监视帝国

棱镜掌握一切

东鸟 著

MONITORING

中南出版传媒集团
湖南人民出版社

监视帝国

棱镜掌握一切

我们相信上帝，我们监视其他所有人。
——美国国家安全局

东鸟 著

MONITORING

中南出版传媒集团
湖南人民出版社

图书在版编目（CIP）数据

监视帝国 ：棱镜掌握一切 / 东鸟著. -- 长沙 ：湖南人民出版社，2013

ISBN 978-7-5438-9671-0

Ⅰ. ①监… Ⅱ. ①东… Ⅲ. ①计算机网络－安全技术 Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2013)第189175号

出　　版：中南出版传媒集团·湖南人民出版社
（地址：长沙市营盘东路3号 410005）
经 销 者：全国新华书店
印 刷 者：北京中印联印务有限公司
开　　本：700×960　1/16
字　　数：200000
印　　张：16.75
出版时间：2013年9月第1版
印　　次：2013年9月第1次印刷
出 版 人：谢清风
责任编辑：曾赛丰
特约编辑：刘　丹
封面设计：尚世视觉
美术编辑：靳　莹
ISBN 978-7-5438-9671-0
定　　价：35.00元

发　　行：中南出版传媒集团·北京涌思图书有限责任公司
（地址：北京市朝阳区安定路39号长新大厦1001室　100029）
联系电话：010-64426679
邮购热线：010-64421810
传　　真：010-64427328
公司网址：www.yongsibook.net
投稿邮箱：pd@yongsibook.net

序　言

美国公民斯诺登曝光“棱镜”网络监视项目，不仅在美国国内激起轩然大波，而且在国际社会掀起舆论风暴，甚至在美国与中国、俄罗斯、拉美、欧洲等国际关系间暗涌政治风浪。

说到“棱镜”和斯诺登，就不得不提到维基解密和阿桑奇。两年前，阿桑奇和他的维基解密网站曝光美国政府大量机密文件，至今阿桑奇仍在厄瓜多尔驻英国大使馆避难，过着不见天日的日子。向阿桑奇泄露美国政府机密文件的“深喉”，25岁的美国陆军情报分析员曼宁，也深陷牢狱之灾，被法院判定间谍罪、盗窃罪和计算机诈骗罪等20项罪名，最高有可能面临140年的刑罚。

如今身处俄罗斯避难的斯诺登，也面临阿桑奇的困境和曼宁的刑罚。不过，这次如鲠在喉的美国政府，对斯诺登的痛恨远远要超过阿桑奇和曼宁，欲置之死地而后快，手段无所不用其极。因为斯诺登打到了美国政府的“七寸”，“毁三观”地颠覆了美国政府的形象，使美国政府成为“全民公敌”，被称为“老大哥”。

对于全球情报界来说，“棱镜”不算是什么秘密。如果算是秘

密，也是一个公开的秘密，只是秘而不宣而已。早在20世纪90年代，美国情报部门的电话和网络监视技术就取得突飞猛进的进展，可以将实时监视的速度提升到惊人的10的10次幂。当时，这种技术被称为“实时区域之门”，通过技术手段可以将所有数据自动存储，并分发给情报分析师。利用“实时区域之门”，情报分析师可以截取电子邮件、监听他人电话，并对各类电子数据进行筛选和分类。美国情报部门甚至可借助这些监视数据，对其他国家计算机网络系统和电话通讯系统发动攻击。

“9·11”事件后，美国情报部门的监视行为更加肆无忌惮。恐怖袭击发生不到1个月，10月4日，时任美国总统小布什就批准了“恐怖分子监视计划”，授权美国国家安全局不必申请法庭授权，就可监视“基地”组织的通话。美国国家安全局通过这种方式，获得了大量电话号码、电子邮件和姓名地址。由此，美国政府利用先进的信息技术，复活了美国冷战期间滥用监视的幽灵。2005年12月，《纽约时报》不知从何处搞到了美国监视项目的材料，并对外公开了一些行动信息，引起舆论和民间团体的激烈抨击。但是小布什辩称监视行动对预防恐怖袭击非常必要，从而有惊无险地化解了这次危机。

但是，这次曝光“棱镜”不同，其所引发的舆论反响和政治风波，是此类事件前所未有的。因为美国政府“窃听美国”、“窃听欧盟”、“窃听亚洲”、“窃听世界”，涉及美国和全球互联网用户的隐私问题，牵涉到俄罗斯、欧洲、拉美、中国内地和香港，舆论的焦点不仅有隐私保护、网络安全问题，还涉及中国、俄罗斯等世界主要大国的国家利益和政治博弈以及国际互联网治理问题。从事件性质演变看，“棱镜门”逐渐偏离美国网络监视这个舆论焦点，演变

为一起涉及世界主要大国的政治性事件。虽然从目前发展态势看，“棱镜门”不可能对美中、美俄关系产生大的影响，但是其毕竟在这些大国之间产生了小的波浪，对大国关系会产生一些微妙的影响。而且，斯诺登掌握了涉及美国国家安全的大量重要情报，不可避免成为一些国家政府和组织重要的政治筹码。从国际互联网治理看，“棱镜门”凸显出美国政府和企业对全球网络空间的控制力和垄断性，而中国、俄罗斯等发展中国家则处于被动地位。一些新兴市场国家可能会借机参与国际互联网治理，推动制定更加公平、安全、合理的国际互联网治理规则。

目前，美国政府及其互联网企业，已经建立了一个可以偷窥一切的监视帝国，知道我们的一切，操控我们的一切。早在2002年，美国联邦调查局就开始在追踪犯罪嫌疑人时使用麦克风窃听技术。2004年，又推出一个名为“流动漏洞”的项目，专门在案件调查中使用以进行窃听。2007年，谷歌公开承认，它们一直存储着每一位用户曾经键入的每一次搜索请求，以及每一位用户随后点击访问的每一条搜索结果。我们在网上每一句言论、每一个访问，都会被互联网企业及其美国情报部门存储，永久记录在案。

《大数据》一书的作者舍恩伯格，在他的另一本书《删除》中，讲述了一个故事。一位60多岁的加拿大心理学家费尔马德，计划穿过美国和加拿大的边境去接一个朋友，这类事情他已经做过上百次。但是这一次，美国边境守卫突发奇想，“谷歌”了一下他的情况，结果发现费尔马德5年前发表在一个小众杂志上的文章，提到自己在30多年前曾经服用过致幻剂。因此，费尔马德不仅被扣留4小时，还不被允许入境，甚至被迫签署声明表示自己服用过致幻剂，所以再也不被允许入境美国。谷歌记住了我们希望忘记可能已经忘记的

一切。美国政府凭借全球垄断的互联网企业，把全球民众的一举一动全部存档，毫无删除的可能性，随时可能成为对我们“不利的证据”。

2013年7月，波士顿爆炸案发生后几个月，纽约萨克福马县一对夫妻因为妻子用谷歌搜索了“高压锅”，丈夫同一时段用谷歌搜索了“背包”，就遭到一个六人组成的联合反恐部队，以“查水表”为名的上门盘问。联合反恐部队盘问他们：你们有炸弹吗？你们有高压锅吗？什么只有电饭煲？能拿来做炸弹吗？为什么美国政府知道这对夫妻用谷歌搜索“高压锅”和“背包”的情况？这自然要归功于“棱镜”和谷歌的监视。类似的上门“查水表”，联合反恐部队竟然每周要有100次。

可叹的是，虽然“棱镜”违背美国标榜的“自由”价值观，揭穿了“网络自由”的虚伪，完全使美国失去以往的道义制高点，但是美国两党和议会甚至媒体，都力挺美国政府的监视行为。除了少数发展中国家外，欧洲、日韩都没有出现集中质疑和反制行动，各国民间要求建立公正合理网络秩序的声音也被西方压制，一些西方政客和媒体甚至把脏水泼向“棱镜”的受害国中国。这无疑又是一个“毁三观”的事情。

目前，斯诺登事件还在发酵之中，有关国家围绕斯诺登何去何从问题还将进行艰苦博弈，俄罗斯显然不会把斯诺登引渡回美国，但允许斯诺登政治避难一年也会让美俄关系横生枝节。光明磊落的斯诺登，却要面临像阿桑奇一样的命运，永远不能光明正大地出入于市井，只能藏匿于不见阳光的暗处。本是“全民公敌”的美国情报部门，本是见不得光的“棱镜”，却可以堂而皇之地监视着我们的一切。

目 录

Contents

第一章 斯特拉

“棱镜”曝光引发全球轩然大波，但这只是美国庞大监视计划的冰山一角。“棱镜”项目源自一个更为秘密的“斯特拉之风”计划，包括“大道”、“码头”、“核子”等鲜为人知的秘密监视项目。

■ 星风

“棱镜”项目源自一个从未公开过的“斯特拉之风”(Stellar Wind)计划，我国也译做“恒星风”或“星风”，在美国情报界圈内称之为“那个计划”。“星风”是恒星表面发出的物质流，是恒星质量流失的一种主要方式。我们最易观察到的“星风”就是太阳风(Solar Wind)。据说，“星风”这个名字出自旅居美国的日本作曲家锋山亘，为2006年的美国电影《左手是天使，右手是恶魔》所创作的主题曲。用它代称美国政府的监视计划，可谓再贴切不过了。

“星风”计划，最早可溯源到1994年。这一年的10月，美国国会通过《法律执行通讯协助法案》(CALEA)，要求所有电信运营商和电信设备制造商（包括硬件和软件）限期完成修改和设计设备、设施、服务，以保证提供内置对电话、宽带互联网、VoIP的实时监视能力。这为实施“星风”计划提供了法律依据。但在当时，《法律执行通讯协助法案》并不适用于互联网服务，比如电子邮件，也不能够针对互联网服务商。美国联邦调查局曾试图将互联网服务也纳入法案适用范围，但国会最终并没有买账。

2001年，“9·11”恐怖袭击事件后，如何避免遭受恐怖袭击成

为美国情报部门的工作重心。美国国家安全局提出了一个“关系链”概念，试图在信息海洋中筛选出有价值的信息，提前获取“敌人”的动向。不久，时任美国总统小布什就开始强化“信息监视”，秘密授权国家安全局直接接入光纤进行数据监视，这项行动被称为“恐怖分子监视计划”，目的是要监视“问题号码”，因为情报人员有理由相信这些号码属于基地组织成员。号码很多来自在战场上被捕的恐怖分子的手机或计算机。

在《抉择时刻：布什自传》这本书中，小布什回忆，由于威胁十分紧迫，我让白宫法律顾问办公室和司法部去研究我能否授权国家安全局，在没有获得外国情报监视法庭授权情况下，监视“基地”组织打入和打出美国的通话。得出的结论是：在战时对敌人进行监视，符合国会战争决议以及宪法赋予总统为战时总司令的权力。原本考虑拿到国会立法，但两党重要议员均认为监视是必要的，如果对此项目立法辩论，我们的方法就会暴露给敌人。于是我下令推进这一计划。

同时，美国国会制定《爱国者法案》，颁布《国土安全法》，修改 1978 年《外国情报监视法案》，允许政府机构运用特定信息系统，监视特定范围内信息流动以及用户活动。其中，2001 年 10 月通过的《爱国者法案》有三项规定最为关键：允许情报或执法部门在监视对象改变通讯工具后，无需重新获得授权即可对新的通讯工具进行监视；允许相关部门向个人或公司索取被认为对调查至关重要的文件或记录；允许相关部门追踪并非隶属某一恐怖组织、独自行动的外国恐怖嫌疑人。

简单地说，这些法案允许国家安全局、中央情报局、联邦调查局以及其他情报部门，对通过电子监视获取的情报信息共享，并授

权在特定情况下，可不经法院签发令状而实施互联网秘密监视。美国情报机关只需要向外国情报监视法庭（FISC），说明监视技术和监视的目标，不需要申请搜查证，就可在一定程度上实现“无证监视”。由此，外国情报监视法庭已悄无声息地变成一家几乎与最高法院（Supreme Court）平起平坐的法庭，对监视问题拥有最终裁决权，并下达极有可能影响未来情报工作的裁决意见。

外国情报监视法庭组建于 1978 年，负责审核和授权对外的情报监视，作为对政府滥用监视权力的一种制约。这个特殊法庭由 11 名成员组成，他们会在华盛顿联邦法院一间无明显特征的房间会面。法庭的法官以七年为一个任期，所有 11 名现任法官都是由首席大法官小约翰·G. 罗伯茨任命，其中 10 名由共和党主席提名。他们中多数来自华盛顿以外的司法辖区，轮流裁决情报部门的监视申请。多数监视裁决只需由一名法官单独签署即可。仅 2012 年，法庭就发出近 1800 项裁决。而且，该法庭以十多项机密裁决，建立了一个秘密的法律体系。有的裁决书长达近 100 页，法庭经常就宽泛的宪法问题给出评价，甚至制定重要判例，担负起一个更加广泛的角色，几乎不受民众监督。

“9·11”事件后，外国情报监视法庭在几个判决中，把所谓“特殊需要”原则在恐怖主义案件中的应用进行了扩大，开创了美国宪法第四修正案的一个例外。第四修正案规定要有搜查令才能搜查和没收。“特殊需要”原则最初是 1989 年由最高法院确立的。在当时的裁决中，最高法院裁定允许对铁路工人进行药检，最高法院认为政府为防范重大公共危险，对隐私权做出最低程度的侵犯是合理的。外国情报监视法庭对这个原则做了更宽泛的延伸，裁决国家安全局搜集和检查美国人的通讯数据是用于追踪可能的恐怖分子的，并不

违反第四修正案。他们认定，单纯搜集像通话时间、电话号码等事实，而不搜集交谈内容，并不违反第四修正案，只要根据国家安全法规提出一个合理的理由就可以。

有了法律和法庭的支持，美国国防部 2002 年推出一个名为“全面信息感知系统”项目，以互联网加上路面以及街旁摄像头的方式，尝试对全美实施有效监视，配合策略识别系统，识别潜在的恐怖分子嫌疑人，但受到美国民众的强烈反对。

小布什并没有因此而挫败，开始秘密策划一个名为“星风”的更加庞大的监视计划，可记录美国民众的通讯活动，包括电子邮件、电话通话、金融交易和互联网活动。但是，小布什再次遭遇挫折。2004 年 3 月，在司法部部长约翰·阿什克罗夫特住院期间，以代理司法部长詹姆斯·科米为首的众多司法部高官拒绝授权，认定未经许可的部分监视项目属非法，但主要是反对有关监视互联网的项目。因为，当时很多通话是通过即时通讯软件的语音功能以及网络电话完成的，美国情报部门希望人们忘记《法律执行通讯协助法案》的细节规定，将法案适用范围扩大到互联网服务领域。但是，美国司法部的高官们，最后以集体辞职方式反对“星风”计划。

3 个月后，小布什耍了一小花招，通过司法程序，由外国情报监视法庭授予国家安全局等情报部门全面监视电话通话和互联网通讯的权力，监视对象不仅限于恐怖主义嫌疑人，还包括涉嫌参与核扩散、谍报和恐怖袭击的人，从而成功绕开美国有关公民隐私的法律困境。但是，外国情报监视法庭裁决的法律依据，至今仍是机密。

为避免“星风”计划遭遇更大阻力，小布什也被迫做出一些让步，缩减了在美国本土的监视项目。为此，小布什将“星风”分拆成秘密执行的四个监视项目，除“棱镜”外，还包括“大道”

(Mainway)、“码头”(Marina)和“核子”(Nucleon)。但这些也只是项目的代号，其具体名称及含义仍被列为美国国家机密。

“大道”和“码头”的规模十分庞大，分别对电话通话和互联网上数以亿兆计的“元数据”(Metadata)进行存储和分析，但不会窃听通话和网络内容。“核子”和“棱镜”的规模要小得多，监视的范围并没有前两者那样广泛，主要专注信息内容，分别负责截取电话通话内容和互联网内容。四合一的“星风”计划，就像一个巨大的吸尘器，将全球通讯网络一网打尽，并秘密储存下来分析。

为了将“星风”合法化，美国国会2008年通过了《外国情报监视法修正案》(FISA)。法案“第702条”允许美国政府可以搜集电子通讯信息，以获取有关对美国国家安全构成威胁的外国目标的情报，这成为了今天美国情报部门肆意监视的法律依据。同时，法案规定，对外国情报监视法庭可以授权公司提供所有相关信息、设施以及必要的帮助。作为回报，提供信息和帮助的公司将得到补偿，例如可在一些潜在诉讼中获得豁免权。该法案还将“外国情报”的定义进行扩展，把“大规模杀伤性武器”也列入其中。这使情报部门能更加便利地获取他们认为可能与核扩散相关、范围更广的数据和通讯内容。

外国情报监视法庭也表态支持，强调一些数据单独来看似乎与恐怖行动调查不存在“关联”，但事实上这些数据综合起来所展示的情况却可能是相关的。而且，外国情报监视法庭在作出有关裁决时，只会听取一方的意见：情报部门，裁决结果也几乎从不公开，当然也不会向有关公司透露任何有关调查的细节。如此，对于政府部门的协查要求，各大公司都会大力配合，因为他们不希望妨碍可能有助于避免恐怖袭击的调查。当外国情报监视法庭接到申诉时，

也会组成一个复核法庭来听取申诉。外国情报监视法庭 1978 年成立以来，只推翻过 11 次政府部门的监视请求，仅仅占全部裁决的 0.03%。

这导致“星风”计划被滥用，效率也不高。依据“星风”计划监视情报立案的案件，甚至被联邦调查局的探员称为“比萨案件”(Pizza Cases)，因为许多看似可疑的案件不过是比萨外卖订单而已。“星风”计划截取的信息中约有 99% 是没有任何价值的垃圾信息。但是，国家安全局辩解称其得担心的是其余 1% 的数据。这些 1% 的数据，用途之一就是创建关于有恐怖活动嫌疑的人的可疑活动报告。当然，也正是“星风”计划的类似监视报告，揭露了纽约州前州长艾略特·斯皮策嫖娼的事实，虽然他从未涉嫌参与任何恐怖活动。

■ 散拍

奥巴马当选美国总统后，继续执行小布什的“星风”计划。不过，这位美国首位黑人总统，立刻将“星风”计划改名为“散拍”(Ragtime) 计划。“散拍”也译作“拉格泰姆”，是一种美国流行音乐形式，采用黑人旋律，依切分音法循环主题与变形乐句等法则，结合而成的早期爵士乐，流行于第一次世界大战前美国经济繁荣时期。如今，它不但在黑人乐手与乐迷间流行，也被美国白人中产阶级所接受。

看来，“星风”改名为“散拍”有其内在必然性。不过，此时“散

拍”的监视对象已不再是外国人。其对内搜集活动，即针对美国国内民众的情报搜集活动，都会使用一个代号“RAGTIME-P”，其中的“P”代表《爱国者法案》(Patroit Act) 中的“爱国者”(Patroit)。在最近一个案例中，美国情报部门截取了一份在美国境内发送的电子邮件附件，因为他们担心电子邮件附件中含有可能与伊朗核计划有关的规划草图或图表。由此，“散拍”可以帮助奥巴马政府秘密解读、记录和存储世界通讯往来的每一个字节。

在全球反恐名义之下，奥巴马继续扩充着全球监视计划，以实现对全球现代通讯的有效监视。2011 年 5 月，奥巴马签署命令，将《爱国者法案》延长 4 年。2012 年 12 月，奥巴马再次签署命令，同意将《外国情报监视法案》延长 5 年。互联网是没有边界的，监视行为也变得没有了边界。一封从巴基斯坦发送给阿富汗的电子邮件沿着光纤传输，可是另一头的接收者可能不仅仅是美国电子邮件服务商的服务器，还会有一台美国政府的监视设备。“散拍”的监视对象是包括美国民众在内的世界每一个人。而且，美国政府部门不会定期删除储存的资料，所有数据都会被封存，意味着所有内容都可被追溯，甚至在 100 年后还可以进行分析。

在“散拍”计划执行中，有数千家科技、金融和制造业公司与美国情报部门密切合作，向其提供敏感信息，包括设备、说明、零日攻击漏洞以及客户私密信息。当然，这种合作是会有回报的，合作公司可以获得访问机密情报等好处。例如，情报部门通过“散拍”计划获得一些情报，会尽快向合作公司发出可能影响其盈利的网络威胁预警，甚至直接告诉网络攻击的幕后操纵者。2010 年，谷歌声称该公司遭到来自中国黑客的攻击。据说，是因为谷歌联合创始人谢尔盖 · 布林从美国情报部门获得高度机密的相关信息，