美国全球监听行动纪录

互联网新闻研究中心

2014年5月26日

目录

导言

一、美国在全球范围广泛从事秘密监听

二、美国把中国当成秘密监听的主要目标

三、美国秘密监听不择手段

四、美国全球监听受到广泛批评

导言

2013年6月，英国、美国和中国香港媒体相继根据美国国家安全局前雇员爱德华·斯诺登提供的文件，报道了美国国家安全局代号为"棱镜"的秘密项目，内容触目惊心。中国有关部门经过了几个月的查证，发现针对中国的窃密行为的内容基本属实。

作为超级大国，美国利用自己在政治、经济、军事和技术等领域的霸权，肆无忌惮地对包括盟友在内的其他国家进行监听，这种行为的实质早已超出了"反恐"的需要，显示出其为了利益完全不讲道义的丑陋一面。这种行为悍然违反国际法，严重侵犯人权，危害全球网络安全，应当受到全世界的共同抵制和谴责。

美国对全球和中国进行秘密监听的行径包括：

—每天收集全球各地近50亿条移动电话纪录。

—窥探德国现任总理默克尔手机长达十多年。

—秘密侵入雅虎、谷歌在各国数据中心之间的主要通信网络，窃取了数以亿计的用户信息。

—多年来一直监控手机应用程序，抓取个人数据。

—针对中国进行大规模网络进攻，并把中国领导人和华为公司列为目标。

美国的监听行动，涉及到中国政府和领导人、中资企业、科研机构、普通网民、广大手机用户等等。中国坚持走和平发展道路，没有任何理由成为美国打着"反恐"旗号进行的秘密监听的目标。

美国必须就其监听行动作出解释，必须停止这种严重侵犯人权的行为，停止在全球网络空间制造紧张和敌意。

一、美国在全球范围广泛从事秘密监听

1.美国监听世界政要

2013年底，英国《卫报》报道，包含联合国秘书长潘基文、德国总理默克尔、巴西总统罗塞夫等多达35国领导人都出现在美国国家安全局的监听名单上。

德国《明镜》周刊今年3月29日援引斯诺登提供的文件披露，美国国家安全局2009年针对122名外国领导人实施监控，并建有一个专门存放外国领导人信息的数据库，其中关于德国总理默克尔的报告就有300份。名单从"A"开始，按每人名字的首字母顺序排列，第一位是时任马来西亚总理阿卜杜拉·巴达维，默克尔排在"A"区的第九位。122人名单的最后一位是尤利娅·季莫申科，时任乌克兰总理。

德国"明镜在线"报道，联合国总部、欧盟常驻联合国代表团都在美国国家安全局的监听范围之内，监听内容涉及政治、经济、商业等领域。

美国国家安全局2012年夏季成功侵入了联合国总部的内部视频电话会议设备，并破解了加密系统。被曝光的秘密文件说，"数据传输给我们送来了联合国内部视频电话会议。"

美国《纽约时报》报道，2010年5月，当联合国安理会考虑是否要因为伊朗的核计划而制裁该国的时候，数个理事国的投票意向悬而未决。当时的美国驻联合国大使苏珊·赖斯请求美国国家安全局的协助，"以便她制定应对策略"。美国国家安全局很快起草出了监控四个理事国外交官所需的法律文件。

根据斯诺登曝光的文件，美国国家安全局已经渗透的使馆与使团名单包括巴西、保加利亚、哥伦比亚、欧盟、法国、格鲁吉亚、希腊、印度、意大利、日本、墨西哥、斯洛文尼亚、南非、韩国、委内瑞拉和越南。

除了联合国总部，欧盟和国际原子能机构的IT基础设施和服务器信息已被美国掌握。欧盟驻联合国机构变换了办公地点，搬进新的办公室后，美国仍在继续其窃听行为。

斯诺登提供给英国《卫报》的一份文件显示，美方设于英国北约克郡一处情报分支机构在2009年的20国集团峰会上监听俄罗斯时任总统梅德韦杰夫与国内的卫星通话。这次监听的时间是梅德韦杰夫与美国总统奥巴马举行会谈后数小时，两人在会谈中刚刚就建立互信达成共识。

一份日期标注为2012年6月的机密文件显示，当时还是墨西哥总统候选人的培尼亚的电子邮件曾被美国国家安全局秘密窃取，其内容包括了培尼亚准备提名的部分内阁成员等。

美国国家安全局在窃取巴西总统罗塞夫的通讯资料时，使用了一种特殊的电脑程序，可以拦截电子邮件及网络聊天的内容。

在2007年联合国气候变化大会上，澳大利亚情报机构国防情报局同美国国家安全局对印尼开展了大规模的监听活动。

2010年6月G20峰会在多伦多召开时，美国国家安全局进行了为期六天的间谍活动，美国驻加拿大使馆当时则变身为安全指挥部。

曝光文件还显示，日本与巴西、伊拉克被共同列为美国"经济稳定与影响"领域的重点监控国。此外，"最新战略科学技术"领域的重点监控对象包括俄罗斯、印度、德国、法国、韩国、以色列、新加坡、瑞典及日本；"外交政策"领域包括中国、德国、法国、俄罗斯、伊朗、朝鲜及日本等17国及联合国。

《纽约时报》总结说，美国国家安全局之所以"敌友不分地进行日常监控"，是为达成"对法德等同盟国的外交优先地位"和"对日本及巴西的经济优先地位"。

2.美国监控全球民众

美国专门监控互联网的项目非常庞大，可以监控某个目标网民的几乎所有互联网活动。英国《卫报》披露，美国情报人员利用名为"XKeyscore"的项目监控互联网活动。该项目在全球多处配备500个服务器。这家报纸评价其是美国国家安全局"最庞大"监控项目，称情报人员"可以监控某个目标网民的几乎所有互联网活动"。

斯诺登曝光的文件显示，美国国家安全局通过接入全球移动网络，每天收集全球高达近50亿份手机通话的位置纪录，并汇聚成庞大数据库。美国国家安全局大规模搜集全球手机短信息，每天收集大约20亿条。

一些美国媒体认为，美情报机构对嫌疑人相关电话进行窃听以掌握情报并非新闻，但涉及国外如此海量信息的收集相当不可思议。

据《华盛顿邮报》报道，美国国家安全局曾秘密侵入雅虎、谷歌在各国数据中心之间的主要通信网络，窃取了数以亿计的用户信息，并且保留了大量数据。通过分析这些数据，美国国家安全局可以获悉这些通讯纪录的发出者、接受者以及双方通讯的时间、地点等信息。

巴西网站Fantastico报道称，美国国家安全局采用MITM攻击方式，通过虚假的安全认证伪装成合法网站，以绕过浏览器的安全防护并截取用户数据。美国国家安全局曾通过这一方式伪装成谷歌网站成功获取用户数据。

英国《卫报》披露美国国家安全局与以色列共享原始监听数据，且可能包括美国公民的邮件和其他数据，而此前美国总统奥巴马坚称不会把监听目标锁定在美国公民身上。

2013年12月31日，德国《明镜》周刊消息称，美国国家安全局非法获取欧洲和亚洲之间最大的海底通讯电缆网络—SEA - ME - WE - 4的数据，取得大量敏感资料，并计划继续监听其他海底通讯电缆。

法国《世界报》报道称，美国国家安全局曾在2012年12月10日至2013年1月8日期间，监听法国民众7030万通电话交谈。

苹果和安卓手机操作系统在美国国家安全局内部被称作"数据资源的金矿"，美英情报部门2007年就已合作监控手机应用程序，美国国家安全局一度将这方面的预算从2.04亿美元追加到7.67亿美元。

据英国《卫报》、美国《纽约时报》报道，美国国家安全局多年来一直从移动设备应用程序（App）中抓取个人数据，包括个人用户的位置数据（基于GPS）、种族、年龄和其他个人资料。这些应用程序包括手机游戏"愤怒的小鸟"、应用程序"谷歌地图"以及"脸谱"、推特和网络相册Flickr的手机客户端。

美国国家安全局至少于2008年起，向全球近10万台计算机植入专门软件，旨在时刻监控或攻击目标计算机，即使计算机没有连接上网，美国国家安全局仍可通过无线电波入侵。自2010年起，美国国家安全局用收集到的资料，分析部分美国公民的"社交连结，辨识他们来往对象、某个特定时间的所在地点、与谁出游等私人信息"。

美国国家安全局所有的监控行为都是暗中操作，而政府也是秘密决定放开对监控的限制，并未通过国家情报法院的审定或者公开的讨论。根据2006年美国司法部的备忘录，该部曾对滥用情报监控进行过警告。

通过一项名为"共同旅行分析"的项目，美国国家安全局在收集"目标人物"相关信息纪录基础上，通过已知"目标人物"的活动发现其未知社会联系，并在一小时内在海量信息中得出"目标人物"活动时间、地点等完整情报。与"目标人物"有过联系的人将可能成为美国国家安全局新的"目标人物"。

美国官员辩称，这一大规模监听活动是合法的，不针对美国国内民众，但事实上，被窃听者包括许多到国外旅行的美国人。美国媒体报道说，美国国家安全局于2010年和2011年进行了一项有关大规模收集美国国内移动电话位置的试验项目。

2013年4月，联合国人权理事会言论自由问题特别报告员拉卢在向联合国人权理事会提交的报告中指出，美国修订"外国情报监控修正案法"，扩大美国政府对境外非美籍人士进行监控的权力，监控内容包括任何利用美国的云服务主机进行的通信。

曝光文件显示德国、韩国、日本等多国被大规模监听，美欧国家的情报机构正在联手对互联网和电话通信展开大规模监控，严重威胁世界各国网络安全。

挪威媒体报道说，挪威也是美国"监控门"的受害者，美国国家安全局曾在2012年12月10日至2013年1月8日间监听了3300多万次在挪威本土登记注册的移动电话通话。

根据意大利《快讯》周刊的报道，英国和美国情报机构大规模窃听意大利的电话和拦截网络数据。

3.监控外国企业

美国政府攻击的商业网络不仅包括互联网，还涉及金融、交通、电力、教育等诸多关系国计民生的关键行业。

斯诺登披露的文件显示，美国国家安全局开展的大规模监听行动不仅包括世界各国领导人，还包括众多国际组织和商业领袖。

据德国《明镜》周刊报道，美国国家安全局的监视项目包括国际间的金融交易，尤其是信用卡交易。全球知名的信用卡品牌维萨公司和总部设在布鲁塞尔的环球银行金融电信协会均在其监视范围之内。

一项名为"追踪金钱"的监视项目专门关注国际上银行金融交易往来。按照美国国家安全局的事先设想，通过追踪所谓的金融往来线索，可以追查到更多的恐怖分子。其为此专门建立一个名为Tracfin的金融数据库，用以存储从各个金融机构得到的信息。2011年，这一数据库的信息量达到1.8亿条，其中84%的数据是信用卡信息，涉及用户主要分布在欧洲、中东和非洲。

此外，该数据库中还有部分信息来自欧洲的环球银行金融电信协会。美国"9·11"恐怖袭击之后，环球银行金融电信协会开始秘密向美国提供金融交易数据。2006年这一事件被媒体曝光后，欧盟要求与美国展开谈判，以保证欧洲银行数据的安全和公民隐私权。在多轮谈判后，欧盟和美国于2010年达成一项协议，允许美国通过环球银行金融电信协会系统获取欧洲银行的交易信息，用于打击恐怖主义，但美国在使用和存储这些金融信息方面必须遵守欧盟数据保护法律之下的严格规定。然而，根据斯诺登的最新爆料，美国从来没有停止过监视环球银行金融电信协会的金融交易往来信息。这意味着，在此期间美欧之间所有的谈判都只是表面功夫，没有实际作用。

2013年12月29日，德国《明镜》周刊称，美国国家安全局多年前就已攻破了主要公司开发的几乎所有安全架构，其中包括来自思科、华为、瞻博和戴尔的产品。

据媒体报道，美国还侵入了巴西国家石油公司的电脑网络。

二、美国把中国当成秘密监听的主要目标

斯诺登曝光的证据证明：中国是美国非法窃听的主要目标之一，窃听范围涵盖国家领导人、科研机构、大学、企业等等。

斯诺登向德国《明镜》周刊提供的文件表明：美国针对中国进行大规模网络进攻，并把中国领导人和华为公司列为目标。攻击的目标包括商务部、外交部、银行和电信公司等。

《明镜》周刊称，美国的监控目标还包括数位中国前任国家领导人和多个政府部门及银行。

中国的政府机构是美国窃听的重点关照对象。白宫的一位外交政策助理也曾透露，美国曾在1990年8月落成的中国驻澳大利亚新使馆的每间办公室的混凝土墙里埋设了光纤窃听器，这种细细的玻璃丝在全面安全检查中没有被发现。直到这件事在前些时候被泄露给《悉尼先驱晨报》和其他新闻媒体后，才引起中国的警觉。

美国《外交政策》杂志报道，美国国家安全局旗下设有一个"获取特定情报行动办公室"，1997年以来通过网络攻击行动获得包括有关中国情报在内的多项重要情报。

据德国《明镜》周刊报道，已被曝光的一份美国2010年的"监听世界地图"包含了世界90个国家的监控点，中国作为美国在东亚的首要监听对象，北京、上海、成都、香港及台北等城市，均在美国国家安全局重点监控目录之下。从2009年开始，美国国家安全局就开始入侵中国大陆和香港的电脑和网络系统，中国大陆和香港已有数百个目标受到监视。在香港的目标中，多数是大学、政府官员、商人和学生。

《南华早报》援引斯诺登的话说："美国国家安全局无所不用其极，利用非法侵入中国主要电信公司等手段，窃取用户的手机数据。"

《南华早报》称斯诺登爆料：美国国家安全局还对中国顶尖高等学府清华大学的主干网络发起大规模的黑客攻击。其中2013年1月的一次攻击中，至少63部电脑和服务器被黑。报道指出，中国六大骨干网之一的"中国教育和科研计算机网"就设在清华大学，"清华的主干网络被黑，意味着数百万中国公民的网络数据可能失窃"。

《南华早报》公布的对斯诺登的采访说，美国政府正大规模入侵中国的主要电信公司，以获取数以百万计短信内容。斯诺登表示，美国监控远不止这些，"美国国家安全局做各种事情，诸如入侵中国移动电话公司，以窃取你们所有的短信数据。"

据路透社报道，美国国家安全局曾与加密技术公司美国安全服务商RSA达成了1000万美元的协议，联合在加密算法中加入漏洞后门，旨在削弱软件加密标准，辅助相关机构RSA开展大规模监控程序。RSA的中国客户包括三大电信运营商中国电信、中国移动、中国联通，中国银行、中国工商银行、中国建设银行等，以及电信设备商华为和家电制造商海尔等。

美国《华盛顿邮报》依据斯诺登提供的多份机密文件爆料说，在2012年5月之前的一年间，美国国家安全局未经授权收集、存储、获取或分发受法律保护的通信信息多达2776次。其中2012年第一季度的非法操作次数增加尤其明显。报告说，原因可能在于2012年农历春节期间美国国家安全局非法监听访美的中国公民大量通话信息。

连网络游戏都成为了美国获取情报的渠道，英国《卫报》和《纽约时报》公布了美国著名新闻调查机构"为了人民"的文件，名为"对恐怖分子利用游戏和虚拟环境的研究"。该文件显示，美英两国的情报人员假扮"玩家"，曾渗透入网络游戏《魔兽世界》、《第二生命》中，收集真正电脑游戏玩家的纪录，监视游戏玩家。而实际上，这两款游戏的中国玩家最多。

针对中国的监控无孔不入：据媒体报道，斯诺登披露了一批机密文件，这些文件显示，腾讯聊天软件QQ和中国移动的移动即时通讯应用飞信竟然也在美国国家安全局的监视范围之内。

美国《外交杂志》说，美国一直就网络攻击问题施压中国之时，却从不提及美方大范围攻击中国网络的情况。而在中方指出美方动作时，面对媒体的求证，美国政府始终拒绝公开置评。

据德国《明镜》周刊网站、《纽约时报》网站报道，美国国家安全局尤其花大力气监控全球第二大通信设备供应商华为公司。2009年初，该局启动了一项针对华为的大规模行动。华为被视为美国思科公司最大的竞争对手之一。美国国家安全局的一个特别小组成功渗透进了华为公司的计算机网络，并复制了超过1400个客户的资料和工程师使用的内部培训文件。

报道称，该局人员不但窃取了华为的电子邮件存档，还获得了个别华为产品的源代码。美国国家安全局渗入华为的深圳总部，因为该公司通过总部处理每个员工的邮件往来，所以美国人从2009年1月起就读取了该公司很大一部分员工的电子邮件—包括公司高管的邮件。

美国情报部门说，如果了解了该公司如何运行，那么未来将会得到回报。迄今为止，网络结构由西方主宰，但中国人将努力使西方的公司变得"更不重要"。那样的话，迄今由美国公司主导的互联网技术标准将被打破，中国将逐步控制网络中的信息流。

美国《纽约时报》网站3月22日称，长期以来，美国官员一直将中国电信巨头华为公司视为安全威胁，竭力阻挠该公司在美国达成商业协议，担心它会在自己的设备中植入"后门"以便让中国军方或北京支持的黑客窃取企业和政府机密。不过，机密文件表明，美国国家安全局正直接向华为的网络植入自己的"后门"。

《纽约时报》报道指出，美国国家安全局对中国的情报活动并不仅仅局限于华为。根据2013年4月斯诺登曝光的文件，去年，美国国家安全局入侵了中国两家大型移动通信网络，从而得以追踪具有战略重要性的中国军方部门。

三、美国秘密监听不择手段

"棱镜"等项目的披露，凸现了美国在互联网时代监听项目多、投入大、范围广、时间长，情报机构、政府和私营企业间在监控上"无缝合作"，其大数据处理能力使得网络监听的广度和深度极大拓展。

1.项目之多、投入之大、范围之广、时间之长，无不是世界之最。

美国情报机构设立的与互联网监控直接相关的项目近十个，涵盖互联网、电信网，不仅有语音电话，也包括各种互联网信息，主要的互联网服务商都囊括在内。

由美国国家安全局兴建的犹他州大数据中心，是目前世界上最大的数据中心，投入20亿美元，其主要任务是通过秘密监控系统收集数据，然后由密码破译专家、数据挖掘人员、情报分析员进行深度处理后分析运用，以获取有价值的情报。

2013年8月30日《华盛顿邮报》披露的《2013财年国会预算论证》卷1—《国家情报项目摘要》显示：2013年美国情报预算翻番，高达526亿美元；网络行动预算占43亿美元，约占8%，任务显著侧重。自2007年9月11日开始从微软搜集信息算起，直到2012年10月开始从苹果搜集信息，此类美国情报机构与私营机构尤其是主要互联网服务提供商的监控合作，从来没有中断过，迄今已持续6年多时间。

德国《明镜》周刊报道了代号为"特等舱"的情报项目：美国、英国、澳大利亚和加拿大的驻外大使馆秘密安装了监控设备，用于截听电子通讯信息。这四个国家和新西兰共同签署了一份情报共享协议。

2.情报机构、政府、私营企业之间的秘密合作极其深入且愈演愈烈。

美国互联网主要的九大软硬件供应商都提供了很核心的技术支持，特别是微软最早与美国国家安全局合作，开放outlook、hotmail内部接口，甚至在outlook.com的加密系统正式发布之间就已将其提供给美国情报部门。曾声称其加密技术和P2P架构无法被政府"搭线接听"的Skype，在被微软收购后，主动为"搭线窃听"打开"后门"。微软还与情报部门合作，帮助其破解大公司编码，以便能够监控用户；微软经常在漏洞发布前告知情报机构，使他们能够利用时间差发起远程漏洞攻击。

3.利用强大的大数据处理和运用能力大幅提升监控范围和深度。

2012年3月，奥巴马政府将大数据战略上升为最高国策，认为大数据是"未来的新石油"，将对数据的占有和控制，作为陆权、海权、空权之外的另一种国家核心能力。而"棱镜"项目与美国大数据战略有着必然联系。美国国家安全局拥有一种名为"无边界情报员"系统，这套系统以30天为周期，可以从全球网络系统中接收到970亿条信息，再通过比对信用卡或通讯纪录等方式，能几近真实地还原个人的实时状况。

4.美国情报机构一直致力于或明或暗地寻找其国内法律漏洞，突破法律限制，谋求从源头和根本上控制网络信息。

"9·11"事件后，美国为了弥补通信情报收集的不足，开始建立监控项目的总统授权。

2001年10月4日，布什总统颁布授权备忘录，"在一定时期内开展特定电子监控行动"。此后，总统授权中的"国内收集"甚至一度被解释为允许对国内信息包括美国境内和美国人的通信信息进行收集。其后数年间，美国国内就这类行政命令的效力、范围和法律依据产生争议。但总体上，美国总统与国家安全局、联邦调查局、司法部等机构就针对外国目标收集信息的法律说明逐渐趋于一致。

2006年5月24日，国外情报监视委员会彻底改变了对《爱国者法案》第215条内容的解读方式，允许联邦调查局与国家安全局分享与恐怖事件调查相关的"商业纪录"，包括电话公司的电话纪录。自此，美国政府每3个月向大型电话公司下达数据索取命令。

2012年10月，奥巴马签署一项名为《美国网络作战政策》的总统指令，要求美国国家安全和情报官员制定一份美国可以进行网络攻击的目标名单。同时，指令规定，为实现美国在全世界的国家安全目标，美国可以动用独特的和非常规的武力，在事先不进行任何警告的情况下发动攻击。

荷兰《新鹿特丹商报》称，斯诺登披露的文件显示，美国国家安全局利用五种收集方式，在全球范围内开展情报收集行动。一份2012年的档案文件显示，五类情报收集方式包括：第三方/联络，即由美国国家安全局国际合作伙伴提供数据，其合作伙伴包括约30多个国家；区域获取，即以80多个区域为基础的专门收集服务行动，该行动是由美国国家安全局和中央情报局在黑色预算支持下开展的；网络入侵，该活动由美国国家安全局下属的获取特定情报行动办公室执行，已经在全球超过5万台计算机中植入了窃取敏感信息的恶意软件，主要目标为中国、俄罗斯、巴西、埃及、印度、墨西哥、沙特阿拉伯及东欧部分地区；大型电缆，即通过20个大型电缆主要节点获取信息，这些节点大多数位于美国境内；外国卫星情报收集，即拦截外国卫星处理的数据，如英国、挪威和日本。

“棱镜”事件反映出美国以国家安全局为主的情报机构，实施互联网信息监控和信息获取的主要手段和方法有以下三种：

—从光缆获取世界范围内的数据。全球的通信流量大部分经过美国，目标数据流可以很容易流入或流经美国。美国国家安全局与国防部等机构在2003年与美国环球电讯公司签署《网络安全协议》，此后的10年间，又与更多的电讯公司签署了类似协议。这些协议规定，电讯企业要在美国本土建立“网络运行中心”，美国政府官员可以在发出警告半小时内进入查访。与此同时，美国的盟友英国、加拿大等也为其提供光缆监听情报。

—直接进入互联网公司的服务器和数据库获取。“棱镜”项目相继与微软、雅虎、谷歌、脸谱、PalTalk、YouTube、Skype、AOL和苹果等9家互联网公司合作，大多数情况下，数据会通过这些公司的服务器以电子方式传输给政府，有时一些公司的服务器还会建立独立安全入口，以便于政府由此调取信息。情报人员可以直接进入上述公司的服务器和数据库获取数据，内容包括电子邮件、即时消息、视频、照片、存储数据、语音聊天、文件传输、视频会议、登录时间和社交网络资料等10类信息，甚至可以直接监控用户网络搜索内容。

—美国国家安全局的特别机构主动、秘密、远程入侵获取。美国国家安全局早在1997年就下设“获取特定情报行动办公室”，其主要任务是通过秘密入侵目标计算机和电信系统、破译密码、攻破受保护目标计算机的安全系统等，窃取存储在目标计算机中的数据，然后复制目标邮件系统中的所有信息和通过的数据流量，来获取境外目标的情报。美国国家安

全局描述这一系列行动的技术术语是"计算机网络漏洞利用侦察"，其实质就是网络攻击窃密。

四、美国全球监听受到广泛批评

"棱镜"计划曝光后，引发了包括美国盟友在内的全球范围对美国的批评。德国总理默克尔表示："我们必须信任我们的盟友和伙伴，而这种信任如今需要重新建立。"

美国国家安全局监控巴西总统罗塞夫和时为墨西哥总统候选人培尼亚·涅托的通信纪录，引发巴墨两国政府强烈不满。罗塞夫说："巴西政府坚决要求美国方面澄清……要求采取具体行动，彻底消除监视的可能性。"由于美方未在巴方要求时间内对监视行为作出解释，罗塞夫推迟对美国的国事访问。

巴西总统罗塞夫还谴责，美国出于"经济和战略"而非国家安全动机侵入巴西国家石油公司电脑网络。她说，美国的监视活动不是为安保或打击恐怖主义，而是为攫取经济和战略利益，"毫无疑问，巴西国家石油公司不对任何国家的安全构成威胁。"

为了绕开美国的网络监控，巴西将与欧洲之间铺设一条海底光缆。巴西政府还下令邮政局和联邦数据处理中心开发一套新的电子邮件系统，旨在防范他国的间谍行为，保障本国经济与政治安全。

2014年4月底在巴西圣保罗举行的互联网管理大会，焦点就是如何建立新的国际互联网治理秩序。一向标榜网络自由的美国尽管尽量低调，但仍不断被"呛声"。巴西总统罗塞夫在会议上不点名地批评美国说，"（在互联网治理中）多边参与是非常重要的。所有参与国家的政府都应该得到平等的、一视同仁的对待，而不是某一个国家比其他国家具有更大的话语权"，矛头直指美国政府对互联网监管机构的控制以及对其他国家的网络监控行为。俄罗斯尖锐地对美国进行了抨击，指责美"一国政府独掌"国际互联网名称和编号分配公司。俄方代表说，"这一现状令国际社会十分担忧"。

美国在马来西亚进行监听的消息曝光后，马来西亚外交部致函美国驻马大使表示抗议。马来西亚总理纳吉布说，监听涉及国家主权及原则问题，马来西亚政府坚决反对美国对马来西亚进行任何形式的监听行动。

九大主要国际公民自由联盟发表联合声明，认为美国联邦政府开展的秘密情报监视项目“棱镜计划”违反国际人权公约。联合声明指出“如此庞大而无孔不入的监视行为违反了隐私权和言论自由权两项最基本的人权。”

在美国本土，批评和抗议的声音此起彼伏。美国民权联盟官员严责美国国家安全局称，该局越权监控私人讯息，侵犯“美国人民生活的每个层面”。

有美国民权组织发表声明，对美国国家安全局如此大规模收集移动电话纪录表示抗议，对如此众多美国人的行踪遭到政府跟踪表示不安。美国公民自由联合会首席技术官克里斯·索格恩说：“在这种情形下，保护隐私权的唯一办法是切断所有现代通信手段，生活在一个山洞中。”

针对美国的全球监听行动，第68届联合国大会通过“数字时代的隐私权”决议，强调非法或任意监控、截取通信、非法搜集个人数据是对隐私权和言论自由的侵犯。一些国家在决议通过前发言，指责美国不仅侵犯隐私权等基本人权，也违背了尊重国家主权和领土完整、不干涉内政等《联合国宪章》宗旨和原则。

美国国家安全局监控华为的行动曝光后，华为在美国的一位高管威廉·普卢默说，华为不知道自己成为美国国家安全局的目标，“讽刺的是，他们对我们所做的，恰恰是他们一直指控中国方面通过我们所做的。”

“华盛顿正在失去其道德”，德国《焦点》周刊引述外交政策专家的评论称，“多年来美国一直以”中国间谍和黑客攻击”为由向中国施压。而实际上，美国自己才是窃听者。”德国新闻电视台称，美国几乎在全方位监听“整个中国”，“说到底，这是因为美国害怕中国超越自己成为世界超级大国。”

斯诺登表示，美国政府“宣称（监视行动）不会针对民间设施”。“棱镜”项目曝光，目的就是揭露美国政府的“伪善”。