外情报监控法院发布命令,强制银行、电信公司等服务机构提供商业记录、文件等。《爱国者法案》将政府有权获取信息的范围进一步扩展为包括商业记录、文件在内的任何有形物品。在《爱国者法案》通过前,政府机构在申请获取商业记录时须提

①与《电子通讯隐私法》所规定的窃听不同,依据《涉外情报监控法》而实施的监听,不会向监听的对象披露,有些受监听的人可能永远都不知道监听的存在。

②美国涉外情报监控法院的上诉法庭在判决中确认了司法部的修订后的监控指南的合法性,其指出,在《爱国者法案》通过后,无需再对涉外情报收集工作与国内刑事侦查活动进行严格区分。参见 In re All Matters to Foreign Intelligence Surveillance,218 F. Supp. 2d 611,(Foreign Intel. Surv. Ct. 2002)。

③《电子通讯隐私法》规定:基于申请,法院“可以”签发命令。这意味着,法院亦可不签发命令。

④《涉外情报监控法》规定,在收到行政机关的符合条件的申请后,法院“应当”签发命令。这意味着法院对于是否签发命令并不享有自由裁量权。

⑤在 2003 年,依据《涉外情报监控法》签发的监控命令为 1724 起,而基于其他法律依据签发的监控命令总共 1 442 起。参见 Peter P. Swire,The System of Foreign Intelligence Surveillance Law,72 Geo. Wash. L. Rev. 1306,1308(2004)。另据《华盛顿邮报》披露,在 1978 年至 2001 年之间,美国政府每年依据《涉外情报监控法》向法院提出的监控申请平均为 600 件,而在 2001 年“911”事件之后,每年的监控申请数平均为 1 700 件,几乎是“911”之前的 3 倍。

供具体的事实以让人有理由相信该记录是属于某外国势力或外国势力代理人的；在法案通过后，只要政府机构提出欲获取的商业记录与反对国际恐怖主义或和反秘密情报活动具有相关性，即可获得许可①。另外，司法部等行政机构还可通过签发“国家安全信函”的方式，强制第三方服务机构提供监控对象的通信记录、银行帐户等信息②。

(四)《2008 年涉外情报监控法修订法案》

在《爱国者法案》通过后，美国政府借“反恐”名义展开了多项大规模信息收集活动，引发了许多法律争议以及人们对隐私受侵犯的担忧。基于此，美国国会颁布了《2008 年涉外情报监控法修订法案》，主要内容包括 3 方面。

第一，放宽了对位于美国境外的“非美国人”进行监控所需条件和程序，更加便利于美国的政府机构在境外从事情报收集活动。

第二，对于美国人，即使是处于美国境外的美国人，政府机构若要进行监控，也要获得法院许可。

第三，对于帮助政府实施监控、向政府提供客户信息或商业记录的服务商，给予责任豁免，禁止他人对其提起民事诉讼。该规定有助于消除与政府合作的商业机构的潜在法律责任威胁和忧虑，便于政府机构从商业机构处获得相关帮助和合作。

四、从技术变革的视角观察美国电子监控制度所面临的挑战

探讨政府实施电子监控时总会涉及到宪法“第 4 修正案”。“第 4 修正案”在制定之初注重的是对公民的住所、文件等财产的保护，“搜查”和“扣押”的含义也是与之相关的。随着电报、电话等通讯技术的出现，电子窃听技术亦随之出现，便出现了电子窃听是否属于“搜查”或“扣押”的问题。最高法院在初次遇到该问题时，仍然固守“搜查”与“扣押”在立法之初的原始含义，而无视技术的进步，认为只有对人身、文件或其他有形的物质财产的搜查或扣押，或者实际物理性侵入他人房屋，才可构成“搜查”或“扣押”③。直到近 40 年之后，美国最高法院才通过“伯格诉纽约州”案和“凯茨诉美国”案正式确认政府进行的电子窃听行为亦属于“搜查”与“扣押”④。相对于技术变革的脚步而言，法律制度的改革显得颇为迟缓。

随着现代信息技术的发展，美国的电子监控制度面临着诸多挑战。美国在 20 世纪 80 年代制定的电子监控法规，如《电子通讯隐私法》，沿袭传统的分类规则，即将通讯信息划分为“信封信息”与“内容信息”两类⑤。在电话通讯中，“信封信息”包括拨打、接收电话的号码、时间、通话时长等；内容信息即通话内容。在电子邮件通讯中，这一分类变得复杂。首先，发送和接收电子邮件的邮箱地址、时间等信息可被认定为信封信息，而电子邮件的内容被认定为内容信息。其次，人们通过互联网进行传输信息时，通讯信息往往被分解成若干个数据包，目的地计算机在接收后再将这些数据包进行整合从而将信息内容予以还原。在这个过程中，可以把每一个数据包看作一封信，每个数据包都含有发送信息和接收信息的计算机 IP 地址等类似“信封信息”，数据包所负载的信息亦可被看作是内容信息。当人们利用计算机和互联网发送和接收电子邮件时，一封电子邮件会在传递过程中会被分解为若干数据包，因此，数据包的“信封”和内容与电子邮件的“信封”与内容是两个概念。因电子邮件的大小而异，一个数据包所负载的内容信息有可能仅含有电子邮件的“信封”信息或内容信息，也有可能两者都包括[3]。

区分信封信息与内容信息的意义在于，它们所受法律保护的程度存在差异。对于邮寄的信件和包裹而言，内容信息是受宪法第 4 修正案保护的；而对于信封信息，客户并不享有合理的隐私期待，因为客户在将信件交给邮局工作人员时应认识到对方会看到信封上的信息⑥。同样，对于电话通讯，当事人的电话交谈内容信息应受宪法第 4 修正案的保护，当事人对于电话公司所保存的其拨打的电话号码等“信封”类信息，不受宪法第 4 修正案保护。在网络通讯环境下，这种规则很难适用，因为网络传输中的数据包的“信封”信息与内容信息无法与真正意义上的通讯的“信封”信息与内容信息一一对应，网络用户在向网络服务提供商所发送信息时

①USA PATRIOT Act，Section 215；50 U.S.C. § 1861。

②“国家安全信函”的性质类似于一种行政传票，由行政机关签发，而无需法院许可，因而通过国家安全信函获取信息更具隐蔽性。目前，美国的司法部、中央情报局、国防部等机构均有权签发国家安全信函。

③Olmstead v. United States，277 U.S. 438(1928)。

④Berger v. New York，388 U.S. 41(1967)；Katz v. United States，389 U.S. 347(1967)。

⑤在传统的通过邮政的通信方式中，所谓“信封信息”，包含信封上所记载的发信人、收信人的姓名、地址，邮戳的时间、地点，以及信封的大小和重量信息等；所谓“内容信息”，指的是有关信件内容的信息。

⑥United States v. Hinton，222 F.3d 664(9 Cir. 2000)。

往往将通讯的“信封”信息与内容信息混杂在一起。因此,当政府机构在对互联网通讯中的数据包进行监控时,很难将通讯内容与所谓的“信封”类信息严格区分。

《电子通讯隐私法》严格区分正在进行传输的通讯与被存储的通讯,并适用不同的法则。其中,“窃听法”仅适用于正在进行传输的通讯,而对于传输过程已结束的通讯则不能适用。该规则适用于搭线窃听电话,但是,对于网络通讯监控却成问题。当事人在利用电子邮件进行通讯时,邮件从发信者的网络服务商(ISP)的服务器先传递至收信者的网络服务商的服务器暂时存储,然后再等待收信者下载。如果政府机构进入收信者的 ISP 服务器中获取了该邮件,那么,通常并不构成对“窃听法”的违反,因为此时该邮件并未处于“传输”状态,只能受“存储通讯法”的保护。对于执法机构违反“窃听法”而获得的通讯内容,适用证据排除规则,而对于违反“存储通讯法”而截获的电子邮件不适用于证据排除规则。上述区分和界定虽然有一定的技术方面的依据,但与普通人的通讯观念不符。在现代社会,电子邮件交流与电话交流同等重要,有些场合前者甚至比后者更为重要,仅仅依据一些技术方面的差异而在法律上给予差别对待,其合理性令人怀疑。

《涉外情报监控法》将监控对象区分为“美国人”和“非美国人”,又将监控活动区分为美国境内与美国境外,这对于传统的监控方式或许还可适用,在网络通讯环境下,事实上已很难区分美国境内与美国境外,亦很难将美国人和非美国人区分开来。在斯诺登事件中,在美国国内倍受争议的政府监控项目中,许多都是针对“非美国人”的监控项目,事实上却有大量的美国人的信息亦被纳入政府的收集范围内。

五、结语

美国的立法、司法机构试图对政府实施的电子监控活动进行某种规制,出于对各种利益的考量,美国电子监控制度的整体走向却是呈现出政府实施监控的权力范围不断扩张的趋势。在现代信息技术变革的背景下,美国原有的电子监控法规亦面临着诸多挑战,亟需做出调整。

参考文献:

[1] William C B, Bowman M E. Executive authority for national security surveillance[J]. America University Law Review, 2001(50): 1.

[2] Daniel J S. Reconstructing electronic surveillance law[J]. George Washington Law Review, 2004(72): 1270–1271.

[3] Orin S K. Internet surveillance law after the USA PATRIOT act: the big brother that isn't[J]. Northwestern University Law Review, 2003(97): 611–615.

Understanding the Transformation of American Electronic Surveillance Law

ZHOU Xuefeng

(School of Law, Beihang University, Beijing 100191, China)

Abstract: The Supreme Court's decisions confirmed that the Fourth Amendment of Constitution applied to the electronic surveillance engaged by the government. However, it didn't applied to the information voluntarily conveyed to the third party. The Congress enacted ECPA and FISA to regulate the government surveillance for the law enforcement purpose and national security purpose. After the event of 911, the Congress enacted PATRIOT Act, which expanded the government's power to collect information. The balance between the national security and personal privacy protection has been readjusted and many disputes arose since then.

Key words: electronic surveillance; government surveillance; personal privacy

[责任编辑:箫姚]