DOI:10.15918/j.jbitss1009-3370.2015.0320

透过斯诺登事件看美国政府监控制度

周学峰
(北京航空航天大学 法学院,北京 100191)

摘 要:通过对美国政府所实施的电话元数据项目、棱镜项目和肌肉项目等政府监控项目的法律分析可以发现,这些监控项目所依据的法律规则的合宪性和合理性都值得反思。美国联邦最高法院在20世纪70年代创设的"第三方例外"规则,在当今信息技术背景下,已显得不合理。美国联邦立法机构在"911"事件后颁布的《爱国者法案》以反恐为借口,不恰当地扩张了政府实施监控的权力范围。美国立法机构应对政府监控进行改革,以维持国家安全与个人隐私之间的平衡。

关键词:政府监控;国家安全;个人隐私
中图分类号:DF84 文献标识码:A 文章编号:1009-3370(2015)03-0143-07

一、问题的由来

2013年6至7月间,英国《卫报》和美国《华盛顿邮报》等媒体披露美国国家安全局(NSA)前承包商雇员斯诺登(Snowden)提供的绝密资料,显示美国国家安全局、联邦调查局等政府机构直接或与电信公司、互联网公司合作,对美国民众、外国政府机构、民间机构和民众的电话记录、上网记录、电子邮件、网络传输数据等信息进行秘密监控,从而在美国国内和国际上引发对政府从事监控活动的热烈讨论。对于斯诺登事件,评论者甚多,人们选取的视角各有不同。依照美国国内法应如何评价美国政府所从事的监控行动,值得深入探讨。

二、电话元数据项目的法律分析

(一)相关事实

2013年6月5日,英国《卫报》披露一份美国涉外情报监控法院(FISC)的命令,该命令系美国联邦调查局(FBI)提出申请的,要求美国的电信公司Verizon向美国的国家安全局(NSA)按日提交其客户的电话记录和"电话元数据"(telephony metadata),既包含美国国内与国外之间的国际长途电话通话记录,也包括完全发生在美国国内的电话通话记录[①]。该事件曝光后,美国许多民众和民权组织纷纷对美国有关政府机构提起诉讼。其中,具有典型性的,如克雷曼(Klayman)诉奥巴马政府案,"美国公民自由协会"(American Civil Liberties Union)"纽约公民自由协会"等机构诉美国国家情报总监、国家安全局局长、国防部长、司法部长和联邦调查局局长案。原告指控被告授权实施的监控行为违反美国联邦宪法和法规,侵害其合法利益,请求法院宣告"电话元数据"项目非法,请求政府停止实施该项行动且销毁所收集的电话记录。

随后,美国司法部代表行政当局发表了"白皮书",为其实施的监控行为进行辩护[②]。据"白皮书"披露,"电话元数据"项目最早开始于2006年,后来经涉外情报监控法院的授权,该项目被续期34次[③]。该项目的内容为:电信服务商依涉外情报监控法院的命令,向政府提供电话记录数据,包括呼出和接入电话的电话号码、拨打电话的时间,以及通话的时长,但是,不包含有关通话内容的信息。通常由联邦调查局向法院提出申请,要求服务商将相关电话记录数据交由国家安全局存储,然后由国家安全局的专业分析师进行数据分析,并将所获得的有关恐怖主义活动的线索提交给联邦调查局的反恐机构。司法部和联邦调查局声称开展此项目的目的在于打击国际恐怖主义活动,试图通过了解那些已知的恐怖分子或恐怖嫌疑分子在与哪些人进行联系,从

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,副教授,法学博士,E-mail:zhouvx@sina.com

①In re Application of the FBI for an Order Requiring the Prod. of Tangible Things from Verizon Bus. Network Servs,Inc. on Behalf of MCI Commc'n Servs,Inc. d/b/a Verizon Bus. Servs. No. BR 13-80(FISC Apr. 25,2013)。

②Administration White Paper:Bulk Collection of Telephony Metadata Under Section 215 of the USA PATRIOT Act(August 9,2013)。

③依照《涉外情报监控法》和涉外情报监控法院的命令,该项目必须每隔90天续期一次。

而挖掘出恐怖组织,破解恐怖活动计划。

(二)相关法律分析

关于"电话元数据"项目,争议的焦点在于政府机构秘密获取海量电话记录的行为是否有法律依据,是否侵害公民合法权益。

1.对《爱国者法案》第 215 条的解释

在该事件中,美国司法部提出,政府机构获取电话记录的直接法律依据为《涉外情报监控法案》和《爱国者法案》第 215 条(以下简称"215 条款")。《涉外情报监控法》原仅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或其代理人之间的通讯进行监控的活动。"215 条款"系对《涉外情报监控法》的修订,规定"联邦调查局局长或其指定的人可以申请一项命令,基于防范国际恐怖主义或秘密情报活动的调查的需要,要求提供任何有形物品(包括书籍、记录、文件、资料及其他物品),但是,不得仅仅基于受《宪法》第 1 修正案保护的活动对美国人展开此类调查。"因此,"215 条款"在适用时需要满足条件:第一,政府机构的调查活动是经过合法授权实施,并且符合司法部发布的有关准则;第二,政府机构要求获得的物品须是可以通过法院发布"携证出庭传票"(subpoena duces teum)或其他命令而能够要求他人提供的物品;第三,政府机构须提供事实说明有合理的根据可以相信其欲获得的物品与经授权实施的调查活动具有"相关性"(relevance)①。

对于"电话元数据"项目而言,满足前两个条件并不难,争议的焦点主要集中在第 3 个条件,即对"相关性"的理解。美国司法部对于"相关性"做出了极其宽泛的解释,认为政府可以运用分析工具对其收集的大容量的电话元数据进行分析,从而有可能发现恐怖分子的通讯网络和相关信息,因此,只要是这种分析工具所需要的信息,都可满足"相关性"条件。美国司法部还声称自己对"相关性"的解释是符合立法原意的,其理由是,司法部每半年向国会的情报委员会报告"215 条款"实施情况,国会并未表示反对,并且在"215 条款"到期后,国会还多次通过新法案对其进行延期。

如果采用美国司法部对"215 条款"的解释,将意味着任何一名美国人无论其是否为外国势力的代理人,也无论其是否为恐怖分子或恐怖嫌疑人,也无论其是否从事过违法或危害国家安全的行为,都有可能因为与反恐或反情报调查"相关"而成为政府监控的对象。

如果司法部的解释符合立法原意,那么不仅应当得到国会的认同,而且还应获得大多数美国民众的认同。然而,事实并非如此。早在 2012 年,就有参议院情报委员会委员致信美国司法部长:"我们相信,如果人们了解到法院是如何秘密解释《爱国者法案》第 215 条的,大多数美国人都会感到震惊。正如我们所看到的,大多数美国人对于法案允许政府做什么的理解,与政府所声称的法案允许其做什么,两者之间存在巨大的差距。"②在"电话元数据"项目曝光后,《爱国者法案》起草者 Jim Sensenbrenner 议员指出,这一项目是属于对法律的滥用,"从所公布的法院命令的范围来看,行政当局和涉外情报监控法院是在依赖一种国会从未有过的意图来对法律进行无限制的解释。"③

2.所涉宪法问题

1)是否违反《联邦宪法》"第 4 修正案"

美国政府所执行的"电话元数据项目"涉及公民个人隐私保护,这与《联邦宪法》"第 4 修正案"相关。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。"

联邦最高法院 1967 年在"凯茨诉美国"案中确认政府的电子监听行为属于《联邦宪法》"第 4 修正案"所规定的"搜查与扣押",要求其事先必须获得司法许可④。然而,最高法院随后又在 1976 年的"美国诉米勒"案和 1979 年的"史密斯诉马里兰"案中确立了"第三方例外"的规则,认为适用宪法第 4 修正案的前提,是当事人对于政府行为所侵害的对象享有"法律上的隐私期待";当事人对于向第三方自愿提供的信息并不享有合理隐私期待,政府机构在从第三方获取此类信息时,可以不受联邦宪法第 4 修正案约束⑤。这意味着当事人对于电信公司所存储的电话通话记录并不享有法律所认可的隐私期待,政府机构在获取此类信息时不受宪法"第 4 修正案"制约。

2013 年 12 月,负责审理"电话元数据"项目所引发案件的纽约南区联邦地区法院和华盛顿特区联邦地区法院做出了截然相反的判决。前者援引

①50 USC § 1861(Access to certain business records for foreign intelligence and international terrorism investigations)。

②Senator Ron Wyden and Mark Udall's Letter to Eric Holder(March 15,2012)。

③转引自"美国公民自由协会"(American Civil Liberties Union)的起诉状。

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

⑤United States v. Miller,425 U.S. 435(1976);Smith v. Maryland,442 U.S. 735(1979)。

“史密斯诉马里兰”等判例，认定 “电话元数据”项目未违反宪法第 4 修正案①。后者则认为本案所面临的情形与“史密斯诉马里兰”案当时的情况明显不同，不宜适用“史密斯诉马里兰”的判决意见，认为“电话元数据”项目不符合宪法第 4 修正案的要求②。对于这一问题，尚待联邦最高法院做出权威判决。

2）是否违反《联邦宪法》“第 1 修正案”

“美国公民自由协会”在其诉状中声称，政府机构获取其电话记录后，便可知晓谁曾经在何时与“美国公民自由协会”进行过电话联系，这会极大地损害相关当事人的利益。“美国公民自由协会”经常会与社会各界人士进行电话联系，而且许多通话都是保密的，如果这些人事先知道他们的通话记录会被政府获得，那么他们就有可能不敢与“美国公民自由协会”进行自由交流。简单地讲，“美国公民自由协会”主张的是，政府对民众电话记录的监控行为会影响到民众的言论自由，而言论自由是宪法“第 1 修正案”保护的主要内容。美国的许多新闻媒体也表达了类似的主张③。

美国司法部辩称其所收集的对象仅限于当事人通话的号码和时长等信息， 而不涉及通话内容，因此不会危及言论自由。这种说法明显站不住脚。即使不含内容信息，电话记录数据本身就蕴含着许多信息，可以揭示通话者身份。如果通话者的身份曝光，其言论自由必将受到影响。美国国会也注意到了这一点，所以，在《爱国者法案》的“215 条款”中明确要求政府机构不得仅仅基于受宪法“第 1 修正案”保护的活动对美国人实施监控。然而，这样的规定在实践中几乎不会发挥任何实际作用，因为法案所禁止的是“不得仅仅基于……”，这种规定很容易被规避，只要政府能够举出其他理由，便可摆脱此规定的束缚。

三、“棱镜”项目的法律分析

在“斯诺登事件”中，最引人注目的当属“棱镜”（PRISM）项目。据英国《卫报》和美国《华盛顿邮报》等媒体报道，美国国家安全局、联邦调查局与谷歌、苹果、脸谱等互联网公司合作，秘密地大规模收集用户互联网通讯信息。据媒体最初报道，美国国家安全局直接进入互联网公司主服务器获取相关信息，随后，谷歌、苹果、脸谱等公司发布公告，称其从未允许国家安全局等机构进入其主服务器自主获取信息， 而是基于法院的命令和行政机关的请求，向其转交所请求提供的信息。

上述分歧涉及到的是政府的直接监控与间接监控的区别。政府直接监控，是指政府机构直接从事对数据进行收集、挖掘和分析，以获取自己所需要的信息；政府间接监控，则是指政府机构委托第三方服务机构从事数据收集、挖掘和分析工作，以获取所需要的信息。相比较而言，间接监控要较直接监控对公民的个人隐私侵害较小。政府在进行监控之前，并不能确切地知道所欲获取的信息在何处，而是需要收集海量数据进行筛选、挖掘和分析。如果进行间接监控，那么大多数无关的数据都会被政府委托的服务机构筛选掉，只将有用的数据和信息转交政府机构。在实践当中，出于节约成本的需要，联邦调查局经常采用间接监控的方式从互联网服务提供商（ISP）获得所需信息，但是，采用间接监控的前提是政府机构必须充分信任互联网服务提供商，而且对方有足够的能力来完成监控任务。在上述条件无法得到满足的情况下，政府机构就只能从事直接监控。其实， 美国联邦调查局在 20 世纪 90 年代末就开发了一种互联网数据监控软件 “食肉者”（Carnivore）用于直接监控，但在该项目曝光后引发了美国民众对侵害个人隐私的担忧[1]。为此，2001 年《爱国者法案》要求政府执法部门在互联网服务提供商的设备上安装自己的追踪和监控设备时，应记录下与设备安装和实施监控有关信息，并向涉外情报监控法院报告，以接受法院监督④。

在“棱镜”项目曝光后，许多人对美国国家安全局进行互联网监控的合法性提出怀疑，美国国家安全局辩称其监控对象主要是“非美国人”，其法律依据系《涉外情报监控法》第 702 条（以下简称“702 条款”）。该条款系美国国会在 2008 年对《涉外情报监控法》修订时增设的，核心内容为：美国司法部部长和国家情报总监共同向涉外监控法院提出认证（certification）申请，用以证明其制定并采用了符合

①American Civil Liberties Union，et al. v. Clapper，et al.，13 Civ. 3994 （WHP），United States District Court for the Southern District of New York，Dec. 27，2013。

②Klayman et al. v. Obama et al.，Civil Action No. 13-0851（RJL），United States District Court for the District of Columbia，Dec. 16，2013。

③例如，美联社总裁在得知政府在秘密收集美联社的电话记录后向司法部表达了强烈抗议，在其看来，欲保障新闻自由，就必须要保证新闻来源提供者的安全，如果政府能够获得相关电话记录，就能够查明新闻线索提供者的身份，那么，就会有许多人害怕受到政府调查而不敢向新闻机构提供线索，从而会危及到新闻业的生存与发展。

④18 U.S.C.§3123（a）（3）。

法律要求的目标确定程序(targeting procedure)和情报收集最小化程序(minimization procedure),该申请一旦获得法院的批准,司法部长和国家情报总监便可以共同授权,在无需法院颁发许可证或命令的情况下,对可合理相信位于"美国以外"的"非美国人"进行长达 1 年的目标监控,以获取涉外情报信息。监控的目标是位于美国境外的人,他们有可能利用美国的通讯服务进行联络,因此,美国政府可以通过与美国的通讯服务商进行合作,以获取境外监控对象的通讯信息。

需要强调的是,依据"702 条款"进行监控的对象应当是非美国人,必须有合理理由相信其位于美国境外。如果是对美国人或位于美国境内的人进行目标监控,则不得依据"702 条款"实施,而是应依其他法律取得的法院许可证或命令,方可实施。由此可见,美国立法者对于美国人和非美国人,美国境内目标和美国境外目标, 采取的是不同的政策,其程序的严格性以及对当事人隐私的保护程度是有明显区别的。然而,据新闻媒体披露,有大量美国人的电子通讯信息亦在美国国家安全局的信息收集范围内。美国国家安全局对此的解释是:由于技术的原因,这些美国人的通讯信息是在对外国目标进行监控时"偶尔地或附带地"收集起来的①。美国国家安全局所收集的信息可谓海量,即便是附带地收集,其存储的信息量亦是巨大的,所以美国民众仍然对此心存疑虑。

四、"肌肉"项目的法律分析

据美国《华盛顿邮报》2013 年 10 月 31 日报道,斯诺登披露的文件显示,美国国家安全局与英国的政府通信总部(GCHQ)共同执行一项代号为"肌肉"(MUSCULAR)的项目,他们通过秘密介入谷歌和雅虎这两大互联网搜索服务商在世界各地的数据中心之间的通讯线路,每天可获取数百万计的数据[2]。"肌肉"项目与"棱镜"项目的不同之处在于,它是美国情报机构直接在美国境外针对国外的互联网用户实施的监控项目,因此它并不适用《涉外情报监控法》,而是依据美国总统签发的《第 12333 号行政命令》(EO 12333)实施②。

既然美国国家安全局可以通过"棱镜"项目要求互联网服务商提供它所需要的各种数据,为什么还要秘密潜入这些互联网服务商的数据中心窃取数据呢? 或者说,既然有"前门"可以进,为什么还要开一个"后门"? 原因在于法律约束不同。如果国家安全局正式要求互联网服务商向其提供数据,就必须依据《涉外情报监控法》申请法院颁布命令并接受法院监督;如果国家安全局通过与外国情报机构合作在美国境外从事互联网监控以获取相关数据,就可以不适用《涉外情报监控法》,无须申请法院颁布命令。美国情报机构在依据《第 12333 号行政命令》实施境外监控时,仅需遵守行政机关内部的程序即可,无需向外部披露,几乎不受任何外部监督,因此情报机构享有非常大的自由度。虽然从理论上讲,美国情报机构在美国境外对美国人的通讯实施监控,仍应受《涉外情报监控法》管辖,但是,情报机构可以声称其有"合理理由"相信监控对象为"非美国人",从而避开《涉外情报监控法》管辖。事实上,互联网的使用已充分"国际化",即使有意仅对外国用户进行监控, 在大规模地收集数据的情况下,也会不可避免地"附带"地收集美国人通讯信息,正因如此,美国民众对于此类涉外监控项目表现了深切的关注和忧虑。

五、对美国现行政府监控制度的反思

(一)在现代信息技术背景下检讨"第三方例外"规则的合理性

美国联邦最高法院在 20 世纪 70 年代确立"第三方例外"规则,从而为个人隐私的宪法保护制造了一个很大缺口。最高法院认为,拨打电话的记录、银行支票上的信息等,属于当事人"自愿"向第三方服务机构提供的信息,因而不存在法律上的隐私期待,从而不受宪法保护。这种理由是很难令人信服的。这里面并不存在真实的自愿选择,而是消费者在使用此种服务时不得不提供的信息,除非消费者自愿摒弃电话、银行等现代社会生活方式。以所谓的自愿披露为借口而认定当事人对第三方存储信息放弃隐私期待, 实际上是一种法律武断处理方式。

随着现代社会已步入信息社会,"第三方例外"规则日渐显得不合情理。在现代生活方式下,人们会处处留下各种"痕迹"。例如,开设银行帐户、购买保险时,会被要求留下许多个人信息;购物刷卡消

①例如,某个美国人有可能与受监控的恐怖分子有联系而被纳入信息收集范围内。参见 National Security Agency:Mission,Authorities,Oversight and Partnerships(August 9,2013)。

②《第 12333 号行政命令》(EO 12333),最初是由美国总统里根在 1981 年签署的,被认为是美国国家安全局等情报机构从事境外收集情报的基本法律依据。从历史上看,在美国国会制定《涉外情报监控法》之前,情报机构从事监控活动的法律依据主要为美国总统的行政授权。由于《涉外情报监控法》的适用范围有限,因此,对于国会立法未及的监控领域,仍依赖于行政命令。

费时，会在银行卡公司留下消费信息；与家人、朋友、客户进行电话联系时，会在电话公司留下电话记录；上网浏览网页、发送和接受电子邮件时，会在网络服务商处留下数据，乘坐火车、飞机时亦会留下身份信息；网购或进行邮寄物品时，会留下家庭住址；去医院看病时，会在医院留下健康信息；向政府申请办理各种登记、执照时亦会被要求披露大量的信息。这些信息在美国宪法上统统被看作当事人没有隐私期待的信息。

更为重要的是，在 20 世纪 70 年代，个人在各种场合留下的数据不仅数量有限、收集困难，而且都是处于分散状态。但是，今天已进入了“大数据时代”，对信息的收集、处理和整合的技术前所未有。通过运用现代信息技术，政府机构可以非常低的成本将从各处收集起来的看似杂乱而各不相关的数据进行配对和整合，从而分析出有价值的信息，进而可以描绘出一个人的近乎全部的生活状况，包括其生活喜好、职业、家庭住址、财务状况、健康状况、日常行踪、生活交际圈子、工作状况，等等。这是 20 世纪 70 年代联邦最高法院在做出判决时所难以想象的。与此同时，随着数据挖掘技术的发展，政府对数据量的需求是空前的，其中只有一小部分是政府机构自己收集的，大量数据实际上都是从电信、银行、交通、医疗等第三方服务机构那里获得的，依照美国联邦最高法院确立的“第三方例外”规则，政府在获取这些数据时是不受宪法制约的[3]。美国联邦最高法院在 30 多年前所制造的宪法保护的缺口，到了今天，已被放大了许多倍，成为难以填补的大窟窿。

今天，美国法律界已开始重新反思“第三方例外”规则的合理性，并对是否继续坚持这一原则展开讨论。审理“克雷曼诉奥巴马政府”案的法官在拒绝适用“第三方例外”规则时称，联邦最高法院在 40 年前判决“史密斯诉马里兰”时，是不可能想像今天的案件情况的：在 40 年前，案件一旦处理完毕，政府机构通常不再保留公民的电话记录，而在今天的“电话元数据”项目中，政府不但保存了电话记录，而且还建立了一个数量极其庞大的数据库；在 40 年前，人们是想像不到今天的人们是如何通过电话相互交往的；40 年前，政府执法机构与电话公司亦有合作，但大多都是一次性或临时性的，而在今天的“电话元数据”项目中，国家安全局与电信公司之间建立了长期持久合作的密切关系；40 年前的法官是无法想像政府机构在今天所拥有的先进的信息收集和信息处理技术的①。

如果抛弃“第三方例外”规则，将政府对本国人所实施的监控行为全部纳入“第 4 修正案”的保护范围，那么许多监控行动的合宪性将会受到重新审视。美国司法部在为“电话元数据”项目进行辩护时声称，即使适用“第 4 修正案”的标准，其行为亦是合宪的：一方面，该项目对于保障国家和人民的安全具有重大价值，例如国家安全局运用分析工具从收集到的海量的电话记录数据中，发现了恐怖主义活动的线索，从而避免了多次恐怖主义袭击；另一方面，“电话元数据项目”所收集的只是电话号码之类的信息，而不涉及通话内容，因此对于当事人的隐私的损害程度非常有限。据此，美国司法部认为“电话元数据”项目达到了“第 4 修正案”所要求的“合理性”标准。然而，这只是美国司法部、国家安全局等政府机构的一面之词。关于“电话元数据”项目对于维护国家安全和反对恐怖主义的价值，参议院情报委员会委员 Wyden 和 Udall 认为：“说‘这些项目’粉碎了‘几十起恐怖袭击阴谋’是具有误导性的，海量收集电话记录的项目事实上所提供的价值极小，几乎没有什么真正的价值。”[4]另外，从美国公民自由协会的主张中，从美国公民对于这一监控项目的关注中，从生活常识出发，也可以正当地认为，电话记录本身即使其不含有内容信息，对于个人隐私保护和言论自由亦具有重要价值。因此，若以《宪法》“第 4 修正案”的标准来衡量，“电话元数据项目”能否达到宪法所要求的水准是令人怀疑的。

(二)国家安全与个人隐私之间的权衡

通过斯诺登事件而披露出来的诸多美国政府监控活动，基本上都是在“911”事件后实施的。在“911”事件发生后，美国人对安全的焦虑是先前所少有的，特别是在国会将这一事件的发生归责于政府情报机构的失败后，美国政府急于通过大规模收集数据来增强安全感，对于美国民众而言，这就意味着以牺牲个人隐私为代价来换取安全。

牺牲个人隐私是否能换来安全，隐私保护与安全之间是否水火不相容。当前被新闻媒体所曝光的并引起广泛争议的监控项目，多数都属于数据挖掘项目。由数据挖掘所得出的信息的可靠性取决于其所使用的数据的可靠性。当政府秘密地大规模收集个人数据时，无法对这些数据的真实性、准确性、相关性进行有效核对；当人们意识到政府监控项目的存在，当人们预料到第三方服务机构有可能会将其

①Klayman et al. v. Obama et al.,Civil Action No. 13-0851(RJL),United States District Court for the District of Columbia,Dec. 16,2013。

获得的个人数据披露给政府的时候,他可能有意识地伪装,或提供错误数据,在数据质量得不到保证的情况下,数据挖掘结果的可靠性也值得怀疑;另外,数据挖掘涉及对各种已收集起来的数据的整合和"二次利用",而数据挖掘项目的目的与这些数据最初被收集起来的目的往往不相关,因此,其对数据的准确性、相关性的具体要求也不同,从而也有可能产生偏差或错误①。其实,数据挖掘与隐私保护并非绝对互不相容,好的隐私保护政策可以保证个人数据的准确性、完整性、相关性、及时性,从而可以提高数据挖掘及其他数据应用技术的可靠性,然而,美国政府的许多做法却是与之背道而驰的②。

200 多年前,富兰克林曾警告:"那些试图通过放弃珍贵的自由以换取片刻的安全的人,最终将既得不到自由,也得不到安全。"[5]这句话,即使今天听起来,依然充满了寓意。美国政府以"反恐"为旗号大规模扩张政府监控的范围,声称监控对象主要为外国势力、恐怖分子和有恐怖涉嫌的人,但实际后果是,有大量美国普通民众的信息亦处于政府监控范围。美国民众最初支持政府监控,是为了换取安全感,然而在获知自己的信息也被大量地秘密收集后,却感到了不安。布兰迪斯大法官在 80 多年前曾警告:"经验告诉我们,在政府用心良好的情况下,最应当注意保护我们的自由。"③历史经验一再表明,政府机构在收集情报时,总会自觉或不自觉地扩张收集范围,往往会超出最初设定的目的和范围。即使政府收集信息的目的确实出于反恐,亦不能不择手段,更不能置民众隐私于不顾。

放弃隐私是危险的,参议员 Sam Ervin 曾警告美国民众:"每当我们放弃关于自己的一小部分信息给政府时,我们就放弃了一些自由。政府机构对我们知道得越多,它对我们拥有的权力就越多。当政府知道我们的所有秘密时,我们将赤裸裸地面对政府权力。"④政府监控的危害还在于,如果民众能够意识到自己的信息可能会被窃取,自己的言行将受到监控,那么,他们就会选择言行谨慎,不敢独立地发表意见,甚至通过伪装以掩饰真实的自我。如果一个人时时刻刻都带着面具生活,那么,就不会存在独立的、自由发展的个性。因此,监控的存在,不仅会损害个人的隐私,更为重要的是它会影响到言论自由,乃至民主政治的根基。

(三)监控活动的隐蔽性与公开性

政府监控问题的症结在于隐蔽性。特别是以保障国家安全和情报收集为目的的监控项目,比以刑事侦查为目的的监控项目更具隐蔽性。对于刑事侦查而言,进行监听或监视完毕后,要告知被监控对象,并在诉讼中进行证据开示,被告人有机会对于证据收集程序的合法性提出挑战,有权要求在刑事诉讼中排除那些通过非法监控程序获得的证据。然而,在以情报收集为目的的政府监控中,监控自始自终都处于保密状态,情报部门不可能向监控对象告知监控的存在,如果那样,实施秘密监控的目的就会落空,另外,此类情报,只要不被用于刑事诉讼程序,那么就无需对外披露。除此以外,《涉外情报监控法案》还明确规定,当政府依据涉外情报监控法院的命令,请求第三方服务机构提供监控对象有关信息记录时,该服务机构应该对此进行保密,如果擅自向外界披露,将构成犯罪。在这种制度背景下,被监控对象往往无法知晓监控的具体存在,无从评估自身个人信息被泄露的程度,更没有机会对于监控的合法性提出质疑。

政府权力的动作,如果不公开,将很容易导致权力滥用,已有无数的历史事件可以证明这一点。美国的立法者对此很清楚,所以在《涉外情报监控法案》中规定了监督与制衡机制。然而,在实践中,这一机制的运行是有问题的。首先,立法虽然规定政府情报部门在实施监控之前应向法院提出申请,在监控完成之后应向法院进行报告,然而,这只是"单方程序",即只存在政府情报部门这一方面的当事人,而被监控对象则没有机会参与到这一程序中,法院只能听到政府情报部门的一面之词,不存在对抗或辩论的程序。因此,这一程序的公正性是令人怀疑的。实践中,政府情报部门所提出的监控申请,绝大多数都能获得法院批准,也就

①例如,美国在"911"之后加强了飞机乘客的安全性的审查,通过数据软件对乘客信息进行筛查,并设立禁飞名单,美国参议员爱德华.肯尼迪的名字竟然也被列入禁飞名单。

②例如,美国司法部在 2003 年授权联邦调查局的"国家犯罪信息中心"豁免适用《隐私法》关于数据"准确性、相关性、及时性和完整性"的要求;美国国土安全部在 2003 年豁免了美国的"交通安全管理局"的乘客筛选数据库适用《隐私法》关于政府存储的个人信息记录的"相关性与必要性"的要求。参见 Fred H. Cate, Government Data Mining: The Need for a Legal Framework, 43 Harvard Civil Rights-Civil Liberties Law Review 435, 482, 483 (2008)。

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

④Introductory Remarks of Senate Sam J. Ervin on S. 3418, Legislative History of the Privacy Act of 1974 S. 3418 (Public Law 93-579)。

不足为奇了[①]。

在美国，不仅政府从事监控活动的申请与实施是保密的，甚至相关法律程序和规则也是保密的。例如，当 2012 年美国《纽约时报》和“美国公民自由协会”提起诉讼请求司法部公开政府对《爱国者法案》中“215 条款”的官方解释时，美国司法部以保护国家安全为由拒绝公开，理由是如果对这一法律条款的解释处于保密状态，那么美国的敌人将无从知晓美国的情报部门的权限有多大。正如美国参议员 Ron Wyden 和 Mark Udall 所批判的那样，这种论点是荒谬的，如果这一逻辑得以成立，那么美国所有关于政府监控的法律都应是保密的，那样的话，美国的对手将更难了解美国政府能获取哪些监控信息[②]。然而，在情报斗争最为激烈的冷战时期，美国国会公布《1978 年涉外情报监控法案》，将情报工作纳入到公开的法律框架内。奥巴马政府宣称，欢迎民众就国家安全与隐私保护问题进行讨论并做出选择，然而，如果民众对于政府能够做什么、个人隐私会在多大程度上受到损害都无从了解的话，将无法进行有意义的讨论或做出真实的选择。

六、结语

“斯诺登”事件为考察美国政府监控制度提供了一个很好的视角，透过这一事件，可以感觉到传统的政府监控制度在现代信息技术背景下所面临的挑战，人们需要重新思考政府监控、国家安全与个人隐私保护之间的关系。

参考文献：

[1] Orin S K. Internet surveillance law after the USA patriot act：the big brother that Isn't[J]. Northwest University Law Review，2003(97)：653–655.

[2] Barton Gellman and Ashkan Soltani. NSA infiltrates links to Yahoo，Google data centers Worldwide，Snowden documents say[N]. Washington Post，2013–10–31(1).

[3] Michael Isaac. Privatizing surveillance：the use of data mining in federal law enforcement[J]. Rutgers Law Review，2006(58)：1058–1079.

[4] Ellen Nakashima. Senators say NSA phone records played little role in stopping terror plots[N]. Washington Post，2013–06–19(3).

[5] Benjamin Franklin. Historical review of pennsylvania[M]. London：British Library，2011：1.

Understanding American Government Surveillance Law through an Analysis of Snowden Event

ZHOU Xuefeng

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

Abstract：Through the legal analysis of American government surveillance programs，such as Telephony Metadata，PRISM and MUSCULAR，one can find that both the constitutionality and reasonableness of the rules backing the surveillance programs should be reconsidered. The rule of Third Party Exception which was established by the Supreme Court in 1970's becomes unreasonable under the background modern information technology. The PATRIOT Act which was enacted by the legislature after the event of 911 overly expanded the government's power of collecting data under the pretext of anti–terror. The legislature should reform the current legal rules of government surveillance to keep the balance between national security and personal privacy.

Key words：government surveillance；national security；personal privacy

[责任编辑：箫姚]

①据统计，1979 年至 2006 年期间，涉外情报监控法院共批准 22 984 件监控申请（其中 40%为 2001 年 911 事件之后的监控申请），只有 5 起申请未获批准。参见 Fred H. Cate，Information Privacy in the War on Terrorism，a White Paper of the Miller Center of Public Affairs at the University of Virginia，Nov. 2007。

②Senator Ron Wyden and Mark Udall's Letter to Eric Holder(March 15，2012)。