国家安全译丛
NATIONAL SECURITY 总策划 王吉胜

DATA AND GOLIATH

# 数据与监控

## 信息安全的隐形之战

## The Hidden Battles to Collect Your Data and Control Your World

大数据时代生存手册

[美] 布鲁斯·施奈尔（Bruce Schneier）◎著　李先奇　黎秋玲◎译

全民监控时代，我们如何保护自己的数据安全不被侵犯？

信息安全教父倾囊相授　反监控实战必读参考书

金城出版社
GOLD WALL PRESS

国家安全译丛
NATIONAL SECURITY 总策划 王吉胜

# 数据与监控

## 信息安全的隐形之战

全新
中文译本

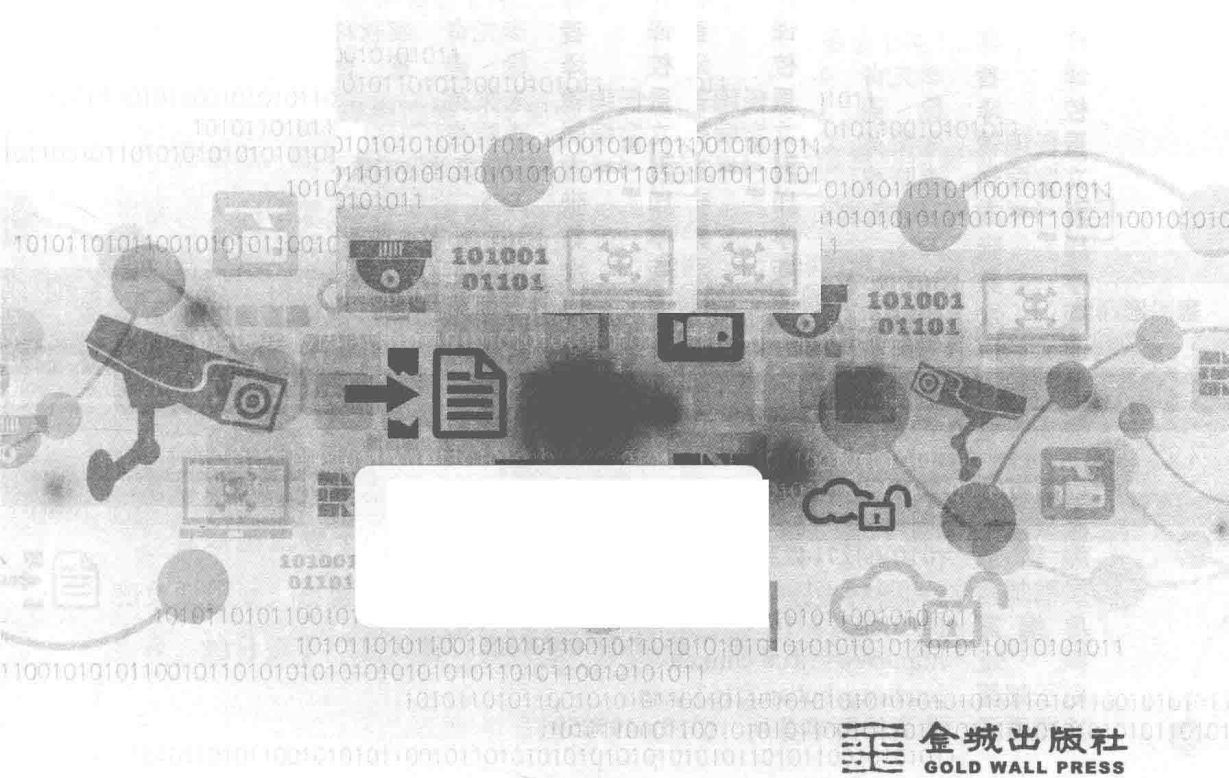
# DATA AND GOLIATH

## The Hidden Battles to Collect Your Data and Control Your World

[美] 布鲁斯·施奈尔（Bruce Schneier）◎著

李先奇　黎秋玲◎译

徐谦　董俐　王砚　张笑然　仇志华　李晨林◎校译



金城出版社
GOLD WALL PRESS

**图书在版编目（CIP）数据**

数据与监控：信息安全的隐形之战 /（美）布鲁斯·施奈尔 (Bruce Schneier) 著；李先奇，黎秋玲译 . —北京：金城出版社，2017.2
（国家安全译丛 / 朱策英主编）
书名原文：Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World
ISBN 978-7-5155-1446-8

Ⅰ. ①数… Ⅱ. ①布… ②李… ③黎… Ⅲ. ①信息安全 Ⅳ. ① TP309

中国版本图书馆 CIP 数据核字（2016）第 303948 号



**数据与监控：信息安全的隐形之战**
SHUJU YU JIANKONG : XINXI ANQUAN DE YINXING ZHIZHAN

| | |
|---|---|
| 作　　者 | [美] 布鲁斯·施奈尔 |
| 译　　者 | 李先奇　黎秋玲 |
| 校　　译 | 徐　谦　董　俐　等 |
| 责任编辑 | 朱策英 |
| 文字编辑 | 李晓凌 |
| 开　　本 | 710 毫米 ×1000 毫米　1/16 |
| 印　　张 | 23.5 |
| 字　　数 | 361 千字 |
| 版　　次 | 2018 年 1 月第 1 版　2018 年 1 月第 1 次印刷 |
| 印　　刷 | 三河市百盛印装有限公司 |
| 书　　号 | ISBN 978-7-5155-1446-8 |
| 定　　价 | 78.00 元 |

| | |
|---|---|
| 出版发行 | **金城出版社** 北京市朝阳区利泽东二路 3 号　邮编：100102 |
| 发 行 部 | (010)84254364 |
| 编 辑 部 | (010)64271423 |
| 投稿邮箱 | gwpbooks@yahoo.com |
| 总 编 室 | (010)64228516 |
| 网　　址 | http://www.jccb.com.cn |
| 电子邮箱 | jinchengchuban@163.com |
| 法律顾问 | 陈鹰律师事务所　(010)64970501 |

# 赞 誉

《数据与监控》一书是独一无二的。除大量曝光网络战、数据泄露和企业窥探的故事之外，斯诺登的爆料让许多人对如何保护自己的隐私感到困惑与怀疑。我希望布鲁斯·施奈尔的新书会让人加入到法庭和其他地方的对话中，讨论如何严肃而诚实地思考我们目前的数字监控状态，更重要的是，如何建立一个让被统治者赞同的数字社会。

——辛迪·科恩（Cindy Cohn），电子前线基金会法务总监

布鲁斯·施奈尔的这本书介绍了大数据和大规模监控如何影响人们的生活，人们该怎么办。这是一部非常有见地的重要作品。按照施奈尔一贯的独特风格，他选择了非常复杂而且不断变化的信息和思想，并使它们精彩生动、容易理解和令人信服。

——杰克·戈德史密斯（Jack Goldsmith），小布什执政时期司法部法律顾问办公室主任

互联网正处于一种监控状态，和其他任何技术一样，监控也有正面和负面作用。布鲁斯·施奈尔借助大范围的技术和历史技能，将它们整理出来。他分析了“老大哥”和许多“小兄弟”带来的挑战。在这个网络时

代，任何对安全、自由、隐私和公正感兴趣的人都必须阅读本书。

——约瑟夫·奈（Joseph S. Nye Jr.），哈佛大学著名教授，
《权利的未来》（*The Future of Power*）一书作者

布鲁斯·施奈尔在我们当下这个时代，一直都代表着安全和隐私方面最清醒、最权威和最渊博的声音。《数据与监控》将他的经验和敏锐的分析技能引入到重要而快速发展的技术和人权问题上。关于政府、金融机构和在线实体收集数据已经被讨论了很多，但对这些看似无限的海量数据的使用，或者可能被使用，讨论得却少之又少。面对这样一种笼罩在保密上的巨大可能性，施奈尔发出的是一种理智的声音。

——塞尼·贾尔丁（Xeni Jardin），BoingBoing 网站联合主编

《数据与监控》对于我们理解，目前在民主市场社会中对自由的最主要威胁，是必不可少的指南。在后斯诺登时代，不管你是否担心政府监控，或者是否担心脸书和谷歌公司基于他们搜集的大量个人信息来暗中控制你，施奈尔这位领先的独立专家为当下人们面临的这些威胁提供了丰富的技术和实践观点，引领我们走向监控社会，并提供了拯救命运的多样化解决方案。

——尤查·本科勒（Yochai Benkler），哈佛大学法学院伯克曼企业法教授，《网络财富》（*The Wealth of Networks*）一书作者

数据、算法和思维机器给企业和政治机构带来巨大而深远的权力。在打破这些权力对我们的隐私、生活和社会的影响上，布鲁斯·施奈尔已经做了非常了不起的工作。《数据与监控》应该列入我们每个人的必读书目。

——奥姆·马利克（Om Malik），美国科技新闻网站 Gigaom 创始人

# 目录

## 第二部分　问题的关键所在

# 第三部分　如何应对

# 前　言

如果你想要确信你生活在一个科幻世界，那么看看你的手机吧。这个可爱、美观且功能强大得令人难以置信的工具，已经理所当然地成为我们生活的中心。无论你在地球的哪一个角落，从口袋中掏出手机，就可以用它和这个星球上的任何一个人通话，这是再普通不过的事情。

但是每天早晨，当你把手机放进口袋时，你已经私下和通信公司达成了一项协议："我要拨打和接听移动电话；作为交换，我同意让这家公司全程知道我的位置。"这个协议没有出现在任何合同规定里，但它固化在通信公司的服务过程中。你可能都没有想过这个问题，但现在我把它指出来，你也许会认为这是个还不赖的协议。手机真的很奇妙，除非移动通信公司知道你的位置，否则它无法提供服务，这意味着你处于它的完全监控之下。

这是一种非常密切的监控。手机跟踪你生活和工作的地方；它追踪你喜欢度过周末和夜生活的地方；[1] 它跟踪监控你多久去一次教堂（去哪个教堂），你在某个酒吧泡了多长时间，驾车是否超速。它还可以掌握你附近所有的其他手机，可以跟踪你和谁在一起，和谁见面吃午饭，和谁睡觉。把这些数据累积起来进行分析，可能会比你自己更加全面地掌握这一天你是如何度过的，因为它不依赖于人的记忆。[2] 2012 年，研究人员就能用这些数据来预测 **24 小时后**你会出现在哪里，精确度在 20 米以内。[3]

在手机出现之前，如果有人想要掌握你的行踪，他将不得不雇佣私

家侦探跟踪你并不断做记录。现在，则完全不必如此；你口袋里的手机能自动完成这一切。也许没有一个人会检索使用这些信息，但事实上它就存储在那里。

你的位置信息非常有价值，每个人都想获得它。警察也想要它。**手机定位分析**是刑事调查方法中很有效的一种方式。[4] 警察通过“ping”[1]一个特定电话来确定手机的位置，使用历史数据来确定它曾经去过哪里，通过搜集某个特定区域的所有手机位置的历史数据来确定谁、什么时间曾在那里出现。[5] 警方正越来越多地使用这些数据来准确达到他们的目的。[6]

政府也使用同样的数据进行恐吓和社会控制。2014 年，乌克兰政府对一定时间内手机在某个特定区域的基辅人发送明确的“奥威尔式”短信：“亲爱的用户，您已被登记为大规模骚乱事件的参与者。”[7] 不要认为这种行为仅仅出现在极权主义国家；2010 年，密歇根地区的警察搜索了所有可能出现在一个预期的劳工抗议场地附近的手机信息。[8] 他们不需要先拿到搜查令。

对个人的实时跟踪已经形成了一个完整的产业链。这些公司通过手机跟踪来了解你在商店如何购物，根据你正在走的道路可以确定你离某个特定商店的距离，根据你当下所处的位置就能向你的手机发送广告。[9]

你的位置信息对手机公司是非常宝贵的，他们把这些数据卖给数据代理人，然后再被转手卖给任何想要购买这些信息的人。[10] 像感觉网络（Sense Networks）这样的公司专注于用这些数据来建立我们的个人档案。[11]

电话公司并不是手机数据的唯一来源。美国慧锐公司（Verint）销售手机跟踪系统给全球的公司和政府部门。[12] 该公司的网站上介绍，它是“一家为用户参与优化、安全情报、欺诈行为、风险管控等提供可操作的智能解决方案的全球领导企业”，客户“涵盖 180 多个国家的 10000 多个组织”。[13] 英国科巴姆公司（Cobham）销售的一套系统，允许某个人给一

[1] 编注：Ping 是 Windows、Unix 和 Linux 系统下的一个命令。利用它可以检查网络是否连通。

部电话发送“盲”呼叫——电话不会响，也不会被察觉。[14] 这个“盲”呼叫会强制电话转到某个特定的频率，让发送者可以跟踪这部电话精确度在1米之内。这家公司说，他们的客户包括阿尔及利亚、文莱、加纳、巴基斯坦、沙特阿拉伯、新加坡和美国。[15] 防御技术公司（Defentek），这是一家在巴拿马注册的神秘公司，销售可以“定位和跟踪世界上任何一部电话……不被网络、载波或者其他目标探测和知晓”的系统。[16] 这绝不是无聊的炫耀；电信研究员托拜厄斯·恩格尔（Tobias Engel）在2008年的黑客会议上演示了同样的事情。[17] 犯罪分子今天也正做着同样的事情。

所有的位置跟踪技术都是基于蜂窝系统。还有一个完全不同且更精确的定位系统已经内置于你的智能手机：GPS模块。这个模块向你手机上运行的各种APP应用程序提供位置信息。一些APP应用程序使用位置信息来提供服务：如谷歌地图、优步（Uber）、Yelp。其他像“愤怒的小鸟”这类应用程序只是想搜集、出售这些信息。[18]

你也可以这样做。HelloSpy是一个应用程序，你可以偷偷地安装在其他人的智能手机上去跟踪她。[19] 对于一个急迫想要窥探其未成年孩子的妈妈，或一个想要窥探自己的妻子或女友的男人而言，这类应用程序非常完美。[20] 雇主可使用类似的应用程序来监视他的员工。[21]

美国国家安全局（NSA）和它的英国同行——政府通信总部（GCHQ），使用位置信息来进行跟踪。国家安全局通过各种渠道搜集手机定位数据：手机连接的发射基站、手机登录的Wi-Fi网络位置和来自互联网应用程序的GPS定位数据。[22] 国家安全局代号为HAPPYFOOT和FASCIA的两个内部数据库，包括全球设备的综合位置信息。国家安全局用这两个数据库来跟踪人们的活动，确定人们之间交往的兴趣和无人机袭击的目标。

即使手机关机，国家安全局也能追踪到。[23]

刚才讨论的只是从手机这一渠道来获取位置信息，但问题远不止如此。在你与计算机不断交互的过程中会产生和你个人密切相关的数据，包

括你读的、看的、听的所有信息，也包括你和谁，交流了什么。最终，它涵盖了所有你正在思考的内容；至少在某种程度上，你思考的内容引导你在互联网上进行搜索。所以，我们正生活在一个监控的黄金时代。[24]

Sun Microsystems（SUN）公司CEO斯科特·麦克尼利（Scott McNealy）[1]早在1999年就明确指出："你根本没有任何隐私。忍受它吧！"[25]对于我们该如何应对监控，他是错误的，但他认为避免监控、保护隐私将会越来越困难的观点却是正确的。

监控是一个满载着政治和情感的术语，但我特意使用了它。美国军方定义监控为"**系统观察**"（systematic observation）。[26]正如我的解释，现代的电子监控确实是这样的。对政府和企业而言，我们都是公开的书本；他们窥视我们集体生活的能力比以往任何时候都强大。

你一次又一次和不同的公司做交易，就是以被监控来换取享受免费服务。谷歌公司董事长埃里克·施密特（Eric Schmidt）和公司"思想引领者"贾里德·科恩（Jared Cohen）在他们2013年合作出版的《新数字时代》（*The New Digital Age*）一书中将这种情况和盘托出。在这里我引述他们的原话：如果你让我们拥有你所有的数据，我们将向你展示你想看的广告，我们将之投放到免费的网络搜索、电子邮件和其他各种服务中。[27]总而言之，它非常方便。我们都是社会性动物，没什么比与其他人交流更有魅力或更有成就感。数字，意味着沟通已经成为最容易和最快捷的方式。然而，为什么我们允许政府获取这些信息呢？因为我们害怕恐怖分子，害怕陌生人绑架我们的孩子，害怕毒贩，害怕此刻坏人逍遥法外。这就是国家安全局设立大规模监控项目的理由；如果你让我们拥有你所有的数据，我们就能减轻你的恐惧。[28]

问题是，这些并不是好的或公平的协议，至少发展到目前，它们已经

[1] 编注：斯科特·麦克尼利（1954— ），SUN公司CEO。1984—2006年，他带领SUN走上持续创新的开放式网络计算之路，使SUN公司成为全球领先的网络计算基础设备供应商。

被结构化了。我们正轻易地接受，但并没有真正理解这些条款。

事实就是如此。今天的技术给政府和企业提供了强大的大规模监控能力。大规模监控极其危险。它允许存在基于种族、宗教、阶级和政治信仰等几乎任何标准而导致的歧视。它正被用来控制我们的所见、所为和所言。它没有给公民提供任何追索权或者选择退出的机会，就直接被执行了，也没有任何有意义的核查与制衡。这让我们缺乏安全感，也毫无自由可言。我们在早期技术体系下建立起来的保护自我的规则，现在完全失效了。因此，我们需要尽快重新调整这些规则。

本书分三部分进行论述。

第一部分介绍了我们所处的监控社会。第 1 章着眼于我们日常生活中产生的各种类型的个人数据。不仅包括前面描述的手机位置信息，也包括我们的电话、电子邮件和短信，以及我们浏览的网页，我们的金融交易数据等等。大多数人还没有意识到计算机能够集成我们所做的一切，或者计算机存储已经廉价到足够保存我们产生的所有数据。大多数人都低估了，通过我们认为的匿名数据识别出我们自己的容易程度。

第 2 章介绍了所有这些数据如何被用于监控。这种情况比比皆是，随处可见。它无须人工干预，就能自动执行。它主要隐藏在我们视线背后。这就是**泛在大规模监控**（ubiquitous mass surveillance）。

聚焦于企业和政府如何搜集数据是很简单的，但获得的信息并不准确。真正的情况是不同的数据流如何被处理、关联和分析。它不只是某一个人的信息，而是我们每个人的数据信息。泛在大规模监控和许多针对个人的监控是完全不同的，其规模是我们前所未见的。这方面问题将在第 3 章进行探讨。

我们作为客户或者用户与企业打交道，这些监控数据主要被提供服务的企业搜集。第 4 章讨论了监控的商业模式，主要是关于个性化广告。得益于我们的数据，整个数据交易行业如雨后春笋般蓬勃发展，个人信息在我们毫不知情的情况下被买卖。因为它正被一种新的计算模式所驱动——

数据存储在云端，利用像 iPhone 这类设备（只要在厂家严格控制下）就可以访问。结果导致大量企业可以访问、控制和我们密切相关的信息。

第 5 章转向政府监控。世界各国政府都在监控本国公民，入侵国内和国外的计算机。他们依靠政府掌握的资源想要监控所有人，目的是找出恐怖分子和罪犯、政治活动家、异见人士、环保人士、消费者权益倡导人士以及自由思想者。我主要关注国家安全局，因为通过爱德华·斯诺登（Edward Snowden）曝光的那些文件，它是我们最了解的美国秘密政府机构。

企业和政府都对我们的信息有一种永不满足的欲望，第 6 章我将讨论这二者如何进行合作。我称之为“公私监控伙伴关系”，它确实是一个根深蒂固的联盟。这也是监控无处不在的主要原因，它会阻碍任何试图改革这个系统的尝试。

即使你相信生活中打交道的企业和政府，这一切也都还是问题。记住，第二部分将转向探讨泛在大规模监控导致的许多相关危害。

在第 7 章，我讨论了政府监控的危害。历史一再表明，允许政府对公民进行肆无忌惮的大规模监控会造成危害。潜在的危害包括歧视和控制、对言论自由和思想自由的极大伤害（寒蝉效应）、（权力）不可避免被滥用、民主和自由的丧失。互联网有潜力成为全世界自由和解放运动的巨大动力；但通过允许政府进行全球范围的监控，我们正在浪费这种潜力。

第 8 章探讨了不受约束的企业监控带来的危害。私人企业现在控制着我们在互联网上聚集的“地方”，他们为了自己的利益正在挖掘我们留在他们那儿的信息。允许企业知道我们的一切，就是允许他们对我们进行分类和操控。这种操控主要是隐蔽的和无管制的，并将随着技术的进步愈加有效。

泛在监控还会带来其他的危害。第 9 章探讨了经济危害，主要是针对美国商业企业，不同国家的公民都竭力防止遭受美国国家安全局及其盟友的监控。互联网是一个全球平台，德国和巴西等国家试图利用他们的数据信息建立国家壁垒，这种做法允许政府监控企业，因此各大企业，尤其是

美国企业不得不审慎考虑。

在第 10 章，我探讨了丧失隐私权的危害。监控的拥护者们，从德意志民主共和国的斯塔西[1]到智利独裁者奥古斯托·皮诺切特（Augusto Pinochet）再到谷歌公司的埃里克·施密特，总是拿出那句老话“如果你毫无隐瞒，你就什么都不用怕”。这是危险狭隘的隐私价值观。隐私权是人类的基本需要，是控制我们和整个世界关系的至关重要的能力。剥夺隐私权是完全不人道的，无论是由便衣警察跟踪我们进行监控，还是通过计算机算法跟踪我们的一举一动，都毫无区别。

第 11 章，我转向探讨监控对安全的危害。政府的大规模监控经常被描绘成出于安全目的，是为保护我们免受恐怖袭击。但到目前为止，尚没有实际证据表明反恐的成功案例缘于大规模监控，由此产生伤害的证据却是不胜枚举。运行泛在大规模监控需要维持一个不安全的互联网（环境），这使我们对敌对政府、罪犯和黑客都缺少安全感。

第三部分论述了我们要做什么，以保护自己免遭政府和企业的监控。这些补救措施和问题一样复杂，往往要求对细节更加关注。在深入探讨具体的技术和政策建议前，第 12 章给出了引导我们深入思考的 8 个通用原则。

接下来的两章，提出了具体的政策建议：第 13 章是针对政府的，第 14 章是针对企业的。这些建议的某些部分可能比其他的更详细，而有些又是可望而不可即的。所有这些都是重要的，遗漏任何一点都可能颠覆其他解决方案。

第 15 章转而探讨我们每个人所能做的。我提供了一些很实用的技术建议以及政治行动建议。我们生活在一个技术可以压倒政治、政治也可以压倒技术的世界里。因此，我们需要从技术和政治两方面一起努力。

[1] 编注：斯塔西，又译史塔西，全称为“德意志民主共和国国家安全部”，成立于 1950 年 2 月 8 日，总部设在东柏林。成立的宗旨是担任民主德国的政治警察，负责搜集情报、监听监视、反情报等业务。