公众对数字时代监控的讨论将会是

a good deal more intelligent if we all read Bruce Schneier first."

—MALCOLM GLADWELL

DATA AND GOLIATH

The Hidden Battles to Collect Your Data and Control Your World

BRUCE SCHNEIER

DATA AND GOLIATH

《收集你的数据，控制你的世界的隐藏战斗》

Bruce schneer

w . w . NORTON & company纽约，伦敦

布鲁斯·施奈尔选集

《继续:来自施奈尔的安全忠告》(2013)

《说谎者与异类:实现社会繁荣所需的信任》(2012)

施奈尔论安全(2008)

超越恐惧:在不确定的世界中理性思考安全问题(2003)

《秘密与谎言:网络世界中的数字安全》(2000)《应用密码学:C语言的协议、算法和源代码》(1994和1996)

给凯伦:DMASC

目录

简介

第一部分:我们正在创造的世界

1. 数据作为计算的副产品
2. 作为监控的数据
3. 分析我们的数据
4. 监控业务
5. 政府监督与控制
6. 机构控制的巩固

第二部分:危在旦夕

7. 政治自由与正义
8. 商业公平与平等
9. 商业竞争力
10. 隐私
11. 安全

第三部分:如何应对

12. 原则
13. 政府解决方案
14. 企业解决方案
15. 我们其他人的解决方案
16. 社会规范与大数据权衡

致谢

备注

索引

引言

电话。如果你需要这个可爱的，时髦的，难以置信地相信你强大的生活工具，在一个科幻小说的中心世界里，看看我们的生活，我们认为这是理所当然的。无论你在地球上的哪个地方，从口袋里掏出这个设备，用它来和别人交谈，无论这个人在地球上的哪个地方，这似乎是再正常不过的事情了。

然而，每天早上当你把手机放进口袋的时候，你其实是在和运营商做一笔隐含的交易:“我想拨打和接听手机电话;作为交换，我允许这家公司随时知道我在哪里。”这种交易在任何合同中都没有明确规定，但它在服务的运作中是固有的。你可能没有想过这个问题，但既然我已经指出了这一点，你很可能会认为这是一个相当不错的交易。手机真的很棒，除非手机公司知道你在哪里，否则手机是无法工作的，这意味着他们会把你置于监视之下。

这是一种非常亲密的监视形式。你的手机会追踪你的居住地和工作地点。它记录了你喜欢在哪里度过周末和晚上。它会追踪你多久去一次教堂(以及哪个教堂)，你在酒吧里花了多长时间，以及你开车时是否超速。因为它知道你所在地区的所有其他手机，所以它会追踪你和谁一起度过的日子，你和谁共进午餐，你和谁睡觉。累积的数据可能比你自己更能描绘出你是如何消磨时间的，因为它不需要依赖于人类的记忆。2012年，研究人员能够利用这些数据预测*24小时后人们的位置*，误差在20米以内。

在手机出现之前，如果有人想知道这一切，他必须雇一个私家侦探跟着你到处做笔记。现在这种工作已经过时了;你口袋里的手机就能自动完成这一切。可能没有人检索到这些信息，但它就在那里。

你的位置信息很有价值，每个人都想获得它。警察也想要。手机定位分析在刑事调查中有几个不同的用途。警方可以通过“ping”特定的手机来确定它的位置，利用历史数据来确定它曾经去过哪里，并收集特定区域的所有手机位置数据来确定谁在那里，什么时候在那里。越来越多的警察正是为了这些目的而使用这些数据。

政府也利用这些数据进行恐吓和社会控制。2014年，乌克兰政府向基辅某一特定地点、某一特定时间段的手机用户发送了这条积极的奥威尔式短信:“亲爱的用户，你已被登记为一场大规模骚乱的参与者。”不要以为这种行为只存在于极权国家;2010年，密歇根州警方在一场预期的劳工抗议活动附近搜索了所有正在使用的手机的信息。他们没有先申请搜查令。

有一整个行业致力于实时跟踪你。公司利用你的手机在商店里跟踪你，了解你是如何购物的，在路上跟踪你，确定你离某家特定的商店有多近，并根据你现在的位置向你的手机发送广告。

你的位置数据非常有价值，以至于手机公司现在把这些数据卖给数据经纪人，数据经纪人再把这些数据转卖给任何愿意付钱的人。像Sense Networks这样的公司专门利用这些数据来建立我们每个人的个人资料。

电话公司并不是手机数据的唯一来源。美国公司Verint向世界各地的公司和政府销售手机跟踪系统。该公司的网站称，它是“可操作智能解决方案的全球领导者，为客户互动优化、安全智能、欺诈、风险和合规提供解决方案”，客户来自“180多个国家的1万多家组织”。UK公司Cobham出售一种系统，可以让人向手机发出“盲”呼叫——不会响，也不会被察觉。这种“盲呼”会迫使手机在特定的频率上传输信号，这样发送者就能在1米内追踪到手机。该公司自称拥有阿尔及利亚、文莱、加纳、巴基斯坦、沙特阿拉伯、新加坡和美国等国的政府客户。在巴拿马神秘注册的Defentek公司出售一种系统，可以“定位和跟踪世界上任何电话号码……不被网络、运营商或目标发现和未知”。这不是空谈;电信研究人员托比亚斯·恩格尔在2008年的一次黑客会议上也展示了同样的东西。如今的犯罪分子也在做同样的事情。

所有这些位置追踪都是基于手机系统。你的智能手机里还有一个完全不同的、更精确的定位系统:GPS。它为手机上运行的各种应用程序提供位置数据。一些应用程序使用位置数据来提供服务:谷歌地图、优步、Yelp。还有一些应用，比如愤怒的小鸟，只是希望能够收集和出售这些数据。

你也可以这么做。HelloSpy是一个应用程序，你可以偷偷地安装在别人的智能手机上跟踪她。非常适合一个焦虑的妈妈想要监视她的青少年，或者一个虐待的男人想要监视他的妻子或女朋友。雇主们已经使用这样的应用程序来监视他们的员工。

美国国家安全局(NSA)和UK政府通信总部(GCHQ)使用位置数据来跟踪人们。NSA从各种来源收集手机位置数据:手机连接的手机信号塔，手机登录的Wi-Fi网络的位置，以及来自互联网应用程序的GPS位置数据。NSA的两个内部数据库，代号为HAPPYFOOT和FASCIA，包含了全球设备的全面位置信息。NSA利用这些数据库跟踪人们的活动，识别与目标人物有关联的人，并确定无人机袭击的目标。

据称，即使手机处于关机状态，NSA也能追踪手机。

我刚才一直在谈论来自一个来源的位置信息——你的手机——但问题远不止于此。与你互动的电脑也在不断地

收集你的个人隐私资料。它包括你所读、所看、所听的内容。它包括你和谁交谈，你说了什么。最终，它涵盖了你在想什么，至少在某种程度上，你的想法会把你引向互联网和搜索引擎。我们生活在监控的黄金时代。

早在1999年，太阳微系统公司(Sun Microsystems)的首席执行官斯科特·麦克尼利(Scott McNealy)就直白地说过:“反正你没有隐私。克服它吧。”当然，他对我们应该如何应对监控的看法是错误的，但他说得对，避免监控和维护隐私变得越来越难了。

监控是一个带有政治和情感色彩的术语，但我是有意使用它的。美军对监视的定义是“系统观察”。我将解释，现代电子监视正是如此。我们对政府和企业都是公开的;他们窥视我们集体个人生活的能力比以往任何时候都要强大。

你一次又一次与各家公司达成的交易是，用监控换取免费服务。谷歌的董事长埃里克·施密特(Eric Schmidt)和创意总监贾里德·科恩(Jared Cohen)在2013年出版的《新数字时代》(The *New Digital Age)一书中阐述了这一点*。我在这里转述一下他们的观点:如果你让我们拥有你所有的数据，我们就会向你展示你想看的广告，我们还会提供免费的网络搜索、电子邮件和各种其他服务。基本上，这是一种便利。我们是社会性动物，没有什么比与其他人交流更有力量、更有回报的了。数字手段已经成为最简单、最快捷的交流方式。为什么我们要允许政府访问呢?因为我们害怕恐怖分子，害怕绑架我们孩子的陌生人，害怕毒贩，害怕任何当下流行的坏人。这就是国安局大规模监控项目的正当化;如果你让我们拥有你所有的数据，我们就会解除你的恐惧。

问题是，这些都不是好的或公平的交易，至少从今天的结构来看是这样。我们太轻易地接受了它们，却没有真正理解其中的条款。

以下是事实。今天的技术赋予了政府和企业进行大规模监控的强大能力。大规模监控是危险的。它使基于几乎任何标准的歧视成为可能:种族、宗教、阶级、政治信仰。它被用来控制我们看到什么、能做什么，以及最终控制我们说什么。这种做法没有为公民提供追索权或任何真正的选择退出的能力，也没有任何有意义的制衡。这让我们更不安全。它让我们更不自由。在早期的技术制度下，我们为保护我们免受这些危险而制定的规则，现在已经严重不足;它们不起作用。我们需要解决这个问题，而且要尽快解决。

在这本书中，我分三个部分来阐述这个问题。

第一部分描述了我们所生活的监控社会。第一章考察了我们在生活中产生的各种各样的个人数据。这不仅仅是我所描述的手机位置数据。它还包括我们的电话、电子邮件和短信数据，以及我们阅读的所有网页、我们的金融交易数据等等。我们大多数人都没有意识到计算机已经融入我们生活的方方面面

否则，计算机存储已经变得足够便宜，可以无限期地保存我们大量产生的所有数据。我们大多数人也低估了使用我们认为是匿名的数据来识别我们是多么容易。

第二章展示了所有这些数据是如何被用于监控的。这种情况随处可见。它是自动发生的，不需要人为干预。而且它在很大程度上隐藏在视线之外。这是无处不在的大规模监控。

人们很容易关注企业和政府是如何收集数据的，但这是一幅扭曲的图景。真正的故事是不同的数据流是如何被处理、关联和分析的。而且这不仅仅是一个人的数据;而是所有人的数据。无所不在的大规模监控与仅仅是大量的个人监控有着根本的不同，它正在以我们从未见过的规模发生。我在第三章中谈到了这一点。

监控数据主要是由与我们互动的公司收集的，要么是作为客户，要么是作为用户。第4章讨论了监控的商业模式，主要是个性化广告。围绕从我们的数据中获利，一个完整的数据经纪人行业如雨后春笋般冒了出来，我们的个人信息在我们不知情和不同意的情况下被买卖。这是由一种新的计算模式推动的，在这种模式下，我们的数据存储在云中，并由iPhone等设备访问，这些设备受到严格的制造商控制。其结果是，企业前所未有地访问和控制了我们最私密的信息。

第五章转向政府监控。世界各地的政府都在监视他们的公民，并侵入国内和国际的电脑。他们想监视每一个人，找出恐怖分子和罪犯，以及——取决于政府——政治活动家、持不同政见者、环保活动家、消费者权益倡导者和自由思想家。我主要关注NSA，因为这是我们最了解的秘密政府机构，因为爱德华·斯诺登公布了文件。

企业和政府都对我们的数据有着永不满足的胃口，我将在第六章讨论这两者是如何协同工作的。我称之为“公私监控伙伴关系”，这是一个深入人心的联盟。这是监控如此普遍的主要原因，它将阻碍改革这一体系的努力。

所有这些都很重要，即使你信任与你互动的公司和你生活在其中的政府。考虑到这一点，第二部分转向了无处不在的大规模监控所带来的许多相互关联的危害。

在第7章中，我讨论了政府监视所造成的危害。历史一再证明，允许政府对公民进行不受限制的大规模监视是危险的。潜在的危害包括歧视和控制、对言论自由和思想自由的寒蝉效应、不可避免的滥用以及民主和自由的丧失。互联网有潜力成为世界各地自由和自由的巨大推动力;我们允许政府在全球范围内进行监控，正在浪费这种潜力。

第八章谈到了不受约束的企业监控所造成的危害。私人公司现在控制着我们在互联网上收集信息的“地方”，他们为了自己的利益而挖掘我们留在那里的信息。通过允许公司了解我们的一切，我们允许他们对我们进行分类和操纵。这种操纵在很大程度上是隐藏的、不受监管的，随着技术的进步，这种操纵将变得更加有效。

无处不在的监控也会带来其他危害。第9章讨论了当不同国家的公民试图保护自己免受NSA及其盟友的监视时所产生的经济损害，主要是对美国企业的损害。互联网是一个全球性的平台，德国和巴西等国家试图在其数据周围建立围墙，这将使允许政府监控的公司——尤其是美国公司——付出相当大的代价。

在第10章中，我讨论了隐私丧失所造成的危害。监控的捍卫者——从德意志民主共和国的斯塔西(Stasi)到智利独裁者皮诺切特(Augusto Pinochet)，再到b谷歌的埃里克·施密特(Eric schmidt)——一直依赖于一句老话:“如果你没有什么可隐瞒的，那么你就没有什么可害怕的。”这是对隐私价值的一种危险的狭隘观念。隐私是人类的一项基本需求，对我们控制自己与世界的关系至关重要。被剥夺隐私从根本上来说是失去人性的，无论是便衣警察跟踪我们，还是计算机算法跟踪我们的一举一动，都没有什么区别。

在第11章中，我将转向监视对安全造成的危害。政府的大规模监控经常被描绘成一种安全利益，可以保护我们免受恐怖主义的侵害。然而，没有任何实际证据表明大规模监控在打击恐怖主义方面取得了任何真正的成功，也没有显著的危害证据。实现无处不在的大规模监控需要维护一个不安全的互联网，这使得我们所有人都不那么安全，不受敌对政府、犯罪分子和黑客的威胁。

最后，第三部分概述了我们需要做些什么来保护自己免受政府和企业的监视。补救措施和问题一样复杂，往往需要对细节进行细致的关注。不过，在我深入研究具体的技术和政策建议之前，第12章提供了8条应该指导我们思考的一般原则。

接下来的两章列出了具体的政策建议:第13章针对政府，第14章针对企业。其中一些建议比其他建议更详细，有些建议是有抱负的，而不是立即可实施的。不过，所有这些建议都很重要，任何遗漏都可能颠覆其他解决方案。

第15章转向我们每个人单独能做什么。我提供了一些实用的技术建议，以及对政治行动的建议。我们生活在一个技术可以胜过政治的世界，同时政治也可以胜过技术。我们需要两者共同努力。

在第16章的结尾，我探讨了作为一个社会，我们必须共同做些什么。第13章和第14章中的大多数建议都要求我们改变对监视的看法和对隐私的重视，因为在社会开始要求之前，我们不会得到任何严肃的法律改革。将我们的数据聚合起来用于医学研究、改善教育和其他有益于社会的任务，具有巨大的价值。我们需要弄清楚如何共同获得这种价值，同时将危害降到最低。这是构成本书所有内容的根本问题。

这本书涵盖了很多内容，而且必然会很快涉猎。尾注为有兴趣深入研究的人提供了广泛的参考资料。这些也可以在这本书的网站上找到:www.schneier.com/dg.html。在那里你还可以找到基于我完成手稿后发生的事件的书的更新。

我的写作带有强烈的美国偏见。大多数例子都来自美国，大多数建议也最适用于美国。首先，这是我所知道的。但我也相信，美国是一个独特的例子，说明了事情是如何出错的，它处于一个独特的位置，可以让事情变得更好。

我的背景是安全和技术。多年来，我一直在写安全技术如何影响人们，反之亦然。我目睹了信息时代监控的兴起，也看到了这个新世界的诸多威胁和不安全感。我习惯于通过安全问题的视角来思考安全问题，以及更广泛的社会问题。这种视角让我对问题和解决方案都有了单一的理解。

我不是反科技的，这本书也不是。互联网，以及整个信息时代，给社会带来了巨大的好处。我相信他们会继续这样做。我甚至不反对监控。电脑知道我们在做什么的好处已经改变了我们的生活。监控彻底改变了传统的产品和服务，并催生了全新的商业类别。它已成为执法部门的宝贵工具。它以各种方式帮助世界各地的人们，并将在未来继续发挥作用。

然而，监控的威胁是真实存在的，而我们对它们的讨论还不够多。我们对所有这些潜移默化的监控的反应基本上是被动的。我们不会考虑我们正在做的交易，因为它们还没有摆在我们面前。技术变革发生了，我们在很大程度上接受了它们。这很难怪我们;变化发生得如此之快，以至于我们还没有真正评估它们的影响，也没有权衡它们的后果。这就是我们最终进入监控社会的原因。监视社会悄悄逼近了我们。

本来不必这样的，但我们必须掌控局面。我们可以从重新谈判我们正在用我们的数据做的交易开始。我们需要积极主动地应对新技术。我们需要思考我们希望我们的技术基础设施是什么样子，以及我们希望它体现什么样的价值观。我们需要平衡我们的数据对社会的价值和它的个人性质。我们需要审视自己的恐惧，并决定我们到底愿意牺牲多少隐私来换取便利。我们需要了解过度监控的诸多危害。

我们需要反击。

——2014年10月，明尼苏达州明尼阿波利斯市和马萨诸塞州剑桥市

PART ONE

THE WORLD WE'RE CREATING

1

数据作为计算的副产品

计算机不断地产生数据。这是它们的输入和输出，但它是它们所做的一切的副产品。在它们的正常操作过程中，计算机不断地记录它们正在做的事情。它们感知和记录的东西比你意识到的要多。

例如，你的文字处理机会记录你写过的东西，包括你的草稿和修改。当你按下“保存”键时，你的文字处理器会记录下新版本，但你的电脑不会删除旧版本，直到它需要磁盘空间来做其他事情。你的文字处理器会时不时地自动保存你的文件;微软的Word每隔20分钟就会保存一次我的文件。Word还会记录谁创建了这份文件，通常还会记录还有谁参与了这份文件的处理。

连接到互联网上，你产生的数据会成倍增加:你访问的网站记录、你点击的广告记录、你输入的单词记录。你的电脑、你访问的网站以及网络上的电脑都会产生数据。你的浏览器向网站发送数据，包括你有什么软件，什么时候安装的，你启用了什么功能，等等。在很多情况下，这些数据足以唯一地识别你的电脑。

我们越来越多地通过电脑与家人、朋友、同事和偶然认识的人交流，使用电子邮件、短信、Facebook、Twitter、Instagram、SnapChat、WhatsApp以及其他任何现在流行的工具。数据是这种高科技社会化的副产品。这些系统不只是传输数据;它们还会创建你与他人互动的数据记录。

在外面走走，你可能不认为你在生产数据，但你确实在生产数据。你的手机会根据它附近的手机信号塔不断计算自己的位置。这并不是说你的手机公司特别关心你在哪里，而是它需要知道你的手机在哪里，以便将电话路由给你。

当然，如果你真的使用了那部手机，你就会产生更多的数据:拨打和接听的电话号码、发送和接收的短信、通话时长等等。如果它是智能手机，它也是一台电脑，你所有的应用程序在你使用它们时都会产生数据——有时甚至在你不使用它们时也会产生数据。你的手机可能有一个GPS接收器，它产生的位置信息比手机信号塔的位置更准确。你智能手机里的GPS接收器会把你定位在16至27英尺(约合16至27英尺)的范围内;手机信号塔，大约2000英尺。

在商店里买东西，就会产生更多的数据。收银机是一台电脑，它会记录你买了什么，以及你买的时间和日期。这些数据流入商家的计算机系统。除非你用现金支付，否则你的信用卡或借记卡信息会与这笔交易绑定在一起。这些数据也会被发送给信用卡公司，其中一些会在你每月的账单中返回给你。

商店里可能会安装一个摄像头，用来记录盗窃或欺诈的证据。当你使用自动取款机时，还有一个摄像头会记录下你的行为。外面有更多的摄像头，监视建筑物、人行道、道路和其他公共场所。

进入汽车，你会产生更多的数据。现代汽车装有电脑，产生你的速度、你踩踏板的力度、方向盘的位置等数据。其中大部分数据会被自动记录在黑匣子记录仪中，这对弄清楚事故中发生了什么很有用。甚至每个轮胎里都有一台电脑，用来收集气压数据。把你的车开到修理店，机械师要做的第一件事就是访问所有的数据来诊断任何问题。一辆自动驾驶汽车每秒可以产生1千兆字节的数据。

拍一张照片，你就又开始了。数码照片中嵌入了日期、时间和地点等信息。是的，许多相机都有拍摄照片的gps;关于相机、镜头和设置的通用信息;以及相机本身的ID号。如果你把照片上传到网上，这些信息通常还会附在文件上。

事情并不总是这样的。在报纸、广播、电视的时代，我们接收到的信息，却没有创造出事件的记录。现在我们通过互联网获得新闻和娱乐。我们过去常常与人面对面交谈，然后通过电话;我们现在通过短信或电子邮件进行交谈。我们过去在商店用现金买东西;现在我们在网上使用信用卡。我们过去在收费站、地铁转门或停车收费表处用硬币支付。现在我们使用自动支付系统，如EZPass，它与我们的车牌号码和信用卡相连。出租车过去只收现金。后来我们开始用信用卡付款。现在，我们用智能手机访问Uber和Lyft等联网出租车系统，这些系统会产生交易的数据记录，以及我们上下车的地点。除了一些特殊的例外，电脑现在无处不在，我们从事商业活动，我们与朋友交往的大多数地方。

去年，当我的冰箱坏了，维修人员更换了控制它的电脑。我才意识到，我之前一直把冰箱想反了:这不是一台有电脑的冰箱，而是一台能让食物保持低温的电脑。就这样，一切都变成了一台电脑。你的手机就是一台可以打电话的电脑。你的汽车是一台有轮子和引擎的电脑。你的烤箱是一台烤千层面的电脑。你的照相机是一台拍照的电脑。甚至我们的宠物和牲畜现在也经常被植入芯片;我家的猫简直就是一台整天在阳光下睡觉的电脑。

电脑正被嵌入到越来越多的联网产品中。b谷歌在2014年以超过30亿美元的价格收购了一家名为Nest的公司，该公司生产一种可以联网的恒温器。智能恒温器可以适应你的行为模式，并对电网上发生的事情做出反应。但要做到这一切，它记录的不仅仅是你的能源使用情况:它还会跟踪和记录你家的温度、湿度、环境光和附近的任何活动。你可以买一台智能冰箱，它可以跟踪食物的保质期，还可以买一台智能空调，它可以了解你的喜好，最大限度地提高能源效率。接下来还有更多:Nest现在正在销售一款

智能烟雾和一氧化碳探测器，并正在计划一系列额外的家庭传感器。许多其他公司也在开发各种各样的智能家电。如果我们想要建立智能电网，这将减少能源使用和温室气体排放，这一切都是必要的。

我们开始收集和分析关于我们身体的数据，作为改善我们健康和幸福的一种手段。如果你佩戴Fitbit或Jawbone这样的健身追踪设备，它会收集你醒着和睡着时的运动信息，并利用这些信息来分析你的运动和睡眠习惯。它还能确定你何时发生性行为。给这个设备更多关于你自己的信息——你的体重，你吃什么——你可以了解更多。当然，你分享的所有这些数据都可以在网上获得。

许多医疗设备开始支持互联网，收集和报告各种生物特征数据。已经有——或者很快就会有——能够持续测量我们生命体征、情绪和大脑活动的设备出现。这不仅仅是专门的设备;目前的智能手机都有一些相当灵敏的运动传感器。随着DNA测序的价格不断下降，越来越多的人开始注册生成和分析自己的基因数据。像23andMe这样的公司希望利用客户的基因组数据来寻找与疾病相关的基因，从而开发出新的、高利润的治疗方法。他们也在谈论个性化营销，保险公司可能有一天会购买他们的数据来做出商业决策。

也许数据生成自我趋势的极端是生活日志:不断捕捉个人数据。你已经可以在智能手机上安装生活记录应用程序，记录你的活动，比如和朋友聊天、玩游戏、看电影等等。但这只是生活日志未来发展的一个影子。未来，它还会包括视频记录。谷歌Glass是第一个具备这种潜力的可穿戴设备，但其他公司也不甘落后。

这些都是物联网的例子。环境传感器将检测污染水平。智能库存和控制系统将减少浪费并节省资金。连接互联网的计算机将无处不在——智能城市、智能牙刷、智能灯泡、智能人行道广场、智能药瓶、智能衣服——为什么不呢?据估计，目前连接互联网设备的数量为100亿。这已经超过了地球上的人口数量，我看到有人预测到2020年这个数字将达到300亿。炒作的程度相当高，我们还不知道哪些应用会成功，哪些应用会失败。我们所知道的是，它们都将产生数据，大量的数据。我们身边的东西会成为互联网的眼睛和耳朵。

所有这些连通性对隐私的影响是深远的。所有这些智能家电都将减少温室气体排放，它们还将传输有关人们如何在家中走动以及如何度过时间的数据。智能路灯将收集人们在室外活动的数据。摄像头只会变得更好、更小、更灵活。雷神公司计划于2015年在华盛顿特区和巴尔的摩上空飞行一架飞艇，以测试其跟踪“目标”(可能是地面、水中和空中的车辆)的能力。

其结果是，我们每天与数百台计算机交互，很快就会达到数千台。每一台电脑都会产生数据。其中很少有明显有价值的数据:我们在餐馆点了什么，晚上慢跑时的心率，或者我们写的最后一封情书。更确切地说，其中大部分是一种被称为*元数据的数据*。这是关于数据的数据-计算机系统用于操作的信息或该操作的副产品的数据。在短信系统中，消息本身就是数据，但是发送和接收消息的账户，以及消息的日期和时间，都是元数据。电子邮件系统也是类似的:电子邮件的文本是数据，但是发件人、收件人、路由数据和消息大小都是元数据——我们可以争论如何对主题行进行分类。在一张照片中，图像是数据;日期和时间、相机设置、相机序列号和照片的GPS坐标都是元数据。元数据听起来可能没什么意思，但是，正如我将解释的那样，它一点也不有趣。

尽管如此，我们产生的这种数据烟雾并不一定是任何人狡猾的结果。其中大部分只是计算的自然副产品。这就是目前科技的运作方式。数据是信息时代的废气。

有多少数据?

简单算一下。你的笔记本电脑可能有一个500g的硬盘。你购买的大备份硬盘可能可以存储2到3tb的数据。你的公司网络可能有1000倍的容量:1拍字节。更大的数字还有其他名字。千拍字节是一个exabyte(十亿亿亿字节)，一千个exabyte是一个zettabyte，一千个zettabytes是一个yottabyte。用人类的语言来说，一个eb字节的数据就是5000亿页的文本。

我们所有的数据废气加起来。到2010年，作为一个物种，我们每天创造的数据比我们从一开始到2003年创造的数据还要多。到2015年，每年将有76艾字节的数据通过互联网传输。

当我们开始思考所有这些数据时，很容易忽略对其保留和使用的担忧，因为假设有太多的数据需要保存，而且无论如何，要从中筛选出有意义的信息都太难了。这在过去是真的。在计算的早期，大部分数据——当然还有大部分元数据——在创建后不久就被扔掉了。保存这些数据占用了太多的内存。但计算各方面的成本多年来不断下降，十年前无法存储和处理的大量数据在今天很容易处理。2015年，1拍字节的云存储成本为每年10万美元，比2011年的100万美元下降了90%。其结果是，存储的数据越来越多。

你可能会把每一条发过的推特都存储在你的家用电脑的磁盘驱动器上。在美国，存储每一通电话的语音对话每年只需要不到300拍字节，也就是3000万美元。一个连续的视频生活记录者每人每年需要700千兆字节的存储空间。用这个数字乘以美国人口，每年就需要2eb，目前的成本是2亿美元。这是昂贵的，但似乎是合理的，而且价格只会下降。2013年，NSA在布拉夫代尔建成了庞大的犹他数据中心。它目前是世界上第三大，也是NSA的第一个

正在建设中。细节是保密的，但专家认为它可以存储大约12eb的数据。到目前为止，它已经花费了14亿美元。在全球范围内，谷歌的存储容量为15eb。

适用于组织的道理同样适用于个人，我就是一个案例研究。我的电子邮件记录可以追溯到1993年。我认为这些电子邮件档案是我大脑的一部分。这是我的记忆。每过一个星期，我都会在这些档案中寻找一些东西:几年前去过的一家餐馆，某人曾经告诉我的一篇文章，我遇到的一个人的名字。我一直给自己发提醒邮件;不仅提醒我回家后要做的事情，还提醒我未来几年可能想要回忆起来的事情。访问这些数据宝库就是访问我自己。

我曾经仔细地对所有的电子邮件进行分类。我必须决定哪些要保存，哪些要删除，我会根据人员、公司、项目等，把保存的电子邮件放入数百个不同的文件夹中。2006年，我不再这么做了。现在，我把所有的东西都保存在一个大文件夹里。2006年，对我来说，保存和搜索比排序和删除更容易。

要理解所有这些数据囤积对个人隐私意味着什么，请考虑奥地利法律系学生马克斯施雷姆斯。2011年，施雷姆斯要求Facebook向他提供公司掌握的关于他的所有数据。这是欧盟(EU)法律的要求。两年后，在一场法庭大战之后，Facebook寄给他一张CD，里面有一份1200页的PDF文件:不仅是他可以看到的朋友和他的新闻推送，还有他曾经点击过的所有照片和页面，以及他曾经看过的所有广告。Facebook并不使用所有这些数据，但该公司发现保存所有数据更容易，而不是弄清楚要保存什么。

2

作为监控的数据

我们把政府赶出去，把企业赶出我们的办公场所、数字化的商店和生活。通常，这种巨大的变化是在没有我们的知识和数据的情况下发生的，而且通常没有我们的同意。基于这些数据，他们得出关于我们的结论，我们可能不同意或反对，这可能会对我们的生活产生深远的影响。我们可能不愿意承认，但我们正处于大规模监控之下。

我们对NSA监控活动的了解大部分来自爱德华·斯诺登(Edward Snowden)，尽管在他之前和之后都有人泄露了NSA的机密。作为NSA的合同工，斯诺登收集了数万份描述NSA许多监视活动的文件。2013年，他逃到香港，把这些文件交给了经过挑选的记者。有一段时间，我与格伦·格林沃尔德(Glenn Greenwald)和《*卫报*》(Guardian)合作，帮助分析一些技术性更强的文件。

第一篇基于斯诺登文件的新闻报道描述了NSA如何收集每个美国人的手机通话记录。政府的一项辩护是，收集的数据“只是元数据”，这也是自那以后反复出现的一段录音。其意图是，NSA没有收集我们在电话交谈中所说的话，只收集双方的电话号码，以及通话的日期、时间和持续时间。这似乎安抚了很多人，但其实不应该这样。收集人们的元数据意味着将他们置于监视之下。

一个简单的思维实验证明了这一点。想象一下，你雇佣了一名私人侦探来窃听某人。侦探会在那个人的家里、办公室和车里安插窃听器。他会窃听那个人的电话和电脑。然后你就会得到一份详细记录那个人谈话内容的报告。

现在想象一下，你让侦探监视那个人。你会得到一份不同的但仍然全面的报告:他去了哪里，他做了什么，他和谁说过话，谈了多久，他给谁写信，他读了什么，他买了什么。这就是元数据。

窃听让你得到对话;监视让你得到其他一切。

单是电话元数据就暴露了我们的很多信息。我们通话的时间、时长和频率揭示了我们与他人的关系:我们的亲密朋友、商业伙伴，以及介于两者之间的所有人。电话元数据揭示了我们对什么和谁感兴趣，对我们来说什么是重要的，无论多么私密。它提供了一扇了解我们个性的窗口。它提供了在任何时间点发生在我们身上的事情的详细总结。

斯坦福大学的一项实验在几个月内检查了大约500名志愿者的电话元数据。研究人员可以推断出的个人性质

来自元数据的数据甚至让他们感到惊讶，这份报告值得引用:

- 参与者A与当地多个神经病学小组、一家专科药房、一家罕见病管理服务机构、一条专门用于治疗复发性多发性硬化症的药物热线进行了沟通。
- 参与者B与一家大型医疗中心的心脏病专家进行了详细的交谈，与一家医学实验室进行了简短的交谈，接到了一家药房的电话，并拨打了一个用于监测心律失常的医疗设备的家庭报告热线电话。
- 参与者C给一家专门从事AR半自动步枪平台的枪支商店打了很多电话，还与一家生产AR生产线的枪支制造商的客户服务部门进行了长时间的交谈。
- 在三周的时间里，参与者D联系了一家家装店、锁匠、水培经销商和一家头部商店。
- 参与者E与她的姐姐进行了一个漫长的清晨电话。两天后，她给当地的计划生育中心打了一系列电话。两周后，她又打了几个简短的电话，一个月后打了最后一个电话。

这是一个多发性硬化症患者，一个心脏病患者，一个半自动武器拥有者，一个家庭大麻种植者，还有一个堕胎的人，所有这些都来自一个元数据流。

网络搜索数据是另一种可以用于监控的私密信息来源。(你可以争论这是数据还是元数据。NSA声称这是元数据，因为你的搜索词嵌入在url中。)我们不会对搜索引擎撒谎。我们与搜索引擎的关系比与朋友、爱人或家人的关系更亲密。我们总是准确地告诉它我们在想什么，用尽可能清晰的语言。谷歌知道我们每个人都在搜索什么样的色情片，我们还会想起哪些旧情人，我们的羞耻，我们的担忧和我们的秘密。如果谷歌决定这样做，它就能找出我们中哪些人在担心自己的心理健康，哪些人在考虑逃税，哪些人在计划抗议某项政府政策。我过去常说b谷歌比我妻子更了解我在想什么。但这还远远不够。b谷歌*比*我更清楚*我*在想*什么*，因为b谷歌永远都记得很清楚。

我对谷歌的自动补全功能做了一个快速实验。这项功能可以根据其他人输入的内容，实时完成你的搜索查询。当我输入“我应该告诉我的w”时，谷歌建议“我应该告诉我的妻子我有外遇”和“我应该告诉我的工作关于酒后驾车”是最受欢迎的填词。谷歌知道谁点击了这些补全内容，以及他们搜索过的所有内容。

2010年，b谷歌首席执行官埃里克·施密特也承认了这一点:“我们知道你在哪里。我们知道你去过哪里。我们可以或多或少知道你在想什么。”

如果你有Gmail账户，你可以自己查看。你可以查看自己任何时候登录的搜索记录。只要你有这个账号，它就可以追溯到你，可能有好几年了。去做吧;你会大吃一惊的。这比你把日记寄给谷歌要亲密得多。尽管谷歌允许你修改你的广告偏好，但你没有权利删除任何你不想要的东西。

私密数据和元数据还有其他来源。你的购买习惯记录揭示了很多关于你是谁。你的微博告诉全世界，你每天早上几点起床，每晚几点睡觉。你的好友列表和通讯录透露了你的政治派别和性取向。你的电子邮件标题透露了你的身份

在你的职业、社交和感情生活中居于中心地位。

一种思考方式是，数据是内容，元数据是背景。元数据可能比数据更能说明问题，尤其是在聚合收集时。当你监视一个人时，谈话、短信和电子邮件的内容可能比元数据更重要。但当你监视整个人口时，元数据就更有意义、更重要、更有用了。

正如前NSA总法律顾问斯图尔特·贝克所说，“元数据绝对会告诉你某人生活的一切。如果你有足够的元数据，你就不需要内容了。”2014年，前NSA和中央情报局局长迈克尔·海登说:“我们根据元数据杀人。”

然而，事实是，这种区别在很大程度上是虚幻的。这些都是关于我们的数据。

更便宜的监控

从历史上看，监控既困难又昂贵。我们只在重要的时候才会这样做:比如警察需要跟踪嫌疑人，或者一家企业需要详细的采购历史记录以进行计费。当然也有例外，而且是极端的、昂贵的。异常偏执的东德政府有10.2万名史塔西监视着1700万人口:也就是说，每166名公民就有一名间谍，如果算上平民线人，每66名就有一名间谍。

企业监控从收集尽可能少的必要数据，发展到收集尽可能多的数据。公司总是收集客户的信息，但在过去，他们收集的信息并不多，只在必要的时候才会保留。信用卡公司只收集他们帐单所需要的客户交易信息。商店几乎从不收集顾客的信息，邮购公司只收集姓名和地址，也许还有一些购买历史记录，这样他们就知道什么时候该把某人从邮寄名单中除名。即使是谷歌，在最开始的时候，收集的用户信息也比现在少得多。在监控信息收集和存储成本高昂的时代，企业尽可能少地将就。

近几十年来，计算技术的成本迅速下降。这是一件非常好的事情。人们交流、发表思想、获取信息等等变得更便宜、更容易了。但同样是价格的下降，也拉低了监控的价格。随着计算机技术的进步，企业能够收集到与他们有业务往来的每个人的更多信息。随着数据存储成本的降低，他们能够保存更多的数据，保存的时间也更长。随着大数据分析工具变得越来越强大，保存更多的信息也变得有利可图。这导致了我将在第四章中讨论的基于监视的商业模式。

政府监控已经从收集尽可能少的人的数据变成了收集尽可能多的人的数据。当监控是人工操作且成本高昂时，只有在极端情况下才有正当理由。搜查令程序限制了警方的监视，

而资源的限制和被发现的风险也限制了国家情报监控。针对特定的个人进行监视，仅收集他们的最大信息。对于不收集其他人的信息，也有严格的最小化规则。例如，如果FBI正在监听歹徒的电话，如果歹徒的妻子或孩子接通了电话，监听者应该挂断电话并停止录音。

随着技术的进步和价格的下降，各国政府扩大了监控范围。国家安全局可以监视大的团体——苏联政府、中国外交使团、左翼政治组织和活动家——而不仅仅是个人。巡回窃听意味着FBI可以窃听人们，而不管他们使用什么设备进行通信。最终，美国机构可以监视所有人，并将数据保存数年。这与不断变化的威胁相吻合，他们继续对特定政府进行间谍活动，同时扩大对广泛人群的大规模监视，以寻找潜在的危险人物。我将在第5章讨论这一点。

其结果是，企业和政府的监控利益已经趋同。现在双方都想知道每个人的一切。动机不同，但方法是一样的。这就是我将在第6章中谈到的强大的公私安全伙伴关系的主要原因。

要了解我所说的监控技术成本是什么意思，只要看看普通消费者能以多么便宜的价格获得精密的间谍设备就知道了。在最近的一次飞行中，我翻阅了一期《天空商城》(*SkyMall*)，这是一份航空公司贴在每个国内飞机座位口袋里的目录。它提供了一支80美元的笔，里面有隐藏的摄像头和麦克风，这样我就可以秘密地记录下任何我以后可能需要证据的会议。我可以花100美元买一个隐藏在时钟收音机里的摄像头，或者伪装成挂在墙上的运动传感器报警装置。我可以将其中一个设置为连续记录，也可以只在检测到运动时进行记录。另一款设备可以让我看到别人智能手机上的所有数据——不管是iPhone还是android——前提是我能弄到手。“即使短信已被删除，也要继续阅读。查看照片、联系人、通话记录、日程安排和访问过的网站。甚至可以利用手机的GPS数据来找出它去过哪里。”只要120美元。

从其他零售商那里，我可以买到键盘记录器，或键盘记录器，以了解别人在她的电脑上键入什么-假设我可以实际访问它-花费不到50美元。我可以花100美元买一个电话拦截软件来监听别人的手机通话。或者我可以花不到1000美元买一架带有机载摄像头的遥控无人直升机，用它来监视我的邻居。

这些都是消费品，其中一些在某些司法管辖区是非法的。专业的监控设备也越来越便宜，越来越好。对于警察来说，不断下降的成本改变了一切。秘密跟踪某人，无论是步行还是开车，每月的成本约为17.5万美元——主要是负责跟踪的特工的工资。但如果警方可以在嫌疑人的车里放置追踪器，或者使用假的手机发射塔设备来欺骗嫌疑人的手机，让其交出位置信息，那么每月的成本就会下降到7万美元左右，因为只需要一名特工。如果警察能在嫌疑人的车里藏一个GPS接收器，价格就会突然降到150美元一个

一个月——主要用于秘密安装设备。从嫌疑人的手机运营商那里获取位置信息更便宜:Sprint每月只向执法部门收取30美元的费用。

这个差额是固定成本和边际成本的差额。如果警察部门进行徒步监视，跟踪两个人的成本是跟踪一个人的两倍。但对于GPS或手机监控，成本主要是用于设置系统。一旦安装到位，多跟踪一个、十个或一千人的额外边际成本就微乎其微了。或者，一旦有人花钱设计和建造一个电话窃听系统，收集和分析阿富汗的所有语音通话，就像美国国家安全局(NSA)帮助美国士兵免受简易爆炸装置的袭击一样，部署同样的技术来对付其他国家的电话网络既便宜又容易。

大规模监视

监控技术成本下降的结果不仅仅是价格上的差异;而是种类上的差异。组织最终会进行更多的监视——多得多。例如，2012年，在最高法院做出裁决后，FBI被要求要么获得搜查令，要么关闭安装在汽车上的3000个GPS监控设备。如果没有自动化，FBI根本不可能跟踪3000辆汽车;该机构就是人手不够。而现在手机的普及意味着每个人都可以被跟踪，每时每刻。

另一个例子是车牌扫描仪，它正变得越来越普遍。有几家公司维护着车主拖欠汽车贷款的车牌数据库。侦察车和拖车在车顶安装摄像头，不断扫描车牌，并将数据传回公司，寻找目标。汽车回收业务可以赚大钱，所以有很多人参与其中——所有人都把数据输入公司的中央数据库。位于加州利弗莫尔的一家名为Vigilant Solutions的扫描公司声称，他们拥有25亿条记录，每月在美国收集7000万次扫描，以及日期、时间和GPS位置信息。

除了财产回收业务，扫描公司还把他们的数据卖给离婚律师、私家侦探和其他人。他们有时会将这些数据实时传递给警察部门，警察部门会将这些数据与他们从州际高速公路匝道、收费广场、边境口岸和机场停车场获得的扫描数据结合起来。他们正在寻找被盗车辆和有未执行的搜查令和未付罚单的司机。FBI已经在使用各州的驾照数据库来识别人，美国国土安全部希望所有这些数据都在一个国家数据库中。在英国，一个类似的基于固定摄像头的政府管理系统在全国范围内部署。它执行伦敦的汽车拥堵费制度，并搜索落后于强制检查的车辆。

预计同样的事情也会发生在自动人脸识别上。最初，来自私人摄像头的数据最有可能被赏金猎人用来追踪保释

跳绳。不过，最终它将被出售作其他用途，并交给政府。FBI已经有了一个包含5200万张人脸的数据库，面部识别软件也相当不错。迪拜警方正在将定制面部识别软件与谷歌眼镜集成，以自动识别嫌疑人。如果城市里有足够多的摄像头，警察就可以在不离开办公桌的情况下跟踪车辆和周围的人。

这是大规模监控，没有电脑、网络和自动化是不可能实现的。这不是“跟着那辆车”;而是“跟踪每一辆车”。警察总是可以跟踪嫌疑人，但有了城市摄像头、车牌扫描仪和面部识别软件，他们可以跟踪每个人——无论是否有嫌疑人。

同样，在嫌疑人的固定电话上安装一种名为“笔式记录器”的设备来记录他拨打的电话号码，过去既耗时又昂贵。但现在，FBI可以要求从电话公司的数据库中获取数据，它可以获得关于美国每个人的信息。而且它已经做到了。

2008年，Waze公司(2013年被b谷歌收购)推出了一款新的智能手机导航系统。他们的想法是，通过追踪使用Waze的汽车的运动，该公司可以推断出实时交通数据，并将人们引导到最快的道路上。我们都想避开交通堵塞。事实上，不只是Waze的客户，整个社会都受益于人们远离交通堵塞，这样他们就不会增加交通堵塞。但是，我们是否意识到我们泄露了多少数据?

历史上第一次，政府和企业有能力对整个人口进行大规模监控。他们可以监控我们的互联网使用、我们的通讯、我们的金融交易、我们的行动……一切。即使是东德人也不可能一直跟踪每个人。现在容易多了。

隐蔽监控

如果你在Kindle上读这本书，亚马逊知道。亚马逊知道你什么时候开始阅读，以及你阅读的速度。公司知道你是从头到尾地阅读，还是每天只读几页。它知道你是直接跳到最后，还是回去重读了一段，还是在某一页上逗留了很长时间，或者你放弃了，没有读完这本书。如果你选中了任何段落，亚马逊也会知道。没有闪烁的灯光，没有弹出的提示框，提醒你Kindle正在向亚马逊发送有关你阅读习惯的数据。它只是静静地、不断地发生着。

我们在网上容忍某种程度的电子监控，这是我们在现实世界中永远不会允许的，因为它不明显，也不宣传。职员要求看身份证是一回事，收费站的摄像头要求拍车牌是一回事，ATM要求出示银行卡和密码是一回事。所有这些行为都会产生监视记录——第一种情况可能需要职员复制或以其他方式捕捉身份证上的数据——但至少它们是公开的。我们知道它们正在发生。

大多数电子监控不是这样发生的。它是隐蔽的。我们在网上看报纸，没有意识到我们读到的文章是被记录下来的。我们浏览网上商店，没有意识到我们买的东西和我们看了之后决定不买的东西都被记录了下来

被监控。我们使用电子支付系统，没有考虑他们如何记录我们的购买。我们随身带着手机，不知道它们一直在跟踪我们的位置。

Buzzfeed是一个娱乐网站，它收集了大量的用户信息。大部分数据来自传统的互联网跟踪，但Buzzfeed也有很多有趣的小测验，其中一些问的是非常私人的问题。其中一个——“你有多有特权?”——询问财务细节、工作稳定性、娱乐活动和心理健康状况。超过200万人参加了这个测试，他们没有意识到Buzzfeed会保存测试中的数据。类似地，WebMD等医疗信息网站也会收集用户搜索和阅读的页面数据。

以免你认为只有你的网页浏览、电子邮件、电话、聊天和其他电子通信被监控，老式的纸质邮件也被跟踪。通过一项名为“隔离控制和追踪”的计划，美国邮政总局拍摄了*每一封*寄到*美国*的*邮件*的正面和背面。每年大约有1600亿封邮件。这些数据可供执法部门使用，当然也可以供其他政府机构使用。

在互联网之外，许多监控技术正变得越来越小，越来越不显眼。在一些城市，摄像机每天都要捕捉我们数百次的影像。有些是显而易见的，但我们没有在天花板灯或ATM上嵌入闭路电视摄像头，也没有在街区外安装十亿像素的摄像头。无人机正变得越来越小，越来越难以看到;它们现在只有昆虫的大小，很快就会变成尘埃的大小。

在这些图像采集系统中添加识别软件，你就拥有了一个无所不在的自动监控系统。人脸识别是在镜头前识别人物最简单的方法，而且这项技术每年都在进步。2014年，人脸识别算法的表现开始超过人。还有其他正在开发的图像识别技术:远距离工作的虹膜扫描仪、步态识别系统等等。

街道上也有更多隐蔽的监控。你钱包里的非接触式RFID芯片卡可以用来跟踪人。许多零售商店通过MAC地址和蓝牙id(基本上是识别号码)秘密地跟踪人们的智能手机。目的是记录他们走过哪条过道，他们停下来看了哪些产品等等。通过这两种方法，人们可以在公共活动中被跟踪。

2014年，福特汽车公司(Ford Motor Company)的一位高管在消费电子展(Consumer Electronics Show)上对观众说，“我们知道每个违法的人，我们知道你什么时候在违法。”我们在你的车上安装了GPS，所以我们知道你在做什么。”这让人感到震惊和意外，因为没有人知道福特一直在监视它的车主。该公司很快收回了这些言论，但这些言论给福特收集车主数据留下了很大的回旋余地。我们从美国政府问责局的一份报告中得知，汽车公司和导航辅助公司都从用户那里收集了大量的位置数据。

太赫兹范围内的雷达可以探测到人身上隐藏的武器，以及穿透8英寸厚的混凝土墙的物体。摄像头可以通过聚焦附近的物体(如薯片袋)并测量它们的振动来“听”电话对话。美国国家安全局，大概还有其他人，可以远程打开你手机的麦克风，监听周围发生的事情。

也有正在开发的体臭识别系统。在互联网上，一家公司正致力于通过打字风格来识别人。有一项研究是通过写作风格来识别一个人。企业和政府都在收集数以千万计的声纹——这是另一种实时识别你的方式。

这就是未来。你一进门，店员就会知道你的名字、地址和收入水平。广告牌会知道你是谁，并记录下你对它们的反应。杂货店的货架会知道你通常买什么，以及如何诱使你多买一些。你的车会知道谁在车里，谁在开车，司机遵守或忽视了什么交通法规。即使是现在，这感觉也很像科幻小说。

随着监控逐渐淡出背景，它变得更容易被忽视。而监控系统的侵入性越强，就越容易被隐藏起来。我们中的许多人在被雇佣到办公室工作之前都会拒绝接受药检，但许多公司会对所有潜在员工进行侵入性的背景调查。同样，在互联网上被数百家公司跟踪——这些公司你从来没有接触过，甚至没有听说过——这种感觉比100名市场调查人员跟着我们做笔记要少得多。

从某种意义上说，我们生活在一个独特的历史时代;我们的许多监控系统对我们来说仍然是可见的。同一性很常见，但他们仍然要求我们出示身份证。摄像头无处不在，但我们还是能看到它们。在不久的将来，由于这些系统将被隐藏起来，我们可能会在不知不觉中默许更多的监控。

自动监控

大量的监控自动发生在我们身上，即使我们尽力选择不参与。它的发生是因为我们与他人互动，而*他们正在*被监控。

尽管我从来没有在facebook上发过帖子或加过朋友——我有一个专业页面，但没有个人账户——但facebook一直在跟踪我。它在其数据库中保留了非facebook用户的个人资料。每当我访问带有Facebook“喜欢”按钮的页面时，它都会跟踪我。它可能可以根据标记的照片很好地猜测出我的朋友是谁，而且它很可能将个人资料链接到它从各种数据经纪人那里购买的其他信息。我的朋友，以及那些有“喜欢”按钮的网站，允许Facebook通过它们监视我。

我尽量不使用谷歌搜索。但谷歌仍然收集了我访问的网站的大量信息，因为很多网站使用谷歌分析来跟踪他们的访问者。同样，这些网站让谷歌通过它们跟踪我。我在浏览器中使用了各种拦截器，所以谷歌无法很好地跟踪我，但它正在研究可以规避的技术

我的隐私保护措施。

我也不用Gmail。相反，我使用当地的ISP，并将我所有的电子邮件存储在我的电脑上。即便如此，谷歌还是有大约三分之一的我的信息，因为我通信的许多人都使用Gmail。不仅仅是gmail。com地址;谷歌托管了许多组织的电子邮件，尽管这些组织保留了它们的域名地址。还有其他的例子。苹果有一个全球范围的Wi-Fi密码数据库，包括我的家庭网络密码，这些密码来自备份iphone的用户。很多公司都有我的联系方式，因为我的朋友和同事在云端备份了他们的地址簿。如果我姐姐公布了她的基因信息，那么我的一半信息也会被公开。

有时候，我们只打算与少数人分享的数据，变成了全世界的监控数据。有人可能会在聚会上拍下朋友的照片，然后发布到Facebook上，这样她的其他朋友就可以看到了。除非她另有说明，否则这张照片是公开的。当然，它仍然很难找到——直到它被自动面部识别系统标记并被搜索引擎索引。现在这张照片可以很容易地通过图像搜索找到。

我经常出现在别人的监控摄像头里。在伦敦、芝加哥、墨西哥城和北京等城市，警察部队到处安装了监控摄像头。在其他城市，比如纽约，这些摄像头大多是私人拥有的。我们在最近的两起恐怖主义案件中看到了不同。伦敦地铁爆炸案是由政府摄像头识别的，波士顿马拉松爆炸案是由企业的私人摄像头识别的。

这些数据几乎可以肯定是数字化的。通常它只是存储在相机上，在一个无尽的循环中，在记录新数据的同时删除旧数据。但是，越来越多的监控视频可以在互联网上找到，并且被无限期地保存着，其中很多是可以公开搜索的。

除非我们采取措施防止这种情况发生，否则随着生活记录仪的普及，被摄像头捕捉到的情况将变得更加不可避免。一旦有足够多的人定期录制他们所看到的视频，你就会出现在他们的视频片段中，你是否戴着录像机就不再重要了。这有点像群体免疫，只不过是反过来的。

无处不在的监控

哲学家杰里米·边沁在18世纪末构想了他的“圆形监狱”，作为建造更便宜监狱的一种方式。他的想法是建造一座监狱，在那里每个囚犯都可以随时被监视，而不被察觉。犯人别无选择，只能假设他总是被监视着，因此会顺从。这个想法被用来比喻大规模的个人数据收集，无论是在互联网上还是在线下。

在互联网上，监控无处不在。我们所有人每时每刻都在被监视，而这些数据将被永久存储。这就是一个信息时代的监控国家的样子，它的效率超出了边沁最疯狂的梦想。

3

分析我们的数据

广告在2012年，优势。《*纽约时报*》这篇文章在塔吉特网站上披露了一个故事，公司如何通过分析确定女性怀孕时的购买模式数据，并利用这些信息向女性发送婴儿相关商品的广告和优惠券。这篇文章讲述了一名明尼阿波利斯男子向塔吉特百货公司投诉，该公司向他十几岁的女儿发送了与婴儿相关的优惠券，但后来他发现塔吉特百货公司是对的。

收集和保存各种数据的一般做法被称为“大数据”，从中提取有用信息的科学和工程被称为“数据挖掘”。像塔吉特这样的公司通过挖掘数据来集中投放广告。巴拉克·奥巴马(Barack Obama)在2008年和2012年的总统竞选中也出于同样的目的广泛挖掘数据。汽车公司从你的汽车中挖掘数据来设计更好的汽车;市政当局从路边传感器中挖掘数据，以了解驾驶状况。我们的基因数据被挖掘用于各种医学研究。Facebook和Twitter等公司挖掘我们的数据用于广告目的，并允许学者挖掘他们的数据用于社会研究。

其中大多数都是数据的二次使用。也就是说，它们并不是收集数据的首要原因。事实上，这就是大数据的基本承诺:保存你能保存的一切，总有一天你能想出这些东西的一些用途。

在某种程度上，大数据集的价值来自于可以从中得出的推论。其中一些是显而易见的。如果你有某人一年的详细位置数据，你就可以推断出他最喜欢的餐馆是什么。如果你有他打电话和发邮件的人的名单，你就可以推断出他的朋友是谁。如果你有他访问过的网站的列表，或者他买过的书的列表，你就可以推断出他的兴趣。

有些推断则更为微妙。某人的购物清单可能暗示了她的种族。或者她的年龄和性别，可能还有宗教信仰。或者她的病史和饮酒习惯。营销人员总是在寻找一些模式，这些模式表明某人即将做一些昂贵的事情，比如结婚、度假、买房、生孩子等等。各国的警察要么在法庭上，要么在秘密中，都将这些模式作为证据。Facebook可以预测种族、性格、性取向、政治意识形态、关系状况和吸毒情况，仅根据点赞次数。该公司在你宣布订婚之前就知道你订婚了，在你出柜之前就知道你是同性恋——它的帖子可能会在你不知情或未经允许的情况下向其他人透露这些信息。这取决于你所居住的国家，这可能只是一个重大的个人尴尬，也可能会让你丧命。

这些推断中有很多错误，我们所有看过互联网广告的人都可以证明，这些广告只是模糊的有趣。但是，当广告走上正轨时，它们可能会令人毛骨悚然——而我们往往不喜欢它。看到痔疮栓剂的广告是一回事

或者在电视上看到帮你找女朋友的服务，我们知道大家都看到了。但当我们根据我们在互联网上发布或点赞的内容，知道它们是专门针对我们的时候，就会觉得更有侵犯性。这就产生了一种有趣的紧张关系:我们愿意分享的数据可能隐含着我们不想分享的结论。我们中的许多人都很乐意告诉Target我们的购买模式，以获得折扣和我们可能喜欢购买的新产品的通知，但我们中的大多数人都不希望Target发现我们怀孕了。我们也不希望伴随这些大型数据库而来的不可避免的大数据盗窃和欺诈。

当我们想到计算机使用我们所有的数据来进行推断时，我们有一种非常人性化的思维方式。我们想象着如何理解这些数据，并将这一过程投射到计算机上。但这是不对的。电脑和人有不同的长处、短处和局限。计算机不能像人一样进行抽象推理，但它们可以更快地处理大量数据。(如果你仔细想想，这意味着计算机更擅长处理元数据，而不是处理会话数据。)而且它们还在不断改进;计算能力仍然每18个月翻一番，而我们人类的大脑大小却保持不变。在处理定量数据方面，计算机已经比人强得多，而且还会继续提高。

现在，数据挖掘是一项热门技术，围绕它有很多炒作和机会主义。目前还不完全清楚什么样的研究将成为可能，或者这个领域的真正潜力是什么。但可以肯定的是，数据挖掘技术正变得越来越强大，并使观察者能够从大数据集中得出越来越惊人的结论。

回溯时间的监控

通过将数据挖掘技术应用于大规模监控数据，你可以做的一件新事情是回溯时间。传统的监控只能了解现在和未来:“跟着他，找出他下一步要去哪里。”但如果你有了一个所有人的历史监控信息数据库，你就可以做一些新的事情:“查找那个人的位置信息，找出他去过哪里。”或者:“监听他上周的通话记录。”

其中一些一直都是可能的。从历史上看，政府收集了关于过去的各种数据。例如，在麦卡锡时代，政府利用政党登记、杂志订阅、朋友、邻居、家人和同事的证词来收集人们的数据。现在的不同之处在于，这种能力更像是一台时光机(Wayback Machine):数据更完整，获取成本也要低得多，而且技术已经发展到可以进行复杂的历史分析。

例如，近年来，瑞士信贷、渣打银行和法国巴黎银行都承认违反了禁止向受制裁团体转账的法律。他们故意改变交易，以逃避“OFAC过滤器”的算法监视和检测，OFAC过滤器是美国财政部下属的外国资产控制办公室。要理清这类不法行为需要大量的历史分析

银行交易和员工通讯。

同样，有人可以用新的分析工具来检查旧数据。想想基因数据。我们还不能从某人的基因数据中学到很多东西，但十年后——谁知道呢?在环法兴奋剂丑闻期间，我们看到类似的事情发生了;几年前从车手身上采集的血液用新技术进行了检测，发现了普遍存在的兴奋剂问题。

NSA存储了大量的历史数据，我将在第五章中详细讨论。我们知道，在2008年，一个名为XKEYSCORE的数据库通常只保存语音和电子邮件内容三天，但它保存了一个月的元数据。一个名为MARINA的数据库保存了人们一年的浏览历史记录。另一个NSA数据库“神秘”(MYSTIC)能够存储百慕大*群岛所有*电话通话的录音。NSA保存了五年的电话元数据。

这些存储限制适用于收集到的所有原始数据。如果NSA的分析师接触到数据库中的某些内容，该机构会将其保存更长时间。如果你的数据是查询这些数据库的结果，你的数据将被无限期保存。如果你使用加密，你的数据就会被无限期保存。如果你使用某些关键字，你的数据会被无限期保存。

NSA存储数据的时间长短更多的是存储容量的问题，而不是对隐私的尊重。我们知道NSA需要增加存储容量来保存它所收集的所有手机位置数据。随着数据存储变得越来越便宜，假设更多的这些数据将被存储更长时间。这就是NSA犹他州数据中心的意义所在。

FBI也存储我们的数据。在2013年的一次合法调查过程中，FBI获得了Freedom Hosting网站上所有数据的副本，包括存储的电子邮件。几乎所有的数据都与调查无关，但FBI保留了整个网站的副本，并从那时起一直在进行不相关的调查。纽约州将车牌扫描数据保留至少5年，甚至可能无限期保留。

任何数据——脸书历史记录、推文、车牌扫描数据——基本上都可以永远保留，或者直到公司或政府机构决定删除为止。2010年，不同的手机公司保留短信的时间从90天到18个月不等。AT&T打败了所有这些公司，保留了7年的数据。

映射关系

大规模监控数据使得人际关系映射成为可能。2013年，当我们第一次得知国家安全局(NSA)正在收集每个美国人的电话通话元数据时，人们对所谓的跳跃搜索(hop search)及其含义感到非常困惑。这是一种新型的搜索，在计算机出现之前理论上是可行的，但只有在大规模监控的世界里才真正具有实用性。想象一下，NSA对爱丽丝感兴趣。它会收集她的数据，然后收集与她通信的每个人的数据，然后收集与他们通信的每个人的数据，然后收集与*他们*通信的每个人的数据。那里离爱丽丝只有三跳，这是NSA的最大值。

跳数搜索的目的是映射关系，发现阴谋。要想弄明白这些数据，就需要能够剔除掉绝大多数被这个“拉网”的无辜者，以及不相关的人共同使用的电话号码:语音信箱服务、披萨店、出租车公司等等。

NSA的文件指出，该机构在2013年的一天内有117,675个“活跃监视目标”。即使保守估计每个人有多少熟悉的人，他们之间有多少重叠，这个系统监控的总人数也轻松超过了2000万。这是经典的“六度分离”问题;我们大多数人与其他人只有几步之遥。2014年，奥巴马总统指示NSA只对一个特定项目收集的电话元数据进行两跳分析，但他没有对NSA收集的所有其他数据的跳进行任何限制。

来自各种来源的元数据对于绘制关系非常有用。我们大多数人使用互联网进行社交互动，我们的关系也会在其中体现出来。这就是NSA和Facebook都在做的事情，这就是为什么后者在暗示你可能认识但还不是你Facebook好友的人时，会如此准确得令人不安。Facebook最成功的广告项目之一是不仅向喜欢某个特定页面或产品的人展示广告，还向他们的朋友和朋友的朋友展示广告。

通过我们的行为找到我们

一旦你收集了每个人的数据，你就可以根据他们的行为来搜索个人。也许你想找到每个经常光顾某个同性恋酒吧的人，或者是阅读某个特定主题的人，或者是有特定政治信仰的人。企业经常这样做，利用海量监控数据来寻找具有特定特征的潜在客户，或者通过搜索在特定主题上发表过文章的人来寻找可以雇佣的人。

除了姓名和其他个人标识符(如身份证号码、电话号码等)之外，人们还可以搜索其他东西。例如，谷歌搜索你所有的Gmail，并使用它找到的关键字来更深入地了解你，用于广告目的。NSA也做类似的事情:它称之为“关于”的搜索。基本上，它在每个人的通信内容中搜索一个特定的名字或单词，或者可能是一个短语。因此，除了检查爱丽丝的数据和距离她两到三跳以内的每个人的数据外，它还可以搜索其他人——整个通信数据库——查找提到她名字的内容。或者，如果它不知道名字，但知道某个特定地点或项目的名称，或者某人使用过的代号，它可以在此基础上进行搜索。例如，NSA的目标是那些在流行的互联网隐私和匿名工具上搜索信息的人。

我们不知道具体细节，但NSA会根据任何联系，而不仅仅是电话联系，将跳线串在一起。这可能包括与目标在同一位置，有相同的通话模式，等等。通过访问每个人的数据，这些类型的搜索成为可能。

你可以使用大规模监控来寻找个人。如果你知道某个人

某天晚上在一家特定的餐馆，三天后的下午在火车站，第二天早上在水电站，你可以查询每个人的手机位置数据库，符合这些特征的人就会跳出来。

你还可以搜索异常行为。以下是NSA如何使用手机数据的四个例子。

1. NSA使用手机位置信息来追踪那些行动有交集的人。例如，假设NSA对爱丽丝感兴趣。如果鲍勃某天晚上和爱丽丝在同一家餐馆，一周后又和爱丽丝在同一家咖啡店，一个月后又和爱丽丝在同一个机场，系统就会将鲍勃标记为爱丽丝的潜在伙伴，即使两人从未通过电子方式交流过。

2. NSA追踪海外美国间谍携带的手机的位置。然后，它会确定是否还有其他手机在跟踪这些特工的手机。基本上，NSA会检查是否有人在跟踪这些特工。

3. 国家安全局(NSA)有一个项目，通过搜集手机元数据来发现那些开机、使用了一段时间、然后关机、再也不用的手机。它利用手机的使用模式将它们联系在一起。这项技术被用来寻找那些希望避免被发现的人使用的“一次性”手机。

4. NSA收集人们关机的数据，以及关机时长。然后，它会收集这些人关闭手机时的位置，并寻找附近同样关闭手机一段时间的其他人。换句话说，它会寻找秘密会议。

我已经讨论过乌克兰政府利用手机位置数据找到参加反政府示威的所有人，密歇根警方利用它找到计划中的工会抗议地点附近的所有人。联邦调查局(FBI)利用这些数据找到了特定目标使用过但与他没有其他关联的手机。

一些公司也会这样做。有一种被称为地理围栏的技术，营销人员使用它来识别在特定企业附近的人，以便向他们发送广告。一家名为Placecast的地理围栏公司在美国和英国为星巴克、凯马特和赛百subway等连锁店的1000万部手机提供基于位置的广告。微软(Microsoft)对经过其部分门店10英里范围内的人也做同样的事情;它与NinthDecimal公司合作。Sense Networks使用位置数据来创建个人档案。

关联不同的数据集

Vigilant Solutions是一家从摄像头中收集车牌数据的公司。它计划用其他汽车识别算法、面部识别系统和来自其他数据库的信息来增强这个系统。其结果将是一个比简单的车牌扫描数据库强大得多的监控平台，无论它有多广泛。

关于大规模监控的新闻报道一般都是以数据收集为框架的，但却忽略了数据关联的故事:将不同数据集之间的身份联系起来，从组合的数据中得出推论。这不仅仅是因为配备强大摄像头的廉价无人机将变得越来越普遍。正是无人机加上面部识别软件，使系统能够自动识别人，再加上庞大的标记照片数据库——来自驾照、Facebook、报纸、高中年鉴——将为该软件提供参考图像。它还具有将识别与众多其他数据库关联起来的能力，以及存储所有这些数据的能力

无限期地存储数据。无所不在的监控是多个大规模监控流捆绑在一起的结果。

我有一张牡蛎卡，我在伦敦时用它来支付公共交通费用。我煞费苦心地让它只收现金，而且不记名。即便如此，如果你要把这张卡的使用情况与访问伦敦的人的名单和日期联系起来——不管这个名单是由航空公司、信用卡公司、手机公司还是互联网服务提供商提供的——我敢打赌，我是唯一一个与这些日期完全相关的人。因此，我在伦敦地铁里的“匿名”活动就变得毫无意义了。

斯诺登披露了csec(加拿大通信安全机构，相当于NSA)的一个有趣的研究项目，该项目展示了将不同的监控信息流关联起来，以发现故意逃避检测的人的价值。

CSEC的一名研究员，有一个听起来很酷的头衔——“间谍技术开发人员”，从两周的互联网识别数据开始:基本上，一个登录到各个网站的用户id列表。他还拥有不同无线网络IP地址的地理位置数据库。通过将两个数据库放在一起，他可以将从不同无线网络登录的用户id与这些网络的物理位置联系起来。他的想法是利用这些数据来找人。如果你知道某个监控目标的用户ID，你就可以在该目标使用机场或酒店无线网络时设置警报，并了解他的旅行时间。你还可以识别出你认识的某个人，他在一系列的日期和时间里去过某个特定的地理区域。例如，假设你正在寻找一个用三个不同的付费电话匿名给你打电话的人。你知道这些电话的日期和时间，以及这些付费电话的位置。如果那个人的口袋里有一部可以自动登录无线网络的智能手机，那么你就可以将登录数据库与你感兴趣的日期和时间以及这些网络的位置联系起来。很可能只会有一个匹配。

卡内基梅隆大学的研究人员也做了类似的事情。他们在公共场所安装了一个摄像头，捕捉路过的人的图像，用面部识别软件和Facebook的公共标记照片数据库识别他们，并将这些名字与其他数据库关联起来。结果是，他们能够在一个人走过的时候实时显示他或她的个人信息。任何人都可以通过智能手机摄像头或谷歌眼镜轻松获得这项技术。

有时，跨数据集连接身份很容易;你的手机与你的名字相连，你的信用卡也是如此。有时候会比较困难;你的电子邮件地址可能和你的名字没有联系，除非时报的人在电子邮件中提到你的名字。像Initiate Systems这样的公司出售将多个数据集的数据关联起来的软件;他们既卖给政府也卖给企业。公司还将你的线上行为与线下行为联系起来。例如，Facebook正在与数据代理商Acxiom和Epsilon合作，将你的在线资料与店内购买相匹配。

一旦你可以将不同的数据集关联起来，你就可以用它们做很多事情。想象一下，在不查看病人记录的情况下建立一个人的健康状况。信用卡记录和超市亲和卡可以显示他买了什么食物和酒，

他在哪家餐馆吃饭，他是否有健身房会员卡，以及他在药店买了哪些非处方药。他的手机会显示他去那家健身房的频率，他的活动追踪器会显示他在那里时的活动水平。网站上的数据显示了他搜索过的医学术语。这就是ExactData这样的公司如何出售网上约会的人、赌博的人、患有焦虑症、失禁或勃起功能障碍的人的名单。

刺穿我们的匿名性

当一个强大的组织对我们电子基础设施的重要部分进行窃听，并能将各种监控流联系起来时，它通常可以识别出试图隐藏的人。这里有四个故事来说明这一点。

1. 中国军方黑客涉嫌对美国政府和企业进行一系列广泛的攻击，因为他们从用于实施攻击的同一网络基础设施访问Facebook，因此被认定为黑客。

2. 赫克托·蒙斯格尔(Hector Monsegur)是因入侵众多商业网络而受到调查的LulzSec黑客运动的领导人之一，他于2011年被FBI确认并逮捕。虽然他通常使用良好的计算机安全措施，并使用匿名中继服务来保护自己的同一性，但他还是犯了一次错误。在一次聊天中，一名调查人员无意中发现了他的汽车，从而在YouTube上找到了一段视频，然后找到了他的Facebook页面。

3. 与中央情报局局长大卫·彼得雷乌斯有染的保拉·布罗德威尔同样采取了广泛的预防措施来隐藏自己的同一性。她从来没有从家庭网络登录过她的匿名电子邮件服务。相反，她在给他发电子邮件时使用的是酒店和其他公共网络。FBI将几家不同酒店的登记数据联系起来，她的名字是通用的。

4. 黑客组织Anonymous的一名名为“w0rmer”的成员因入侵美国执法网站而被通缉，他使用了一个匿名推特账户，但链接到一张用iPhone拍摄的女性乳房照片。照片中嵌入的GPS坐标指向澳大利亚的一所房子。另一个提到wormer的网站也提到了Higinio奥乔亚这个名字。警方掌握了奥乔亚的Facebook页面，其中包括他有一个澳大利亚女友的信息。女友的照片与引发这一切的原始照片相符，警方逮捕了沃默，又名奥乔亚。

在无处不在的监控下保持网络匿名几乎是不可能的。如果你忘记启用你的保护，或者点击错误的链接，或者输入错误的东西，你已经永久地将你的名字附加到你正在使用的任何匿名提供商。面对集中而坚决的调查，维护隐私和匿名所需的操作安全水平甚至超出了训练有素的政府特工的资源。就连一支训练有素的以色列刺客团队，也在迪拜根据城市周围的监控录像，迅速被指认出来。

对于大量的匿名数据集也是如此。我们可能会naïvely认为我们人太多了，很容易隐藏在数据的海洋中。或者我们的大部分数据都是匿名的。这是不正确的。大多数匿名化数据的技术都不起作用，而且数据的去匿名化只需要很少的信息。

2006年，AOL公布了65.7万用户三个月的搜索数据:总共有2000万次搜索。当时的想法是，这将对研究人员有用;为了保护人们的同一性，他们用数字代替了名字。所以，比如，Bruce Schneier可能是608429。当研究人员能够通过将个人搜索历史中的不同项目关联起来，将名字与数字联系起来时，他们感到很惊讶。

2008年，Netflix公布了50万匿名客户对1000万部电影的排名，作为挑战的一部分，人们需要想出比该公司当时使用的推荐系统更好的推荐系统。研究人员通过将排名和时间戳与互联网电影数据库(Internet Movie Database)中的公开排名和时间戳进行比较，能够对人们进行去匿名化处理。

这些看起来可能是特殊情况，但相关性机会比你想象的要频繁得多。例如，可以访问电话记录的匿名数据集的人可能会通过将其与目录商家的电话订单数据库相关联来部分地去匿名化它。或者，亚马逊的在线书评可能是使信用卡购买细节数据库部分去匿名化的关键。

计算机科学家拉塔尼亚·斯威尼利用1990年人口普查的公开匿名数据发现，美国2.48亿人口中有87%的人，也就是2.16亿人，可以通过他们的五位数邮政编码、性别和出生日期来唯一识别。对于大约一半的人来说，只需要一个城市、城镇或直辖市的名称就足够了。其他研究人员使用2000年的人口普查数据报告了类似的结果。

谷歌拥有用户互联网搜索的数据库，可以对互联网购物的公共数据库进行去匿名化处理，或者对医疗术语的搜索进行零化处理，从而对公共卫生数据库进行去匿名化处理。维护详细的客户和购买信息的商家可以使用他们的数据对任何大型搜索引擎的搜索数据进行部分去匿名化处理。拥有多家公司数据库的数据经纪人可能能够将这些数据库中的大部分记录去匿名化。

研究人员已经能够通过将数据与家谱网站和其他来源的信息进行比较，从匿名DNA中识别出人们的身份。甚至像阿尔弗雷德·金赛在20世纪30年代和40年代的性研究数据也不安全。金赛煞费苦心地保护他的研究对象的匿名性，但在2013年，研究员拉奎尔·希尔(Raquel Hill)能够识别出其中97%的人。

这是违反直觉的，但它需要比我们想象的更少的数据来唯一地识别我们。尽管我们都很典型，但我们仍然与众不同。事实证明，如果你剔除每个人都看的前100部电影，我们的观影习惯都是非常个性化的。我们的读书习惯、网上购物习惯、打电话习惯和网络搜索习惯也是如此。我们可以通过我们的人际关系被独一无二地识别出来。很明显，你可以通过你的位置数据被唯一识别。有了手机上的24/7位置数据，你的名字就能被发现，不需要太大的麻烦。你甚至不需要所有这些数据;95%的美国人仅仅*通过*四个时间/日期/地点点就能识别出他们的*名字*。

遗憾的是，针对这一问题的明显对策是不够的。公司通过删除一些数据，更改时间戳，或在他们替换名称的唯一ID号中插入故意错误来匿名化数据集。然而，事实证明，这类调整只会让去匿名化变得更加困难。

这就是为什么基于“个人识别信息”概念的监管不起作用的原因。PII通常被定义为姓名、唯一账号等，以及

特殊规则适用于它。但PII也与数据量有关;某人掌握的关于你的信息越多，甚至是匿名信息，她就越容易识别出你。

在大多数情况下，我们的保护仅限于我们使用的公司的隐私政策，而不是通过任何技术或数学。而通过一个唯一的数字来识别，往往也不能提供太多的保护。这些数据仍然可以被收集、关联和使用，最终我们会做一些事情，把我们的名字附加到那个“匿名”的数据记录上。

在无处不在的监控时代，每个人每时每刻都在收集我们的数据，匿名性是脆弱的。我们要么需要开发更强大的技术来保护匿名性，要么完全放弃这个想法。

4

监视业务

他们也在做着同样的事情。大多数人惊讶不戴手表的东西，大概是因为今天他们的手机手机是有多少个时钟的。其他人的东西不带摄像头，因为它们是大多数智能手机的标配。

相机闪光灯也可以当手电筒使用。其中一款适用于安卓手机的手电筒应用是GoldenShores Technologies, LLC公司开发的“最亮手电筒免费版”(Brightest flashlight Free)。这款应用非常好用，而且有很多很酷的功能。评论者把它推荐给去玩“不给糖就捣蛋”的孩子们。评论者没有提到的一个功能是，这款应用收集了用户的位置信息，据称还把这些信息卖给了广告商。

实际情况要复杂得多。公司的隐私政策，不管有没有人看，都是在主动误导消费者。它说公司会使用收集到的任何信息，但却没有提到这些信息会卖给第三方。而且，尽管用户必须点击他们也没有阅读的许可协议上的“接受”，但在人们点击之前，这款应用就开始收集和发送位置信息了。

当研究人员在2012年发现这一问题时，这让该应用的5000万用户几乎都感到惊讶。美国联邦贸易委员会介入，迫使该公司清理其欺诈行为并删除其收集的数据。不过，由于这款应用是免费的，它并没有对该公司处以罚款。

想象一下，美国政府通过了一项法律，要求所有公民携带追踪设备。这样的法律会立即被认定为违宪。然而，我们走到哪里都带着手机。如果当地的警察部门要求我们每交一个新朋友都要通知它，整个国家都会反抗。但我们还是通知了Facebook。如果这个国家的间谍要求我们所有的谈话和通信的副本，人们会拒绝。然而，我们却向我们的电子邮件服务提供商、手机公司、社交网络平台和互联网服务提供商提供了副本。

绝大多数的监控都是由企业进行的，它之所以发生，是因为我们表面上同意了它。我并不是说我们在知情的情况下做出了同意的决定;相反，我们接受它，要么是因为我们从服务中获得了价值，要么是因为我们得到了包括监控在内的一揽子交易，在这件事上没有任何真正的选择。这就是我在导言中谈到的交易。

本章主要是关于互联网监控，但请记住，一切都是——或者很快就会——与互联网相连。互联网监控实际上是互联网连接世界中监控的简写。

网络监控

所有这些企业互联网监控的主要目标是广告。其中也有一些市场调查和客户服务，但这些活动都是次要的，主要目的是更有效地向你销售东西。

传统上，互联网监控是基于一种叫做cookie的东西。这个名字听起来很温和，但技术描述“持久标识符”要准确得多。cookie并不是用来做监控设备的;相反，它们的设计目的是让上网更容易。网站本身并不会记住你一次又一次的访问，甚至是一次又一次的点击。cookie为这个问题提供了解决方案。每个cookie包含一个唯一的号码，允许网站识别您的身份。所以现在当你点击一个互联网商家的网站时，你会不断地告诉它，“我是顾客#608431。”这样网站就能找到你的账户，把你的购物车挂在你身上，下次你来的时候记得你，以此类推。

公司很快意识到，他们可以在属于其他网站的页面上设置自己的cookie——在获得他们的许可并支付特权的情况下——于是第三方cookie诞生了。像DoubleClick(2007年被谷歌收购)这样的企业开始在许多不同的网站上跟踪网络用户。这就是广告开始在网络上跟踪你的时候。搜索特定的汽车或度假目的地或医疗状况，几周后，你会在你访问的每个商业网站上看到该汽车或城市或相关药物的广告。

这已经演变成一个令人震惊的广泛、强大和有利可图的监控架构。你在互联网上的任何地方都被许多公司和数据经纪人跟踪:一个网站上有十家不同的公司，另一个网站上有十几家公司。Facebook跟踪你在每个网站上的Facebook喜欢按钮(无论你是否登录到Facebook)，谷歌跟踪你在每个网站上有谷歌加+1按钮或简单地使用谷歌分析来监控自己的网络流量。

大多数跟踪你的公司都有你从未听说过的名字:Rubicon Project, AdSonar, Quantcast, Pulse 260, Undertone, Traffic Marketplace。如果你想知道是谁在跟踪你，那就安装一个可以监控cookie的浏览器插件吧。我保证你会吓一跳。一位记者发现，有105家不同的公司在36小时内跟踪他的互联网使用情况。2010年，像Dictionary.com这样看似无害的网站在你访问时在你的浏览器上安装了200多个跟踪cookie。

在你的智能手机上也是如此。那里的应用程序也会跟踪你。它们会追踪你的位置，有时还会下载你的地址簿、日历、书签和搜索历史记录。2013年，说唱歌手Jay-Z和三星合作，为下载应用程序的用户提供在Jay-Z新专辑发行前收听的功能。这款应用要求用户能够查看手机上的所有账户，追踪手机的位置，并追踪用户正在与谁通话。而《愤怒的小鸟》这款游戏甚至会在你不玩游戏的时候收集位置数据。

康卡斯特(Comcast)等宽带公司也对用户进行监控。如今，他们主要监控用户是否非法下载了受版权保护的歌曲和视频，但其他应用也不甘落后。威瑞森、微软和其他公司正在开发一种机顶盒，它可以监控房间里发生的事情，并提供广告

基于这些信息。

少了老大哥，多了几百个搬弄是非的小兄弟。

如今，网络监控远比饼干更顽固。事实上，一场小规模的军备竞赛正在进行。你的浏览器——甚至是谷歌chrome——都有屏蔽或删除cookie的广泛控制，很多人都启用了这些功能。DoNotTrackMe是最受欢迎的浏览器插件之一。互联网监控行业则以“flash cookies”作为回应——基本上就是类似cookie的文件，存储在Adobe的flash播放器中，当浏览器删除cookie时还会保留下来。要屏蔽这些文件，你可以安装FlashBlock。但还有其他方法可以唯一地跟踪你，比如evercookies、帆布指纹和cookie同步等深奥的名字。不仅仅是营销人员这么做;2014年，研究人员发现白宫网站使用了evercookies，违反了自己的隐私政策。我将在第15章给出一些关于阻止网络监控的建议。

cookie本质上是匿名的，但公司越来越能够将它们与其他能够肯定我们身份的信息联系起来。你自愿向许多互联网服务表明自己的身份。通常你只使用用户名，但越来越多的用户名可以与你的真实姓名联系在一起。谷歌试图通过其“实名政策”来强制用户使用他们的合法姓名注册谷歌加，直到2014年取消了这一政策。Facebook要求实名制。任何时候你用你的信用卡号买东西，你的真实同一性都与参与交易的公司设置的任何cookie绑定在一起。你在智能手机上的任何浏览都与你作为手机主人的身份联系在一起，尽管网站可能不知道这一点。

免费又方便

监控之所以是互联网的商业模式，主要有两个原因:人们喜欢免费，人们喜欢方便。然而，事实是，人们并没有太多的选择。要么被监视，要么什么都不做，而且监视很方便，是看不见的，所以你不用去想它。这一切之所以成为可能，是因为美国法律未能跟上商业实践的变化。

1993年之前，互联网完全是非商业性的，免费成为网络规范。当商业服务第一次冲击互联网时，有很多关于如何收费的讨论。很快就发现，除了投资和色情网站等少数孤立的情况外，人们甚至不愿意为访问支付哪怕一小笔费用。就像电视的商业模式一样，广告是唯一有意义的收入模式，而监控让这种广告更加有利可图。网站可以对个人定向广告收取比广播广告更高的价格。这就是为什么我们最终得到了名义上免费的系统，这些系统收集和出售我们的数据以换取服务，然后用广告轰炸我们。

“免费”是一个特别的价格，有各种各样的心理学研究表明，人们在这个价格周围不会理性地行动。我们高估了免费的价值。当某样东西是免费的时候，我们会消费得过多。我们强迫别人去消费它。免费扭曲了我们对成本与收益的正常观念，人们最终会交易他们的

以低于其价值的价格获取个人数据。

公司故意确保隐私对用户来说不突出，这加剧了这种低估隐私的倾向。当你登录Facebook时，你不会想到你向公司泄露了多少个人信息;你会和朋友聊天。当你早上醒来的时候，你不会去想怎么让一堆公司全天跟踪你;你只是把手机放进了口袋。

其结果是，互联网公司可以通过减少用户隐私来改善他们为实际客户提供的产品。多年来，Facebook一直在系统地做这件事，定期更新其隐私政策，以获得更多访问你数据的机会，同时减少你的隐私。Facebook也改变了默认设置，让更多的人可以看到你的名字、照片、涂鸦墙、你发布的照片、点赞等等。b谷歌也做了同样的事情。2012年，它宣布了一项重大变化:谷歌将把来自搜索、Gmail、YouTube(谷歌拥有)、谷歌Plus等网站的数据链接到一个关于你的大数据集。

在这一点上，苹果多少是个例外。该公司的存在是为了推销消费产品，尽管它可以监视iCloud用户的电子邮件、短信、日历、地址簿和照片，但它没有这样做。它只使用iTunes的购买信息来推荐用户可能想要购买的其他歌曲和视频。2014年底，苹果开始将此作为一种市场差异化手段。

便利是我们愿意将高度个人数据交给企业利益集团，并忍受成为他们监控对象的另一个原因。正如我一直在说的，基于监控的服务是有用的，也是有价值的。当我们可以访问我们的地址簿、日历、照片、文件和我们碰巧在附近的任何设备上的其他所有东西时，我们喜欢它。我们喜欢Siri和谷歌Now这样的服务，当它们对你了解很多的时候，它们的效果最好。社交网络应用让我们更容易和朋友一起出去玩。谷歌地图、Yelp、天气预报和优步等手机应用程序在知道我们的位置后运行得更好更快。让Pocket或Instapaper这样的应用程序知道我们正在阅读的内容，感觉就像在一个方便的地方获得我们想要阅读的一切所付出的小小代价。我们甚至喜欢广告正好针对我们感兴趣的内容。监控在这些和其他应用中的好处是真实的，而且是显著的。

我们尤其不介意一家公司收集我们的数据，并将其用于自己的服务中，以更好地为我们服务。这就是为什么当人们抱怨企业监控时，很少提到亚马逊的推荐。亚马逊会根据你买过的东西和别人买过的东西不断向你推荐东西。亚马逊在收集你的数据的同一背景下使用你的数据，这对用户来说是完全透明的。这对亚马逊来说是一笔很大的生意，人们基本上接受了它。然而，当他们的数据在未经他们知情或同意的情况下被买卖和使用时，他们就开始反对了。

数据经纪人行业

客户监控的历史要比互联网早得多。在互联网出现之前，有四种基本的监控流。第一种来自公司对客户的记录。这是一家制造供应公司，知道它的企业客户订购什么，谁来订购。这是诺德斯特龙(Nordstrom)记住客户的尺寸和他们喜欢的剪裁类型，航空公司和酒店跟踪他们的常客。最终，这演变成了数据库，使公司能够从最初的询问到最终的购买全程跟踪销售线索，以及零售会员卡，为消费者提供折扣，但其真正目的是跟踪他们的购买情况。现在，许多公司向各种规模的公司提供客户关系管理(CRM)系统。

第二个传统的监控流是直接营销。纸质邮件是媒介，目的是为公司提供想要接收营销邮件的人的名单，而不是浪费邮资给那些不希望收到营销邮件的人。这必然是粗糙的，基于人口统计、杂志订阅或相关企业的客户名单等因素。

第三流来自征信机构。这些公司收集人们的详细信用信息，并将这些信息卖给银行，以确定是否向个人提供贷款以及以什么利率贷款。这一直是一种相对昂贵的个人数据收集形式，只有在大量资金受到威胁时才有意义:发行信用卡，允许某人租赁公寓，等等。

第四股来自政府。它由各种公共记录组成:出生和死亡证明、驾驶执照记录、选民登记记录、各种许可证和执照等等。越来越多的公司能够下载，或者购买这些公共数据。

信用机构和直销公司将这四种数据流结合在一起，成为像Acxiom这样的现代数据经纪人。这些公司从与你有业务往来的公司那里购买你的个人数据，与你的其他信息结合起来，再卖给那些想要更多了解你的公司。而且他们也搭上了电脑化的顺风车。你产生的数据越多，他们收集的数据就越多，他们对你的描述也就越准确。

数据经纪人掌握的信息的广度和深度是惊人的。他们收集人口统计信息:姓名，地址，电话号码，电子邮件地址，性别，年龄，婚姻状况，家庭中子女的存在和年龄，教育程度，职业，收入水平，政治派别，驾驶汽车，以及关于房屋和其他属性的信息。他们收集你买过的东西的清单，你什么时候买的，以及你是如何付款的。他们记录着你家人的死亡、离婚和疾病。他们收集你在互联网上所做的一切。

数据经纪人利用你的数据把你分成各种有市场的类别。想要“潜在继承人”或“有年迈父母的成年人”类别的人的名单，或者“关注糖尿病”或“老年人需求”的家庭地址?Acxiom可以提供给你。InfoUSA出售的是“受苦的老年人”和易受骗的老年人名单。2011年，数据经纪公司Teletrack出售申请非传统信贷的人的名单

发薪日贷款等产品卖给那些想把他们作为不良金融交易目标的公司。2012年，经纪商Equifax向一家折扣贷款公司出售了拖欠抵押贷款的人的名单。由于这是金融信息，两家经纪人都因其行为被FTC罚款。几乎所有其他的事情都是公平的。

个性化广告

我们使用监视我们的系统来换取服务。这就是当今互联网的运作方式。如果某样东西是免费的，你就不是顾客;你就是产品。或者，正如戈尔所说，“我们有一个跟踪者经济。”

广告一直存在这样一个问题:大多数看到广告的人并不关心产品。啤酒广告在不喝啤酒的人身上是浪费。一个汽车广告很大程度上是浪费，除非你在市场上买一辆车。但由于不可能对单个广告进行定向投放，所以各公司只能利用手头的数据尽其所能。他们根据地理位置对人群进行细分，并猜测哪些杂志和电视节目最能吸引他们的潜在客户。他们将人口作为一个整体，或者是一个大的人口群体进行追踪。这是非常低效的。有一句名言，最可靠地追溯到零售业巨头约翰·沃纳梅克:“我知道我的广告有一半是浪费的。问题是，我不知道是哪一半浪费了。”

无处不在的监控有可能改变这一点。如果你确切地知道谁想买割草机，或者谁担心勃起功能障碍，你就可以在正确的时间把广告投放到正确的人身上，消除浪费。(事实上，一家全国性的草坪护理公司就利用航拍来更好地推销自己的服务。)如果你知道潜在客户的细节——什么样的论点最有说服力，什么样的图片最吸引他——你的广告就会更有效。

这也适用于政治广告，并且已经改变了政治竞选的进行方式。奥巴马在2008年和2012年都使用了大数据和个人营销，取得了巨大的效果，其他两党候选人也纷纷效仿。这些数据被用来针对筹款活动和个性化的政治信息，并确保你在选举日那天真的去了投票站——假设数据库显示你投票给了正确的候选人。

很多商业监控数据都充满了错误，但这些信息即使不是很准确，也是有价值的。即使你最终有三分之一的时间把你的广告展示给了错误的人，你仍然可以有一个有效的广告活动。重要的不是完美的定位准确性;而是数据比以前好得多。

例如，在2013年，研究人员能够通过分析与其他推特用户的相似性来确定人们在推特上的实际位置。他们的准确率并不完美——他们只能以58%的准确率预测用户所在的城市——但对于大量的商业广告来说，这种精确度已经足够了。

尽管如此，大量证据表明，基于监控的广告被夸大了。那里

向人们展示他们想要的东西的广告是有价值的，尤其是在他们正考虑购买的时候。这就是谷歌试图用Adwords做的事情，它的服务是在搜索结果旁边放置广告。这也是所有零售商试图做的“买了这个的人也买了这个”的广告。但这类事情都是建立在最低限度的监控基础上的。

目前尚不清楚的是，更多的数据有多大帮助。了解人们广泛的个人细节是有价值的:他们是同性恋，他们正在结婚，他们正在考虑去热带度假，他们有一定的收入水平。虽然知道你对SUV感兴趣而不是敞篷车对汽车公司来说可能是非常有价值的，但知道你更喜欢蓝色而不是绿色的，这一点就更有价值了。如果知道你有两个孩子，其中一个还需要汽车座椅，那就没那么有价值了。或者其中一个孩子死于车祸。是的，经销商会首先推出更大的SUV，然后再宣传安全性，但两者的收益递减。而且，过于有针对性的广告会让人感到毛骨悚然，可能会让客户失去兴趣。

机器人技术的一个概念在这里很有用。我们倾向于接受那些明显看起来像机器人的机器人，以及那些看起来完全像人类的机器人。但我们对那些看起来很像人但看起来不完全像人的机器人感到非常不舒服。日本机器人专家Masahiro Mori将这种现象称为“恐怖谷”。科技评论家Sara M. Watson认为，广告业也存在类似的现象。人们可以接受草率的个性化广告，也可以接受无缝、微妙的个性化广告，但当他们看到足够多的东西，意识到自己被操纵了，或者当广告与他们的自我意识不符时，他们就会感到毛骨悚然。

随着时间的推移，这一切都会改变，因为我们已经习惯了个性化广告。“令人毛骨悚然”的定义是相对的、流动的，很大程度上取决于我们对相关技术的熟悉程度。现在，在互联网上跟踪我们的广告会让人觉得毛骨悚然。毛骨悚然也是一种自我纠正。谷歌对不允许的搜索广告有一个长期而复杂的政策，因为用户发现某些类型的广告太令人毛骨悚然。其他公司则允许用户点击链接，以了解他们为什么会成为某个特定广告的目标，希望这能让用户更适应这个过程。

另一方面，有些公司只是把它隐藏得更好。在塔吉特发现少女怀孕的消息传开后，该公司改变了向人们发送定向广告的方式。它并没有停止向它认为怀孕的女性投放广告，但它将这些定向广告嵌入到更普通的广告中。这些邮件的收件人并不觉得有针对性，所以他们不那么被广告吓到。

与此同时，广告在我们的环境中盛行，这使得个人广告的价值降低了，原因有两个。首先，随着广告充斥我们的世界，单个广告的价值下降了。这是因为我们要花的钱的总量并没有改变。例如，所有的汽车制造商都在争夺你将购买的那一辆车的利润。如果你看到十倍的广告，每一个都只值十分之一的价格，因为最终你只会买一辆车。

第二，我们更擅长把广告屏蔽掉。自从20世纪70年代中期模拟录像机普及以来，电视广告商就注意到他们的

广告要快进，因为有很多人就是这么看的。网络广告为吸引我们的注意力而发动了一场更为复杂的战斗。最初，广告是页面顶部的横幅广告。当我们学会了如何忽略它们时，广告商把广告放在了页面的主要部分。当我们学会忽略它们时，它们开始闪烁并播放视频。现在它们越来越多地干扰我们想要阅读的内容，所以我们需要故意把它们赶走。超过5000万人在他们的浏览器上安装了AdBlock Plus来帮助他们做到这一点。

其结果是，在互联网广告整体成本不断上升的情况下，单个互联网广告的价值却在迅速下降。相应地，我们的数据对广告主的价值也在快速下降。几年前，详细的消费者资料很有价值;现在很多公司和数据经纪人都有数据，这是一种常见的商品。对2013年财务报告的一项分析计算出，每个用户对bb0的价值为每年40美元，而对Facebook、LinkedIn和雅虎的价值仅为6美元。这就是b谷歌和Facebook等公司不断加大赌注的原因。他们需要越来越多关于我们的数据来卖给广告商，从而使自己在竞争中脱颖而出。

有可能我们已经达到了顶峰，广告作为收入来源的盈利能力将开始下降，最终作为唯一的商业模式变得不可持续。我想没有人知道，如果广告泡沫破裂，基于监控的营销被证明无效，互联网会变成什么样子，互联网公司需要回归到更传统的商业模式，比如向用户收费。

新的中间商巩固了权力

互联网早期的一个比喻是，它将消除传统的企业中间商。你不再需要依靠报纸来策划每天的新闻，并将其以易于阅读的纸质包装提供给你。你可以出去设计自己的报纸，从这里和那里取点东西，创造出你想要的东西。同样，你也不再需要依靠集中的店面来积累和转售收藏品;eBay直接连接买家和卖家。音乐推广和分销、机票，以及在某些情况下的广告，都是如此。旧的守门人的商业模式依赖于低效的技术，而互联网改变了这种动态。

今天更是如此。AirBnB允许个人与传统连锁酒店竞争。TaskRabbit让想做零工的人和需要做零工的人更容易联系起来。Etsy、CafePress和eBay都绕过了传统的跳蚤市场。Zillow和Redfin绕过房地产经纪人，eTrade绕过投资顾问，YouTube绕过电视网。Craigslist绕过了报纸的分类广告。Hotwire和Travelocity绕过了旅行社。

这些新公司或许打破了传统的古玩店、报纸、出租车公司的权力集团，但通过控制买卖双方之间的信息流，它们自己也成为了强大的中间商。我们越来越多地看到新旧中间商在市场上的战斗:苹果和它的iTunes商店对抗

音乐产业，亚马逊与传统出版业，优步与出租车公司。新的信息中间商正在取得胜利。

b谷歌首席执行官埃里克·施密特说:“我们相信现代技术平台，如谷歌、Facebook、亚马逊和苹果，比大多数人意识到的更强大……而赋予它们力量的是它们的增长能力——具体来说，是它们的扩展速度。”除了生物病毒，几乎没有什么能像这些技术平台那样迅速、有效或积极地扩展，这也使得构建、控制和使用它们的人变得强大起来。”

施密特所指的是信息中间商固有的垄断性。各种经济效应奖励先行者，惩罚后来者，诱使人们加入最大的网络，并使他们难以切换到竞争系统。其结果是，这些新的中间商比他们所取代的中间商拥有更大的权力。

百度控制着美国三分之二的搜索市场。几乎四分之三的互联网用户拥有Facebook账户。亚马逊控制着美国30%的图书市场和70%的电子书市场。康卡斯特拥有美国宽带市场约25%的份额。这些公司仅仅因为他们的经济地位就对我们拥有巨大的权力和控制权。

他们都收集和使用我们的数据来增加他们的市场主导地位和盈利能力。当eBay刚开始的时候，买家和卖家在eBay系统之外很容易沟通，因为人们的电子邮件地址在很大程度上是公开的。2001年，eBay开始隐藏电子邮件地址;2011年，它禁止了商品列表中的E-mail地址和链接;2012年，又禁止它们在用户间通信。所有这些举措都有助于将eBay定位为一个强大的中介，使买家和卖家更难将建立在eBay内部的关系转移到eBay之外。

越来越多的公司利用他们的权力来影响和操纵他们的用户。从广告中获利的网站花费大量精力确保你花尽可能多的时间在这些网站上，优化他们的内容，以最大限度地让你上瘾。少数几个允许你选择退出个性化广告的网站让你很难找到这样的选择。一旦公司将这些技术与个人数据结合起来，结果将更加阴险。

我们与许多我们所依赖的互联网公司的关系，并不是传统的公司-客户关系。这主要是因为我们不是客户。我们是那些公司卖给他们*真正*客户的产品。这种关系比商业关系更封建。这些公司类似于封建领主，我们是他们的附庸、农民，运气不好的时候是农奴。我们是这些公司的佃农，在他们的土地上工作，提供数据，然后他们出售以获取利润。

是的，这是一个比喻，但它经常给人的感觉是这样的。有些人已经宣誓效忠b谷歌。他们有Gmail账户，使用谷歌日历和谷歌文档，并拥有安卓手机。其他人也承诺效忠于苹果。他们有imac、iphone和ipad，并让iCloud自动同步和备份

所有东西。还有一些人让微软包揽一切。我们中的一些人几乎完全放弃了电子邮件，转而使用Facebook、Twitter和Instagram。我们可能更喜欢一个封建领主而不是其他领主。我们可能会在其中几个公司中分配我们的忠诚，或者故意避开我们不喜欢的某个公司。无论如何，我们越来越难以不对其中至少一家公司宣誓效忠。

毕竟，客户在拥有封建领主的过程中获得了很多价值。让别人来保管我们的数据、管理我们的设备，简单来说更容易、更安全。我们喜欢让别人来管理我们的设备配置、软件管理和数据存储。我们喜欢我们可以在任何地方，从任何电脑上访问我们的电子邮件，我们喜欢Facebook可以在任何地方，从任何设备上运行。我们希望我们的日历条目能自动出现在我们所有的设备上。云存储网站在备份我们的照片和文件方面做得比我们自己管理的要好;苹果公司在阻止恶意软件进入iPhone应用商店方面做得很好。我们喜欢自动安全更新和自动备份;这些公司在保护我们的设备方面比我们做得更好。我们真的很高兴，当我们失去了智能手机，买了一个新的，我们所有的数据在一个按钮下就会重新出现在它上面。

在这个新的计算世界里，我们不再需要管理我们的计算环境。我们相信封建领主会善待我们，保护我们免受伤害。这都是两种技术趋势的结果。

首先是云计算的兴起。基本上，我们的数据不再存储和处理在电脑上。这一切都发生在许多不同公司拥有的服务器上。结果是我们不再控制我们的数据。这些公司为了任何他们想要的盈利目的而访问我们的数据——包括内容和元数据。他们精心制定了服务条款，规定了我们可以在他们的系统上存储哪些类型的数据，如果他们认为我们违反了这些条款，他们可以删除我们的整个账户。他们在我们不知情或未经我们同意的情况下，将我们的数据交给执法部门。更糟糕的是，我们的数据可能存储在数据保护法不那么严格的国家的计算机上。

第二个趋势是由供应商密切管理的用户设备的兴起:iphone、ipad、安卓手机、kindle、chromebook等。其结果是，我们不再能够控制我们的计算环境。我们已经放弃了对我们能看到什么、能做什么、能使用什么的控制。对于iOS设备上可以安装哪些软件，苹果是有规定的。你可以把自己的文档加载到你的Kindle上，但是亚马逊可以删除它已经卖给你的书。2009年，由于版权问题，亚马逊从用户的kindle中自动删除了乔治·奥威尔(George Orwell)的《*1984*》(1984)的一些版本。我知道，你就是没法把这些东西写得更讽刺了。

即使是两大电脑操作系统，微软的Windows 8和苹果的Yosemite，也在朝着这个方向发展。两家公司都在推动用户只从集中商店购买授权应用。每次操作系统升级后，我们的电脑看起来更像是智能手机。

不仅仅是硬件。买一个软件，然后在你的电脑上随心所欲地使用，已经变得越来越难了。越来越多的供应商开始转向订阅

adobe在2013年推出了Creative Cloud，这给了供应商更多的控制权。微软还没有放弃购买模式，但它的MS Office订阅服务非常有吸引力。而且Office 365将文档存储在微软云上的选项很难关闭。很多公司都在推动我们朝这个方向发展，因为它能让我们作为客户或用户获得更多利润。

考虑到目前的法律，信任是我们唯一的选择。没有一致或可预测的规则。我们无法控制这些公司的行为。我无法就雅虎何时能访问我在Flickr上的照片的规定进行谈判。我不能要求对我在Prezi上的演示文稿或在Trello上的任务列表提供更高的安全性。我甚至不知道这些公司将基础设施外包给了哪些云服务提供商。如果这些公司中的任何一家删除了我的数据，我没有权利要求它回来。如果这些公司中的任何一家允许政府访问我的数据，我也没有追索权。如果我决定放弃这些服务，很可能我不能轻易带走我的数据。

政治学家亨利·法雷尔(Henry Farrell)观察到，“我们的大部分生活都是在网上进行的，换句话说，我们的大部分生活都是在大型私营企业制定的规则下进行的，这些规则既不受太多监管，也不受太多真正的市场竞争的影响。”

常见的辩护是类似于“生意就是生意”的说法。没有人被迫加入Facebook或使用谷歌搜索或购买iPhone。潜在客户之所以选择加入这些准封建的用户关系，是因为他们从中获得了巨大的价值。如果他们不喜欢，他们就不应该这么做。

这个建议不实际。告诉人们，如果他们不喜欢数据收集，他们就不应该发电子邮件、网上购物、使用Facebook或使用手机，这是不合理的。我无法想象学生们在没有互联网搜索或维基百科的情况下完成学业，更不用说事后找工作了。这些都是现代生活的工具。它们是事业和社会生活所必需的。在大多数情况下，对我们大多数人来说，选择退出是不可行的选择;它违反了已经成为非常现实的当代生活规范。

在提供者之间进行选择，并不是选择监视还是不监视，而只是选择
哪个封建领主可以监视你。

5

政府监察及管制

政府，很难不去理解，因为它是政府最严重的侵犯者，但因为监视。我们知道我会关注美国的活动——主要是由于爱德华·斯诺登的行为。

美国的国家安全监控在政治上、法律上和技术上都很强大。斯诺登的文件披露了至少三个不同的NSA收集bbb用户数据的项目。这些项目基于三种不同的技术窃听能力。它们依赖于三种不同的法律权威。它们涉及三家不同公司的合作。这是Gmail。几乎可以肯定，其他所有主要的电子邮件提供商也是如此——手机通话记录、手机定位数据和互联网聊天记录也是如此。

要理解监视在美国情报中的作用，你需要了解国家安全局(NSA)全球窃听任务的历史，以及间谍活动性质的变化。由于这段历史，NSA是政府的主要窃听组织。

NSA由杜鲁门总统于1952年成立，他将美国的信号情报和密码破译活动合并为一个组织。它过去是，现在仍然是美国军队的一部分，最初完全是一个外国情报收集组织。这一任务在冷战期间变得越来越重要。当时，对苏联的偷窥是常态，电子间谍是其中的重要组成部分——随着一切都被计算机化，电子通信变得更加普遍，这一点变得更加重要。随着我们的能力和需要收集的通信量的增加，我们收集的信息也越来越多。

其中一些是有用的，尽管很多是无用的。事实的秘密——比如苏联新型坦克的特点——要比意图的秘密——比如赫鲁晓夫下一步要做什么——容易了解得多。但这些都是我们的敌人，我们收集了一切可以收集的信息。

随着共产主义在20世纪80年代末和90年代初的垮台，这一独特的使命本应作为和平红利的一部分而减少。有一段时间的确如此，而NSA的另一项任务——保护通信不受他人监视——也变得越来越重要。NSA变得更加注重防御，更加开放。但在“9·11”恐怖袭击之后，窃听获得了新的、更激烈的生命力。当然，“再也不发生”是一个不可能完成的任务，但唯一有希望阻止某些事情发生的方法，就是了解正在发生的一切。这导致NSA将整个地球置于监视之下。

传统的间谍活动让政府对抗政府。我们监视外国政府和他们的代理人。但是恐怖主义的敌人是不同的。它

不就是一帮政府领导“在那边”吗;而是某个随机的恐怖组织，其成员可能在任何地方。现代政府监控监控着每一个人，无论是国内的还是国际的。

这并不是说政府对人口的监控是一件新鲜事。极权政府这么做已经有几十年了:苏联、东德、阿根廷、中国、古巴、朝鲜等等。在美国，NSA和联邦调查局在20世纪60年代和70年代监视各种各样的美国人——反战活动家、民权领袖和非暴力持不同政见的政治团体的成员。在过去的十年里，他们再次关注反战活动人士和非暴力持不同政见的政治团体成员，以及穆斯林美国人。随着NSA成为主要负责追踪海外基地组织的机构，这项最新任务变得越来越重要。

随着目标的改变，通信技术也发生了变化。在互联网出现之前，专注于对外通信很容易。一个中国的军事网络只承载中国的通信。俄罗斯的一个系统只用于俄罗斯的通信。如果NSA窃听了彼得罗巴甫洛夫斯克和符拉迪沃斯托克之间的海底电缆，它就不必担心不小心截获了底特律和克利夫兰之间的电话。

互联网的工作方式就不同了。每个人的通信都在同一个网络上混在一起。恐怖分子和其他人使用相同的电子邮件提供商。传送俄罗斯、伊朗和古巴政府通讯的电路也可能传送你的推特信息。纽约和洛杉矶之间的互联网电话可能最终会通过俄罗斯的海底电缆传输。里约热内卢de Janeiro和里斯本之间的通信可能要经过佛罗里达。谷歌不会把你的数据存储在山景城的公司总部;而是存放在世界各地的多个数据中心:智利、芬兰、台湾、美国和其他地方。随着全球电子通信网络的发展和扩大，不收集美国人的数据变得很难，即使他们不是目标。

与此同时，每个人都开始使用相同的硬件和软件。曾经有使用俄罗斯技术的俄罗斯电子产品、收音机和计算机。再也没有了。我们都在用微软的Windows、思科的路由器，以及同样的商业安全产品。你可以在大多数国家买到iPhone。这意味着，例如侵入中国军事网络或委内瑞拉电话通话的技术能力，可以推广到世界其他地方。

美国拥有世界上最广泛的监视网络，因为它有三大优势。它的情报预算比世界上其他国家的总和还要多。互联网的物理布线导致世界上大部分的流量要跨越美国边境，甚至是两个国家之间的流量。几乎所有世界上最大、最受欢迎的硬件、软件和互联网公司都位于美国，并受其法律管辖。美国是霸主。

NSA的监视目标在其绝密报告中被巧妙地描述为:“收集一切”、“了解一切”和“利用一切”。该机构窃听电信公司和有线电视公司的互联网，收集电子邮件、短信和浏览记录

历史记录、好友列表、地址簿、位置信息，以及几乎所有它能得到的信息。没有证据表明NSA在美国录下了所有的电话，但我们知道它(至少)在阿富汗和百慕大的SOMALGET项目下这样做了。国安局2013年的预算为108亿美元;它直接雇佣了大约3.3万人，还有更多的人是合同工。斯诺登泄露的文件之一是NSA和其他情报机构的绝密“黑色预算”;2013年的总金额为530亿美元。据估计，美国每年在情报方面的支出为720亿美元。

NSA用于现代监视基础设施的大部分资金来自于9/11战争后在阿富汗和伊拉克的努力:识别和定位敌方目标的进攻努力，以及识别和消除简易爆炸装置的防御努力。也就是说，这些能力是针对这些国家的网络开发的，因为世界上其他所有人都使用同样的设备，所以它们可以更便宜地部署在其他地方的系统上。

一个明显的问题出现了:这合法吗?真正的答案是，我们不知道。NSA目前的监控权力来自三个地方:

- 里根总统于1981年签署的第12333号行政命令，允许NSA在国外进行广泛的监视。它只对美国公民提供一些保护，但允许广泛收集、分析和保留美国人的数据。
- 2001年颁布的《美国爱国者法案》(USA PATRIOT Act)第215条允许NSA收集“任何有形的东西(包括书籍、记录、文件、文件和其他物品)”——关于任何人，而不仅仅是外国人——“用于调查，以防止国际恐怖主义或秘密情报活动”。最后一点听起来像是一种限制，但一个秘密法庭将其解释为包括对每个美国人的电话元数据的持续收集。
- 2008年《外国情报监视法》(FISA)修正案第702条追溯授权NSA在9/11事件后非法进行的收集活动。它扩大了NSA收集外国人数据的职权范围，而对美国公民的保护却微乎其微。NSA利用这一权力监视进入美国的互联网骨干连接，收集外国人和美国人的数据。

讨论没有就此结束的原因有两个方面。其一，这些法律中的许多监视条款，无论是作为非法搜查还是非法扣押，几乎肯定是违宪的。第二，NSA对这些法律的一些解释几乎肯定是非法的。这两个方面的挑战目前正在法庭上进行辩论。我相信，NSA目前所做的很多事情最终都会被法院叫停，而NSA目前所做的更多事情将会被新的立法叫停。当然，到那时，美国人将已经受到数十年的广泛监视，这很可能一直是nsa的战略。我将在第13章详细讨论这一点。

NSA收集了大量关于美国人的数据。其中一些是“偶然的”。也就是说，如果NSA监视法国的电话网络，它将收集法国和美国之间的通话数据。如果它监视大西洋下面的一条互联网电缆，它将收集美国人的数据，这些数据的流量恰好经过该电缆。NSA制定了最小化规则，旨在限制其收集、分析和保留的美国人数据的数量，尽管从我们了解到的很多情况来看，这些规则并没有很好地发挥作用。这些规则对于通信内容和元数据是不同的，而且

根据NSA用来证明连接合法性的法律权威，规则也有所不同。最小化并不意味着美国人的数据被删除;它只是意味着，除非有人真的想看，否则它会被匿名化。NSA在这里做了很多玩弄规则的事情，甚至那些试图监督NSA活动的人也承认，他们无法弄清楚它到底在做什么。

2014年，一份由斯诺登提供的对一些实际截获的通信的分析发现，有关无辜者(包括美国人和非美国人)的数据远远超过了有关授权情报目标的数据。这在一定程度上反映了情报的本质;即使是最小化的关于某人的信息，也会包含与无辜者的各种交流，因为从字面上讲，与目标的每一次交流，只要提供了任何有趣的信息，都会被保留下来。

NSA可能会成为头条新闻，但美国情报界实际上由17个不同的机构组成。当然，还有CIA。你可能听说过nro——国家侦察办公室——它负责国家的间谍卫星。然后是与所有四个军种有关的情报机构。司法部(包括FBI和DEA)、国务院、能源部、财政部和国土安全部以及其他一些机构都在进行监视。可能还有一个仍然保密的第18个机构。(这不太可能，但也有可能。直到20世纪70年代，也就是NSA成立20多年后，其任务的细节基本上都是保密的。)

在NSA之后，FBI似乎是最多产的政府监控机构。它与NSA紧密相连，两者共享数据、技术和立法权力。我们很容易忘记，《*卫报*》公布的第一份斯诺登文件——要求威瑞森公司交出其所有客户的通话元数据的命令——是FBI将数据移交给NSA的命令。我们知道NSA、CIA、DEA、DIA和国土安全部之间有相当大的共享。NSA代号为ICREACH的项目向超过23个政府机构提供监控信息，其中包括美国人的信息。

也就是说，与NSA的监视不同，FBI的监视传统上是在司法监督下通过搜查令程序进行的。根据美国宪法第四修正案，政府必须向法官证明，搜查可能合理地揭示犯罪证据。然而，FBI有权在没有搜查令的情况下，通过使用国家安全信函(nsl)收集各种个人信息，无论是有针对性的还是大量的。这些基本上是行政传票，由FBI发出，没有司法监督。2001年，根据《美国爱国者法案》(USA PATRIOT Act，第505条)，这些传票的范围被大大扩大，尽管这些传票最初的法律依据起源于1978年。今天，nsl通常用于从第三方获取数据:b谷歌的电子邮件，金融机构的银行记录，Dropbox的文件。

在美国，由于所谓的第三方原则，我们已经减少了对所有这些数据的隐私权。早在1976年，迈克尔·李·史密斯在巴尔的摩抢劫了一名妇女，然后在电话中多次骚扰她。在警方确认了符合史密斯描述的人之后，他们让电话公司在史密斯的电话线上安装了一个“笔录”，以创建史密斯拨打的所有电话号码的记录。之后

在证实了史密斯给那个女人打过电话后，他们拿到了他家的搜查令，并以抢劫的罪名逮捕了他。史密斯试图使笔录证据作废，因为警方没有获得搜查令。在1979年的一项裁决中，最高法院裁定没有必要申请搜查令:“本院一贯认为，一个人在自愿移交给第三方的信息中，对隐私没有合法的期望。”基本上，因为史密斯与他的电话公司分享了这些电话号码，他失去了对这些信息的隐私的任何期望。这在1979年可能是有道理的，当时我们几乎所有的数据都是由我们自己掌握的，离我们很近。但今天，我们所有的数据都在云端的某个地方，由不确定信任的第三方持有。

科技已经大大提高了FBI在没有搜查令的情况下进行监视的能力。例如，FBI(以及当地警方)使用一种叫做imsi捕集器的工具，这基本上是一个假的手机信号塔。如果你听说过它，你应该听说过它的代号黄貂鱼，它实际上是哈里斯公司销售的一种特殊类型的imsi捕集器。通过架设信号塔，它可以欺骗附近的手机连接到它。一旦这种情况发生，imsi捕获器就可以收集手机的身份和位置信息，在某些情况下，还可以窃听电话交谈、短信和网页浏览。FBI非常害怕在公众面前解释这种能力，因此该机构要求当地警察在使用该技术之前签署保密协议，并指示他们在法庭上使用该技术时撒谎。当佛罗里达州萨拉索塔的当地警方似乎有可能向针对他们的民权诉讼中的原告公布有关黄貂鱼手机监听设备的文件时，联邦法警没收了这些文件。

要追踪所有参与监控的美国政府机构是很困难的。国家反恐中心负责跟踪恐怖主义身份数据集市环境，这是美国政府的国际恐怖主义嫌疑人中央存储库。该机构维护着一个庞大的美国公民数据库，在2007年对70万个身份标识符(有点像人，但不是真的)进行监视，各种监视名单就是从这里来的。进入这些名单的程序似乎非常随意，当然，一旦有人上了名单，就没有追索权了。波士顿马拉松爆炸案凶手塔梅尔兰·萨纳耶夫(Tamerlan Tsarnaev)就在这个名单上。

还有组织犯罪毒品执法特遣部队负责毒品相关调查，以及针对计算机威胁的综合国家网络安全倡议。美国烟酒枪械局正在建立一个庞大的数据库来追踪人们和他们的朋友。就连五角大楼也在监视美国人，这是通过一个鲜为人知的机构——2008年关闭的反情报领域活动(Counterintelligence Field Activity)。2010年，海军刑事调查局(Naval Criminal Investigative Service)监控了华盛顿州每一台运行特定文件共享程序的电脑，不管它是否与军方有关——这明显违反了法律。

在联邦政府之外，更多的监视和分析监视数据的活动正在进行。自9/11以来，美国在全国各地建立了“融合中心”。这些机构通常由州和地方执法部门管理，旨在作为这些组织与FBI和国土安全部等国家机构之间的信息桥梁。

它们使当地警方能够获得以前无法获得的监控能力和数据。他们最初应该专注于恐怖主义，但越来越多地用于更广泛的执法。因为它们是在当地运行的，不同的融合中心有不同的规则——以及对这些规则的不同遵守程度。监管很少，可能存在非法军事介入，以及过度保密。例如，众所周知，核聚变中心对政治抗议者进行了监视。

联合恐怖主义特遣部队也由当地管理，定义模糊，并且极度保密。他们被发现调查政治活动人士，传播反伊斯兰宣传，骚扰无辜平民。

总的来说，美国存在着大量过度热情的、受意识形态驱动的监控。

在大西洋彼岸，NSA在英国的对等机构是政府通信总部(GCHQ)。它从本国和阿曼、塞浦路斯等地的远程监听站对本国和全世界的公民进行广泛的间谍活动。它与NSA有着非常密切的合作关系，并且越来越多地在本国境内进行大规模监视。其他监听本国公民和其他国家公民的国家包括德国、法国、丹麦、澳大利亚、新西兰、以色列、加拿大……可能还有其他所有有足够资金拥有情报预算的国家。澳大利亚政府声称，其对印尼的监视帮助挫败了该国的几次恐怖主义威胁。

我们对其他国家政府监控的了解要少得多;但不要仅仅因为那里的告密者没有将这些故事曝光，就认为他们没有做同样的事情。其他国家的政府也在尽可能多地利用互联网做同样的事情，而且往往对他们的活动没有那么多法律限制。

俄罗斯收集、存储和分析来自电话、电子邮件、互联网使用、社交网络、信用卡交易等方面的数据。俄罗斯的“行动调查措施系统”(简称SORM)就建在互联网上。在2014年索契奥运会期间，我们看到了这个系统的广泛程度，俄罗斯当局几乎监控了网上发生的一切。犯罪和恐怖主义为监控提供了理由，但这些数据也被用来对付俄罗斯记者、人权活动人士和政治对手。

中国也试图监控其公民在互联网上以及越来越多地在互联网外的一切行为。中国还利用手机的位置信息对民众进行大规模跟踪。它远程打开手机来窃听人们，并通过其2000万至3000万个监控摄像头监控物理空间。和俄罗斯一样，犯罪是所有这些监听行为表面上的借口，但异见也是一个主要原因。TOM- skype是一家中国视频和短信服务公司，是微软和中国TOM在线公司的合资企业。包含“天安门”、“国际特赦组织”和“人权观察”等词的信息，以及涉及毒品和色情的信息，都会被复制和保存。有3万多名网警在进行监控。

几年前，当印度、俄罗斯、沙特阿拉伯、阿联酋和印度尼西亚都威胁说，如果黑莓不允许他们访问用户通信，他们就会禁止黑莓。黑莓的数据通常是加密的，可以防止窃听。黑莓与印度达成了一项协议，允许企业用户保护他们的数据安全，但政府将能够跟踪个人用户的电子邮件、聊天记录和网站访问。我们不知道它可能与其他国家达成了什么协议，但我们可以假设它们是相似的。

较小的国家通常会向较大的国家求助，以帮助他们建立监控基础设施。中国帮助伊朗在自己的互联网基础设施中建立了监控系统。我将在第6章详细介绍西方公司帮助专制政府建立监控系统。

这些国家和其他国家的行为——我可以举出一整本书的例子——往往比美国或其盟友所做的任何事情都更具压迫性和极权主义。而且，美国对政府数据收集的法律控制和限制比世界上任何其他国家都要多，包括欧洲国家。在泰国、印度和马来西亚等国家，根据人们的互联网对话和活动逮捕他们是常态。我将在第7章讨论风险和危害;现在，我想坚持讲能力。

政府黑客

今天的电子间谍活动与冷战前互联网时代的情况不同。在互联网出现之前，当监视主要由政府对政府的间谍活动组成时，像NSA这样的机构会针对特定的通信线路:彼得罗巴甫洛夫斯克和符拉迪沃斯托克之间的苏联海底电缆，一颗军事通信卫星，一个微波网络。这在很大程度上是被动的，需要在附近国家建立大型天线场。

现代的目标监视很可能涉及主动侵入对手的计算机网络，并安装恶意软件，旨在接管该网络并“泄露”数据——这是NSA对窃取数据的说法。更直白地说，别人窃听你的通信最简单的方法，不再是在传输过程中拦截;而是黑进你的电脑。

现在有很多政府的黑客行为。

2011年，一名伊朗黑客入侵了荷兰证书颁发机构DigiNotar。这使他能够冒充谷歌、CIA、MI6、摩萨德、微软、雅虎、Skype、Facebook、Twitter和微软的Windows更新服务等组织。这反过来又让他得以监视这些服务的用户。他把这种能力传给了其他人——几乎可以肯定是伊朗政府——这些人反过来又用它来大规模监视伊朗人，可能还有外国人。Fox-IT估计有30万伊朗人的Gmail账户被侵入。

2009年，加拿大安全研究人员在达赖喇嘛的电脑上发现了一个名为GhostNet的恶意软件。这是一个复杂的监控网络，由

一台在中国的电脑进一步的研究发现，它安装在103个国家的政治、经济和媒体组织的电脑上:基本上是中国间谍目标的名人录。Flame是研究人员2012年在伊朗网络上发现的一款监控工具;我们认为美国和以色列把它放在了那里或其他地方。在2013年被发现之前，“红色十月”在全球范围内对计算机进行了5年的黑客攻击和间谍活动，据信是俄罗斯的监视系统。针对西方政府电脑的Turla也是如此，它在2014年被搜出。面具也于2014年被发现，据信是西班牙人。伊朗黑客专门针对美国官员。像这样已知的监视工具还有很多，可能还有其他未被发现的工具。

公平地说，我们没有证据表明这些国家是这些监控网络的幕后黑手，也没有证据表明这些监控网络是政府资助的。各国政府几乎从不承认他们侵入了对方的电脑。研究人员通常会从目标名单中推断出攻击的来源国。例如，假面具攻击的目标包括几乎所有说西班牙语的国家，以及摩洛哥和直布罗陀的一堆电脑。听起来很像西班牙。

在美国，负责入侵电脑的组织是NSA内部的“量身定制访问行动组”(TAO)。我们知道TAO利用代号很酷的程序远程渗透电脑，比如QUANTUMINSERT和FOXACID。我们知道，TAO开发了专门的软件，可以入侵从电脑到路由器再到智能手机的一切设备，其工作人员通过拦截和感染传输中的计算机和网络设备，将硬件“植入”到计算机和网络设备中。一种估计是，该组织已经成功入侵了全球8万台计算机，并正在从这些计算机中窃取信息。

当然，我们对《TAO》和美国黑客行动的了解大多来自于斯诺登提供的NSA绝密文件。其他国家还没有类似的泄密事件，所以我们对他们的能力了解得少得多。

我们确实对中国了解很多。中国已被可靠地确认为许多高调攻击的源头:针对b谷歌、针对加拿大政府、针对《*纽约*时报》、针对安全公司RSA和其他美国公司，以及针对美国军方及其承包商。2013年，研究人员发现了疑似中国政府的恶意软件，目标是西藏活动人士的安卓手机。2014年，中国黑客入侵了美国人事管理办公室(Office of Personnel Management)的一个数据库，该数据库存储了多达500万美国政府雇员和获得安全许可的承包商的详细数据。

为什么?其中很多是政治和军事间谍活动，但也有一些是商业间谍活动。很多国家为了自己的军事和商业优势，对外国公司进行间谍活动的历史都很悠久。美国声称不从事商业间谍活动，这意味着它不会侵入外国公司的网络，并将这些信息传递给美国的竞争对手以获取商业优势。但它确实从事经济间谍活动，通过侵入外国企业网络，并在政府贸易谈判中使用这些信息，直接使美国企业利益受益。最近的例子是巴西石油公司(Petrobras)和欧洲的SWIFT

国际银行支付系统。事实上，1996年的一份政府报告吹嘘说，NSA声称，它的一个项目给美国工业带来的经济利益“在过去几年中总计达数百亿美元”。你可能看不出这两种间谍活动之间有什么实质性的区别。中国政府和企业之间没有如此清晰的区分，所以没有。

许多国家从私营公司购买软件，以方便他们进行黑客攻击。我将在第6章中更多地讨论这种商业关系。现在，以一家名为Hacking Team的意大利网络武器制造商为例，该公司向世界各国政府出售黑客系统，用于攻击计算机和智能手机操作系统。这种移动恶意软件可以远程安装自己，收集电子邮件、短信、通话记录、地址簿、搜索历史数据和击键信息。它可以截屏，录制音频以监控通话或环境噪音，抓拍照片，并监控手机的GPS坐标。然后，它会秘密地将所有这些信息传回给它的处理器。埃塞俄比亚利用这款软件潜入欧美记者的电脑。

我们可以合理地假设，大多数国家都拥有这些黑客能力。他们用它们来对付谁，以及用什么法律规则来控制这种使用，这取决于这个国家。

政府攻击

当我们第一次收到关于中国为了间谍目的侵入美国计算机网络的报告时，我们用非常强硬的语言描述了它。我们给中国的行为贴上了“网络攻击”的标签，有时还会用到“网络战”这个词。在斯诺登揭露NSA一直在对世界各地的计算机网络做与中国完全相同的事情之后，美国使用了更为温和的语言来描述自己的行动，比如“间谍活动”、“情报收集”或“间谍活动”，并强调这是和平时期的活动。

当中国华为公司试图向美国出售网络设备时，我们担心美国政府在交换机上安装了后门，并认为这是“国家安全威胁”。但是，正如我们最终了解到的那样，NSA一直在做同样的事情，无论是对华为的设备，还是对在中国销售的美国制造的设备。

问题是，当它们发生时，从受害者的角度来看，国际间谍活动和攻击看起来非常相似。现代网络间谍活动是网络攻击的一种形式，两者都涉及侵入另一个国家的网络。它们之间唯一的区别是，是否故意破坏网络运行。当然，这是一个巨大的差异，但这种差异可能会推迟几个月甚至几年。因为侵入外国网络会影响到另一个国家的领土，所以根据那个国家的法律，这几乎肯定是非法的。即便如此，各国仍在不断地对彼此这么做。

这里有一个例子。2012年，NSA多次渗透叙利亚的互联网基础设施。其意图是在该国的一个核心路由器中远程安装窃听代码，但却意外造成了全国范围内的互联网中断。窃取数据和摧毁一个国家的互联网，涉及的操作完全相同。

各国政府正大举卷入网络战。大约有30个国家在其军队中设有网络战部门:美国、俄罗斯、中国、主要欧洲国家、以色列、印度、巴西、澳大利亚、新西兰和少数非洲国家。在美国，这是由国防部内的美国网络司令部领导的。海军上将迈克尔·s·罗杰斯同时负责这个组织和NSA。这两项任务距离如此之近。

很少有网络攻击对人或属性造成实际损害的例子浮出水面。2007年，爱沙尼亚遭受了一系列广泛的网络攻击。这通常被称为第一次网络战争，因为它恰逢与邻国俄罗斯的紧张局势加剧。前苏联共和国格鲁吉亚也是网络攻击的受害者，一年后，俄罗斯军队入侵了格鲁吉亚的土地。2009年，韩国遭受了一次网络攻击。所有这些都是拒绝服务攻击，在此期间，选定的互联网站点被流量淹没，暂时停止工作。它们具有破坏性，但从长远来看不会造成很大的破坏。

在所有这些案例中，我们都不确定肇事者是谁，甚至不知道肇事者是否是政府。2009年，一个亲克里姆林宫的青年组织宣称对2007年爱沙尼亚的袭击事件负责，尽管唯一被判有罪的人是一名居住在塔林的22岁俄罗斯人。这种可识别性是罕见的。就像前面讨论的间谍攻击一样，网络攻击很难追踪。我们只能通过受害者名单来推断攻击者。与俄罗斯的民族关系紧张:俄罗斯当然是罪魁祸首。韩国受到攻击:除了朝鲜，还有谁会有动机?

Stuxnet是第一个被一个国家用来攻击另一个国家的军事级网络武器。2009年，美国和以色列针对伊朗纳坦兹核设施发射了这枚导弹，并成功地造成了重大的物理破坏。据信，2012年针对沙特阿美石油公司(Saudi Aramco)的攻击造成该国有石油公司约3万台电脑受损，是伊朗的报复行动。

一个单一的全球监控网络

监控会产生一种有趣的垄断效应。在本章前面，我对政府对政府的间谍活动和政府对人口的监视进行了区分。间谍活动基本上遵循地缘政治路线;一个国家与盟国联合起来，共同对对手进行间谍活动。我们在冷战期间就是这么做的。这是政治。

大规模监控是不同的。如果你真的担心来自任何地方任何人的攻击，你就需要监视任何地方的每个人。既然没有一个国家可以单独做到这一点，那么与其他国家共享数据是有意义的。

但与谁共享呢?你可以和你的传统军事盟友分享，但他们可能不会监视你最担心的国家。或者他们可能对地球上足够多的地方进行监视，不值得分享。加入最广泛的间谍网络是最有意义的。那就是美国。

这就是现在正在发生的事情。美国与许多国家的情报合作伙伴。它是富裕的英语国家极其密切关系的一部分

被称为五眼:美国、英国、加拿大、澳大利亚和新西兰。其他伙伴关系包括“九眼联盟”，由丹麦、法国、荷兰和挪威组成;以及德国、比利时、意大利、西班牙和瑞典组成的“十四只眼”。美国与传统上较为冷淡的国家合作，比如印度，甚至与沙特阿拉伯这样的残酷镇压政权合作。

所有这些使得NSA几乎可以访问所有信息。斯诺登在2014年向欧洲议会作证时表示，“结果是一个欧洲集市，像丹麦这样的欧盟成员国可能会允许NSA进入一个窃听中心，但(不可强制执行的)条件是NSA不搜查丹麦人，德国可能会允许NSA进入另一个窃听中心，但前提是它不搜查德国人。”然而，这两个窃听点可能是同一条电缆上的两个点，因此，NSA只是在德国公民过境丹麦时截获他们的通信，在丹麦公民过境德国时截获他们的通信，同时完全按照双方的协议进行考虑。”

2014年，我们得知NSA监视土耳其政府，同时与土耳其政府合作监视土耳其境内的库尔德分裂分子。我们还了解到，NSA对其密切监视伙伴之一的德国政府进行间谍活动。我们可能会监视我们所有的合作伙伴，除了五眼联盟的其他国家。即使NSA吹嘘其反恐成功，其中大多数都是针对外国的外国威胁，与美国无关。

美国与以色列共享情报数据不足为奇。通常情况下，为了保护我们的隐私，在与另一个国家共享这些数据之前，美国人的身份会被删除，但以色列似乎是个例外。NSA向以色列的秘密部队8200提供“原始信号情报”——即信号情报。

即使是历史上的敌人也在与美国分享情报，即使只是在有限的基础上。9/11事件后，俄罗斯将车臣分裂分子重新定义为恐怖分子，并说服美国通过分享情报来提供帮助。2011年，俄罗斯就波士顿马拉松爆炸案凶手塔梅尔兰·萨纳耶夫(Tamerlan Tsarnaev)向美国发出警告。作为回报，我们在索契奥运会上密切关注威胁。

当情报的主要目标是政府与政府之间的间谍活动时，这些伙伴关系毫无意义，但当主要目标是对全球人口进行监视时，这些伙伴关系是明显和适当的。因此，尽管德国政府对NSA监视该国领导人表示愤怒，但德国联邦情报局(BND)仍在继续与NSA合作，监视其他所有人。

这样做的结局并不美好:这是一个全球监视网络，所有国家都串通起来监视整个地球上的每个人。这可能在一段时间内不会发生——会有像俄罗斯这样的顽固国家坚持自己做这件事，而僵化的意识形态差异永远不会让像伊朗这样的国家与俄罗斯或美国充分合作——但大多数较小的国家将有动力加入。从一个非常狭隘的角度来看，这是一件理性的事情。

6

机构控制的巩固

交织的;企业监督二者相辅相成，政府相互扶持。这是一种公私监督，并不是分开的监督。他们的合作关系遍及全球。这不是一个正式的协议;它更像是一个利益联盟。虽然它不是绝对的，但它已经成为事实上的现实，许多强大的利益相关者支持它的延续。尽管斯诺登披露的NSA监控事件导致了这种伙伴关系的裂痕——我们将在第14章讨论这些裂痕——但这种关系仍然很牢固。

斯诺登的文件清楚地表明，NSA在多大程度上依赖美国公司在互联网上进行窃听。NSA并不是从零开始建立一个庞大的互联网窃听系统。它注意到企业界已经在建立这样一个系统，并对其进行了窃听。通过像“棱镜”这样的项目，NSA合法地迫使微软、bb0、苹果和雅虎等互联网公司提供数千个人的数据。通过其他项目，NSA可以直接访问互联网主干，对每个人进行大规模监视。有时候这些公司愿意和NSA合作。有时他们被法院强迫交出数据，大部分是秘密的。在其他时候，NSA在未经允许的情况下侵入了这些公司的基础设施。

这种事情在世界各地都在发生。许多国家利用企业的监控能力来监控本国公民。通过诸如TEMPORA之类的项目，UK政府通信总部向英国电信和沃达丰等电信公司支付费用，以获得世界各地的大量通信。沃达丰为阿尔巴尼亚、埃及、匈牙利、爱尔兰和卡塔尔——可能总共有29个国家——提供了直接接入其国内互联网流量的服务。我们不知道这些国家在多大程度上像UK那样为访问付费，或者只是要求访问。法国政府窃听了France t<s:2> <s:2> com和Orange。中国和俄罗斯我们已经在第五章讲过了。大约有十几个国家有数据保留法——2014年在欧盟被宣布为违宪——要求互联网服务提供商将其客户的监控数据保存几个月，以防政府想要访问这些数据。伊朗、越南、印度和其他地方的网吧必须收集并保留顾客的同一性信息。

类似的事情在互联网之外也在发生。911事件发生后，美国政府立即从数据经纪人那里购买数据，包括火炬概念公司的航空乘客数据和选择点公司的墨西哥选民数据库。美国法律要求金融机构向政府报告1万美元及以上的现金交易;对于货币兑换商，这个门槛是1000美元。许多政府要求酒店报告当晚有哪些外国人在酒店住宿，还有更多的政府会复印客人的身份证和护照。闭路电视摄像头、车牌采集系统和手机定位数据被许多政府使用。

出于同样的原因，企业为了自己的目的获取政府数据。伊利诺伊州、俄亥俄州、德克萨斯州和佛罗里达州等州向私人买家出售包括照片在内的驾驶执照数据。一些州出售选民登记数据。UK政府在2014年提出出售纳税人数据，但公众的强烈抗议阻止了这一计划，至少暂时停止了。UK国民健康服务也计划将病人的健康数据出售给药品和保险公司。这是一个反馈循环:企业主张更多的政府数据收集，然后主张数据应该在开放政府法下发布，然后重新包装数据，再卖回给政府。

最终的结果是，大量的监控数据在政府和企业之间来回流动。这样做的一个后果是，很难通过有效的法律来遏制企业的监控——政府并不想通过削弱为他们提供资金的企业的手来限制自己对数据的访问。

关于“禁止追踪”的争论就是一个很好的例子，说明事情有多糟糕。多年来，隐私倡导者一直试图通过一项法律，强制要求互联网用户可以选择配置他们的浏览器，这样网站就不会跟踪他们。美国已经提出了几项国家法律，但遭到互联网公司的激烈反对，从未获得通过。2013年，加州通过了一项法律，但被游说者冲淡，几乎没有给用户带来什么好处。作为用户，你可以配置浏览器，告诉网站你不希望被跟踪，但网站完全可以无视你的意愿。

欧洲的情况就有点不同了。EU数据保护指令(EU Data Protection Directive)等法律对企业监控施加了更多限制，并产生了效果。但美国和EU之间的“安全港”协议意味着，个人数据可以从EU流向参与其中的美国公司，其标准不如EU适用的标准严格。

公私监控伙伴关系

政府不会单独进行监视、审查和控制行动。它们得到了一个庞大的公私监控伙伴关系的支持:一系列营利性公司。2010年的一项调查发现，在美国境内，有1931家不同的公司从事情报、反恐或国土安全工作。在2013年的一*篇报道中,《华盛顿*邮报》报道称，美国70%的情报预算流向了私营公司，48.3万名政府承包商持有绝密许可，占140万人的三分之一。政府和这些公司之间存在着一扇牢固的旋转门。1992年至1996年担任NSA局长的海军上将麦克·麦康奈尔(Mike McConnell)离职后，成为强大的政府承包商博思艾伦公司(Booz Allen Hamilton)的副总裁，继续从事国家情报工作。在2013年从NSA的领导职位上退休后，基思·亚历山大创办了自己的互联网安全咨询公司，并为他声称是自己发明的安全技术申请了专利。他聘请了NSA的首席技术官，该首席技术官也将继续为NSA工作。

许多网络武器制造商向世界各国政府出售黑客工具。例如，根据UK和德国公司伽马集团的宣传材料，FinFisher是一种“进攻性IT入侵解决方案”。各国政府

购买这种软件来监视人们的电脑和智能手机。2012年，研究人员发现有证据表明，FinFisher工具包已在巴林、新加坡、印度尼西亚、蒙古、土库曼斯坦、UAE、埃塞俄比亚、文莱以及美国和荷兰部署。

在第五章中，我提到了意大利公司骇客团队。其电脑和手机入侵和监控产品被阿塞拜疆、哥伦比亚、埃及、埃塞俄比亚、匈牙利、意大利、哈萨克斯坦、韩国、马来西亚、墨西哥、摩洛哥、尼日利亚、阿曼、巴拿马、波兰、沙特阿拉伯、苏丹、泰国、土耳其、UAE和乌兹别克斯坦等国政府使用。摩洛哥政府利用骇客团队的软件，透过一封自称来自一名处于危险中的匿名公民的电子邮件，攻击公民记者组织Mamfakinch;所附文件中包含恶意软件的有效载荷。

2011年，在巴林被捕的异见人士被出示了他们的私人电子邮件和聊天记录，这些记录是政府利用诺基亚和西门子提供的工具收集的。

国际情报支持系统(ISS world)大会在迪拜和巴西利亚等城市频繁举行贸易展。2014年的宣传册宣传了关于位置监控、通话记录挖掘、攻击性IT入侵和破解加密的会议，赞助商名单是这些能力的名人录。很多国家都派代表参加。在美国和欧洲也有类似的会议。

大多数美国大型国防承包商，如雷神公司、诺斯罗普·格鲁曼公司和哈里斯公司，都为美国军方制造网络武器。许多大型IT公司帮助在世界各地建立监控中心。法国公司Bull SA帮助利比亚政府建立了监控中心。尼日利亚使用的是以色列埃尔比特系统公司。叙利亚使用了德国西门子公司、意大利Area SpA公司和其他公司。利比亚的卡扎菲政权从中国的中兴通讯和南非的VASTech购买了电话监控技术。我们不知道阿塞拜疆和乌兹别克斯坦使用的互联网监控系统是谁建造的，但几乎可以肯定的是，一些西方公司帮助了他们。几乎没有禁止这种技术转让的法律，现有的法律也很容易被绕过。

这些不仅是专门设计的政府窃听系统;很多政府监控基础设施都是为企业使用而建的。总部位于美国的Blue Coat公司销售用于企业网络的监控和内容过滤系统，这些系统也用于缅甸、中国、埃及、印度尼西亚、尼日利亚、卡塔尔、沙特阿拉伯、土耳其和委内瑞拉等国的政府监控。Netsweeper是一款加拿大企业过滤产品，用于卡塔尔、也门、阿联酋、索马里和巴基斯坦政府的审查。美国Fortinet公司的过滤软件被用来审查缅甸的互联网;来自美国McAfee公司的SmartFilter通常用于学校，帮助突尼斯和伊朗政府审查本国的互联网。来自英国公司Sophos的商业安全设备被叙利亚和其他专制政权用来监视和逮捕他们的公民。

技术是价值中立的。你可以用手机拨打911，也可以计划抢劫银行。政府使用工具进行身份识别在技术上没有区别

罪犯和持不同政见者。企业和政府的使用没有技术上的区别。阻止员工通过电子邮件发送机密数据的合法公司工具可能被专制政府用于监视和审查。相反，沙特和伊朗持不同政见者用来逃避政府的反审查工具，也可能被犯罪分子用来传播儿童色情。加密可以让好人交流而不被坏人窃听，也可以让坏人交流而不被好人窃听。而且，迪士尼在主题公园里用来挑选顾客可能想买纪念品的照片的面部识别技术，同样可以识别中国的政治抗议者，以及纽约的“占领华尔街”抗议者。

颠覆商业体系的政府

到目前为止，我已经讨论了政府监控如何依赖于企业能力。虽然这在很大程度上是正确的，但政府并没有强迫企业为他们进行间谍活动。

早在20世纪90年代初，FBI就开始担心自己进行电话监控的能力。FBI可以用老式的模拟电话开关来做到这一点:这是一个涉及鳄鱼夹、电线和录音机的繁琐过程。问题是数字交换机不能这样工作。孤立个人联系变得更加困难，FBI开始担心可能会失去窃听能力。因此，它大力游说国会，并于1994年通过了一项名为《执法通信协助法案》(Communications Assistance for law Enforcement Act，简称CALEA)的法律，要求电信公司重新设计其数字交换机，以内置窃听功能。

快进20年，FBI再次希望IT行业让自己的监控变得更容易。很多通信不再通过电话进行。而是通过聊天进行交流。它们通过电子邮件发生。它们通过Skype发生。FBI目前正在游说将《CALEA》立法升级，该法案将涵盖*所有*通信系统:所有语音、视频和文本系统，包括《魔兽世界》和在线拼字游戏附带的小聊天窗口。

FBI的最终目标是政府禁止真正安全的通信。联邦调查局(FBI)总法律顾问瓦莱丽·卡普罗尼(Valerie Caproni)在2010年这样说:“任何人都不应该向客户承诺，他们会对美国法院的命令嗤之以鼻。他们可以承诺强大的加密技术。他们只需要弄清楚如何向我们提供纯文本。”换句话说，你无法为你的客户提供安全保障。

根据系统的不同，FBI想要做的事情从容易到不可能。Gmail这样的电子邮件系统很容易。这些邮件未加密地保存在b谷歌的服务器上，该公司有一个办公室，专门负责响应来自世界各地政府的访问个人账户的请求。像“不记录”(Off the Record)这样的加密聊天程序是不可能被破坏的;聊天会话是在熟客的电脑上加密的，没有中心节点可以窃听。在这种情况下，满足FBI要求的唯一方法就是为用户添加后门

软件，这会使它对每个人都不安全。我将在第11章讨论这个想法的愚蠢之处。

尽管这一措施很严厉，但至少讨论是在公开场合进行的。政府对企业通信基础设施的控制在很大程度上是秘密进行的，我们只是偶尔听说而已。

Lavabit是一种电子邮件服务，它比我们大多数人使用的大型企业电子邮件服务提供更多的安全隐私。这是一家小公司，由一个名叫拉达尔·莱维森的程序员拥有和经营，在精通技术的人中间很受欢迎。它拥有50万用户，其中包括爱德华·斯诺登。

2013年斯诺登逃到香港后不久，莱维森收到了一封国家安全信函，要求公司交出保护Lavabit所有用户的主加密密钥，然后不要告诉任何客户他们可能受到监控。莱维森在法庭上反对这一命令，当他明显败诉时，他关闭了他的服务，而不是欺骗和损害他的客户。

道德是显而易见的。如果你经营一家企业，而联邦调查局(FBI)或国家安全局(NSA)想把它变成一个大规模监控工具，它认为自己有权这样做，完全凭自己的权力。这个机构可以强迫你修改你的系统。它可以秘密地完成这一切，然后强迫你的企业保守这个秘密。一旦它这样做了，你就不能再控制你业务的那一部分了。如果你是一家大公司，你就不能关闭它。你不可能终止部分服务。从一个非常真实的意义上说，这不再是你的事了。它已经成为美国庞大监控机构的一个分支，如果你的利益与nsa的利益冲突，nsa就赢了。你的业务被征用了。

我们知道这个故事的唯一原因是莱维森经营着自己的公司。他没有企业主子。他没有股东。出于道德原因，他能够毁掉自己的生意。规模更大、债台高筑的公司绝不会这么做。我们必须假设，其他所有收到类似要求的电脑公司最终都会遵守要求。

例如，我们知道美国政府通过贿赂、胁迫、威胁或法律强制说服skype改变程序的运作方式，以方便窃听。我们不知道这些变化是什么，不知道它们是在微软2011年收购Skype之前还是之后发生的，也不知道它们是如何满足政府的要求的，但我们知道它们确实发生了。

2008年，美国政府秘密威胁雅虎，如果它不加入NSA的PRISM计划并向其提供用户数据，每天将被罚款25万美元。2004年，NSA付钱给RSA安全公司，让它把一个后门的随机数生成器作为其加密库的默认值。

其他类型的政府征用也在进行，背后是那些技术被颠覆的公司。如果NSA没有与公司签订协议，可以进入他们的系统，它就会尽最大努力秘密地这样做。例如，NSA不满意通过PRISM从bb0和雅虎接收到的数据量，于是入侵了两者之间的干线连接

公司的数据中心，可能与他们的服务提供商Level 3 Communications合作。谷歌的一位安全工程师在他的个人谷歌Plus页面上愤怒地回应道:“去他妈的那些家伙。”b谷歌已经对数据中心之间的连接进行了加密，以防止NSA进入。雅虎声称也在做同样的事情。

这并不是NSA入侵美国科技公司的唯一例子。该机构创建虚假的Facebook页面来入侵人们的电脑，其TAO分支机构在运输过程中拦截思科设备，以安装硬件植入物。

我们不知道美国政府对主要的互联网云提供商施加了什么样的压力，说服他们允许他们访问用户数据，也不知道这些公司可能与NSA达成了什么秘密协议。我们知道，NSA的BULLRUN项目和GCHQ的EDGEHILL项目都成功地破解了互联网上常见的安全系统。NSA是否要求b谷歌提供主加密密钥，并迫使其保密，就像它对Lavabit所做的那样?它的“量身定制访问操作”小组是否侵入谷歌的海外服务器并窃取密钥，或者拦截谷歌海外数据中心的设备并安装后门?这些都是NSA的战术记录。在第一种情况下，b谷歌将被法律禁止承认，在第二种情况下，它不想承认，在第三种情况下，它甚至不知道。总的来说，我们知道，在9/11之后的几年里，美国政府得到了许多公司的自愿合作，这些公司的领导人认为他们是爱国的。

我相信，由于NSA想要的数据类型，我们将看到更多的大量访问我们的数据。NSA过去能够从互联网骨干公司和宽带提供商那里得到它想要的一切。随着加密技术——特别是SSL加密技术——变得越来越普遍，这种情况变得不那么真实了。随着越来越多的互联网被加密，这种情况将变得更加不真实。为了克服这个问题，NSA需要从服务提供商那里获得大量数据，因为他们是拥有我们的明文数据的人，尽管在传输过程中有任何加密。要做到这一点，它需要颠覆这些网站用来保护数据的安全协议。

其他国家也参与了类似的欺诈行为。人们普遍认为，中国政府在其自有公司华为制造和销售的所有网络设备中都植入了窃听能力。我们有理由怀疑，英国、俄罗斯、以色列和法国的互联网产品也被他们的政府植入了后门。

我们不知道政府是否试图秘密地在他们没有直接政治或法律控制的公司的产品中插入后门，但许多计算机安全专家认为这种情况正在发生。是否有在美国大型软件公司工作的中国公民试图让中国政府更容易入侵这些公司的产品?法国程序员?以色列程序员?或者，至少，他们是在把源代码传回自己的国家，这样他们就能更容易地发现漏洞?是否有美国特工在亚洲设计和制造的电脑芯片中植入后门?我们知道他们在中国等国家秘密安插了员工

中国、德国和韩国协助颠覆计算机和通信系统。

面对这种情况，企业做出了充满警告的虚假保证。在2013年的一次技术会议上，谷歌首席执行官埃里克·施密特试图安抚听众，他说他“非常确定谷歌内部的信息现在是安全的，不会受到任何政府的窥探。”更准确的说法可能是:“除了我们不知道的方式和我们无法告诉你的方式之外，你的数据是安全的，不会被政府窥探。”这是一个糟糕的营销手段，但只要NSA被允许使用秘密法庭命令，基于对秘密法的秘密解释，它就永远不会有任何不同。

对大多数互联网公司来说，这不是问题。施密特没有说的另一件事是:“当然，我们仍然可以完全访问它，并且可以随意将其出售给我们想要的任何人……而且你没有追索权。”只要这些公司已经对他们的客户和用户进行了大规模的监控，他们就更容易遵守政府的要求，并与NSA分享财富。而只要政府继续要求获取信息，并避免立法保护，就更容易设计出允许这种行为的系统。这是一个强大的反馈循环:商业模式支持政府的努力，而政府的努力证明了商业模式的合理性。

PART TWO

WHAT'S AT STAKE

7

政治自由与正义

-

2013年，洛杉矶第一基督教会(First uaran Chrch of Los Angeles)起诉美国国家安全局从事国内间谍活动，称其对教会成员电话通话习惯的监控阻碍了他们团结起来倡导政治事业。教会并不是妄想狂。在20世纪50年代和60年代，联邦调查局因为其牧师的政治立场而监视他。今天，教会担心，无论是美国人还是外国人，都会因为与教会有联系而被列入监视名单。

政府的监视是昂贵的。最明显的是，它非常昂贵:美国每年花费720亿美元。但它也让我们的社会付出了高昂的代价，无论是在国内还是在国际上。哈佛大学法学教授Yochai Benkler将国家安全局的监控比作一种自身免疫性疾病，因为它攻击我们所有的其他系统。这是一个很好的类比。

最大的代价是自由，而风险也足够真实，以至于不同政治意识形态的人都反对监控系统的纯粹侵入性和普遍性。就连政治上保守、亲商业的《经济学家》杂志(Economist)也在2013年一篇关于视频监控的社论中指出，它走得太远了:“本刊坚持的信仰之一——技术进步通常应该受到欢迎，而不是恐惧——在这里与支持自由的更深层次的冲动发生了冲突。自由必须包括一定程度的隐私权:如果你的一举一动都被记录下来，自由就受到了限制。”

数据指控

17世纪，法国政治家黎塞留(Cardinal Richelieu)曾说过一句名言:“给我看世界上最诚实的人写的六行字，我就能从中找到足以绞死他的证据。”前苏联约瑟夫·斯大林的秘密警察头子拉夫连提·贝利亚(Lavrentiy Beria)宣称:“给我看这个人，我就给你看他的罪行。”两人的意思都是一样的:如果你有足够的关于某个人的资料，你就能找到足够的证据来判定他有罪。这也是很多国家的法院禁止警察进行“钓鱼调查”的原因。这也是美国宪法明确禁止一般搜查令的原因——一般搜查令基本上允许警察搜查任何东西。一般搜查令可能被极度滥用;它们被英国人在殖民时期的美国用作社会控制的一种形式。

无处不在的监视意味着，一旦警察下定决心，任何人都可能被判违法。生活在这样一个世界里，你所做的一切都可以被储存起来，并在以后的某一天作为对你不利的证据被提出来，这是非常危险的。允许警方深入研究这些大型数据集并找到不法行为的“证据”是非常危险的，尤其是在美国这样一个拥有如此多模糊和惩罚性法律的国家，这些法律赋予检察官自由裁量权，可以指控谁犯有什么罪，以及

过于宽泛的重要证人法考虑到“恐怖主义”这两个法律意义上的术语扩大到包括传统罪犯，“大规模杀伤性武器”扩大到几乎包括任何东西，包括一支被锯断的猎枪，情况尤其如此。美国的术语是如此广泛，以至于向哈马斯的人道主义机构捐赠10美元的人都可能被视为恐怖分子。

监视让我们有被当权者滥用权力的风险，即使我们在监视时没有做错任何事。对“错误”的定义往往是武断的，而且可能很快就会改变。例如，在20世纪30年代的美国，成为共产主义者或社会主义者是一种知识分子的时尚，在受过教育的阶层中并不被认为是错误的。20世纪50年代，随着参议员约瑟夫·麦卡锡(Joseph McCarthy)的政治迫害，这种情况发生了戏剧性的变化，许多聪明、有原则的美国公民发现，一旦他们的政治经历被公开，他们的职业生涯就毁了。有人读过的占领运动、茶党运动、动物权利、枪支权利网站，会在五到十年后成为颠覆的证据吗?

我们正在产生如此多的数据，并无限期地存储这些数据，这一事实加剧了这种情况。这些钓鱼探险可以追溯到过去，找到你在10年、15年或20年前可能做过的事情，并不断计算。今天的成年人能够超越他们年轻时的轻率行为;今天的年轻人就没有这种自由了。他们的全部历史将被永久记录下来。

政府监控的另一个危害是它导致人们被分类和歧视的方式。乔治华盛顿大学法学教授丹尼尔·索洛夫称这种情况是卡夫卡式的。这么多的数据都是秘密收集和使用的，我们无权反驳，甚至无权看到对我们不利的证据。随着系统开始使用监控数据自动做出决策，这种情况将会加剧。

监控数据已被用来证明许多处罚的合理性，从让人们接受更严格的机场安检到将他们驱逐出境。2012年，在洛杉矶度假之前，26岁的爱尔兰人利·范·布莱恩在推特上写道:“本周自由，在我去摧毁美国之前，快速八卦/准备一下。”美国政府一直在监控他的整个推特。特工们收到了布莱恩的信息，并将其与飞机乘客名单联系起来，当他从爱尔兰抵达时，他们在边境等着他。他的评论并不严肃，但他还是被审问了5个小时，然后被送回了家。我们知道，机场的炸弹笑话会让你被拘留;现在看来，在互联网上的任何地方，你都必须小心谨慎，即使是含糊不清的国际喧闹承诺。

2013年，一名夏威夷男子在脸书上发布了一段自己酒后驾车的视频。警方因此逮捕了他;他的辩护是，这是恶搞，视频中并没有真正饮酒。

英国的情况更糟。在那里，人们因为一条种族主义的推文或一条没有品位的脸书帖子而入狱。当然，在其他国家，这种情况更为极端，人们经常因为在网上写的东西而被逮捕和折磨。

最令人担忧的是，美国军方在一定程度上根据他们的目标来确定无人机袭击的目标。

数据。无人机瞄准有两种类型。第一种是“定点清除”，即通过电子或其他监视手段确定已知目标的位置。第二种是“签名打击”，针对身份不明的个人，根据他们的行为和个人特征:他们的表面年龄和性别，他们的位置，他们似乎在做什么。在2009年和2010年巴基斯坦无人机行动的高峰期，有一半的击毙行动都是“签名打击”。我们没有任何信息表明这种分析有多准确。

这是错误的。我们应该可以自由地和朋友聊天，或者给家人发短信，或者读一本书或一篇文章，而不必担心政府会怎么看:我们今天的政府，我们五年或十年后的政府，或者其他政府。我们不应该担心我们的行为会被怎样解读或误读，也不应该担心这些行为会被怎样用来对付我们。我们不应该受到本质上是无限期的监视。

政府审查制度

自由也依赖于思想的自由流通。政府的审查制度往往是通过监视来实现的，这两者都被扼杀了。

中国通过所谓的“金盾”(Golden Shield)，或者更常见的“中国防火长城”(Great Firewall of China)，保护其公民免受互联网上外部新闻和观点的“危险”。这是一个庞大的项目，花了8年时间，耗资7亿美元建成，它的工作是审查互联网。其目的与其说是消除有害思想或压制言论，不如说是阻止有效组织。防火墙运行得很好;那些有技术头脑的人可以避开它，但它阻止了大多数中国人找到各种各样的东西，从达赖喇嘛的信息到许多西方搜索网站。

如今，政府对互联网的审查比以往任何时候都要多。这不仅仅是政治问题。国家审查网站的原因还包括网站的性性质、网站所信奉的宗教观点、网站主办的赌博平台，以及网站对吸毒或非法活动的宣传。大多数中东国家的公民都生活在无处不在的审查之下。法国、德国和奥地利审查新纳粹的内容，包括纳粹纪念品的网上拍卖;其他国家则对煽动暴力的网站进行审查。越南的“72号法令”禁止人们在网上讨论时事。许多国家对侵犯版权的内容进行审查。英国默认对色情内容进行审查，不过你仍然可以选择不进行审查。2010年，美国审查了维基解密(WikiLeaks)。

大多数审查都是通过监视来执行的，这导致了自我审查。如果人们知道政府在监视他们所说的一切，他们就不太可能阅读或谈论被禁止的话题。这就是2014年俄罗斯一项要求博主向政府注册的法律背后的意义。这就是为什么中国防火长城作为一种审查工具如此有效的原因:它不仅仅是防火墙的技术能力，而且试图逃避它的人的威胁将被他们的同胞发现和报告。那些进行举报的人甚至不一定同意政府的观点;如果不报道，他们自己也可能面临处罚。中国的互联网公司对用户的审查经常超出官方要求。

而被抓的后果越严重，人们自我审查就越过分。

寒蝉效应

监控对社会可能产生巨大的寒蝉效应。美国最高法院大法官索尼娅·索托马约尔在2012年的一起案件中承认了这一点，该案涉及联邦调查局在某人的汽车上安装GPS追踪器。她的评论范围更广:“意识到政府可能在监视，这让结社和表达自由感到寒心。政府不受限制地收集数据，从而暴露同一性的私人方面，这种权力很容易被滥用。最终的结果是，GPS监控——通过以相对较低的成本提供政府在其自由裁量权下选择跟踪的任何人的大量私密信息——可能以一种对民主社会有害的方式改变公民与政府之间的关系。’”

哥伦比亚大学法学教授埃本·莫格伦(Eben Moglen)写道，“无处不在的侵入性倾听会产生恐惧。而这种恐惧是理性、有序的自由的敌人。”监视是一种恐吓策略。

在美国，我们已经看到了这种寒蝉效应的开始。根据人权观察组织的一份报告，报道情报机构、国家安全和执法的记者受到政府监视的严重阻碍。消息来源不太可能与他们联系，他们自己也担心被起诉。人权观察的结论是，需要报道的符合国家利益的故事没有得到报道，结果是公众了解的信息较少。这就是令人不寒而栗的效果。

处理涉及情报利益的案件的律师——外国政府客户、毒品、恐怖主义——也会受到影响。和记者一样，他们担心自己的谈话被监控，与客户的讨论也会落入控方手中。

“9·11”事件后的监控导致作家们进行自我审查。他们避免撰写和研究某些主题;他们小心翼翼地与消息来源、同事或国外的朋友交流。皮尤研究中心(Pew Research Center)在斯诺登的第一篇文章发表后不久进行的一项研究发现，人们不愿在网上谈论NSA。一项更广泛的哈里斯民意调查发现，由于NSA的监视，近一半的美国人改变了他们的研究、谈论和写作内容。监控使穆斯林美国人、环保主义者、枪支权利活动家、毒品政策倡导者和人权工作者等团体对互联网的使用降温。在2013年斯诺登泄密事件之后，世界各地的人们不太可能在b谷歌上搜索个人敏感词。

联合国人权事务高级专员2014年的一份报告指出，“即使通信信息被捕获的可能性很小，也会对隐私造成干扰，对包括言论自由在内的权利产生潜在的寒蝉效应。

以及结社自由。”

这不是妄想症。2012年，法国总统萨科齐在一次竞选演讲中说:“任何经常浏览宣扬恐怖、仇恨或暴力的网站的人都将被判入狱。”

这种对审查的恐惧不仅存在于当下;它也与过去有关。政客们已经生活在这样一个世界里:反对派不断拿着相机跟着他们，希望能记录下一些可以断章取义的东西。他们过去说过的话、做过的事，都会在当下被仔细研究和评判，其精准程度远远超过仅仅几年前人们的想象。想象一下，这对每个求职者来说都是正常的。

当然，监控对每个人的影响并不平等。我们中的一些人并不关心政府的监视，因此根本没有受到影响。而我们中的其他人，尤其是那些不受统治精英青睐的宗教、社会、种族和经济群体的人，则会受到更大的影响。

杰里米·边沁在构思他的panopticon时的关键观察是，当人们相信自己被观察时，他们就会变得墨守成规、顺从。圆形监狱是一种社会控制的架构。想想看，当一辆警车在你旁边行驶时，你会怎么做，或者当国家特工在监听电话时，整个国家会怎么做。当我们知道一切都在被录音时，我们就不太可能畅所欲言，也不太可能单独行动。当我们的行为不断受到评判、批评和纠正的威胁时，我们变得害怕——无论是现在还是不确定的将来——我们留下的数据会被任何关注我们曾经私密和无辜行为的权威带回，牵连到我们。作为回应，我们没有采取任何不同寻常的行动。我们失去了个性，社会停滞不前。我们不会质疑或挑战权力。我们变得顺从和顺从。我们变得不那么自由。

抑制异议和社会变革

这些寒蝉效应对政治话语尤其有害。持不同意见是有价值的。而且，反常的是，违法也可能有价值。这是我们作为一个社会进步的两种方式。无处不在的大规模监控是民主、自由、自由和进步的敌人。

捍卫这一论断涉及到一个微妙的论点——我在之前的书《*说谎者和异类*》(*Liars* and outliers)中写过——但它对社会至关重要。我们可以这样想。在美国各地，各州即将废除几十年前关于同性恋关系和大麻使用的法律。如果旧的法律能够通过监控得到完美的执行，社会就永远不会达到大多数公民认为这些事情是可以接受的地步。必须有一段时间，它们仍然是非法的，但却越来越被容忍，这样人们就可以环顾四周，说:“你知道，那并没有那么糟糕。”是的，这个过程需要几十年的时间，但这是一个不违法就不可能发生的过程。弗兰克·扎帕(Frank Zappa)在1971年也说过类似的话:“不偏离规范，就不可能取得进步。”

无处不在的政府监控所带来的完美执法使这一进程降温。我们需要不完善的安全系统，让人们自由地尝试新事物，就像不公开的头脑风暴会议可以放松束缚，培养创造力一样。如果我们没有这些，我们就不能慢慢地从一件事是非法的、不好的，到非法的、不确定的，到非法的、可能的，最后到合法的。

这是很重要的一点。我们现在认为理所当然的自由，往往一度被过去的权力结构视为威胁，甚至是犯罪。如果当局能够通过监视实现社会控制，这些变化可能永远不会发生。

这是我们所有人都应该关心新兴的监控架构的主要原因之一，即使我们个人并没有因为它的存在而感到寒意。我们之所以会受到影响，是因为我们周围的人不太可能宣扬新的政治或社会理念，也不太可能做出不同寻常的举动。如果j·埃德加·胡佛(J. Edgar Hoover)对马丁·路德·金(Martin Luther King Jr.)的监视成功地让他噤声，那么受影响的人将远远超过金和他的家人。

当然，许多违法的行为理所当然会永远违法:盗窃、谋杀等等。然而，在极端情况下，完美的执法可能会产生无法预料的后果。如果警察可以全天候跟踪你的车，然后在月底给你寄一张账单，列出你每次超速、闯红灯、非法左转或跟在你前面的车太近的时候，这对社会意味着什么?或者，如果你所在的乡镇可以利用空中监控自动对你进行罚款，因为你没有定期修剪草坪或铲平人行道?我们的法律体系很大程度上是基于人类的判断。虽然存在与有偏见和偏见的判断相关的风险，但用算法效率取代这种判断也存在风险。

无处不在的监控可能会导致2002年汤姆·克鲁斯(Tom Cruise)的电影《少数派*报告》(Minority* Report)中描绘的那种社会，人们在犯罪之前可能会成为警方调查的对象。执法机构已经在利用预测分析工具来识别嫌疑人并指导调查。从那里到老大哥和思想犯罪的世界只有很短的一步。

这种让某些犯罪无法逃脱的想法是新的——这是所有这些新技术的潜在结果——这是我们在实施之前需要仔细考虑的事情。正如法学教授Yochai Benkler所说，“不完美是自由的核心维度。”

秘密蠕变

保密通常会掩盖政府的监视，并对自由开放的社会构成威胁。

在美国，这表现在几个方面。首先，政府极大地扩大了可以被视为机密的范围。国家安全的一个不言而喻的真理是，在情报、外交政策和国防事务中，保密是必要的。如果政府决定某些事情——军队调动、武器装备、

谈判立场——敌人就会改变自己的行为，使之对自己有利。几千年来，这种军事保密的观念一直是正确的，但最近发生了巨大的变化。我在这里以美国为例。在第一次世界大战中，我们关心的是具体事实的保密性，比如军事单位的位置和战斗的精确计划。在第二次世界大战中，我们将这种保密性扩展到大规模行动和整个知识领域。我们不仅对制造原子弹的计划保密;整个核武器科学都是秘密的。9/11之后，我们进一步普遍化，现在几乎任何事情都可以成为秘密。

其结果是，美国政府的保密行为爆发了。没有人知道确切的数字——这当然是保密的——但合理的估计是，美国每年有数千亿页的政府文件被列为机密。与此同时，获得安全许可的人数也在迅速增加。截至2012年10月，美国有近500万人拥有安全许可(140万人拥有绝密级别)，自1999年以来增长了50%。

几乎所有NSA监控的细节都是保密的，以免给坏人通风报信。(我将在第13章回到这个论点。)在斯诺登之前，你不允许阅读授权NSA进行大部分监视的总统政策指令。你甚至不被允许阅读授权进行这种监视的法院命令。这些都是保密的，如果斯诺登文件的泄露没有导致政府的一系列解密，现在仍然是保密的。

NSA和军方并不是唯一提高保密级别的机构。地方执法部门也开始类似地掩盖自己的监视行动。例如，警方对手机监控的请求通常会被授权他们的法院封存。(英国警方甚至不承认他们使用了这项技术。)这样的例子还有很多。

这种保密削弱了我们现有的监督监督的制衡机制，更广泛地说，削弱了我们所有人都受到法律公平对待的机制。自9/11恐怖袭击以来，FBI和NSA要求各公司提供监控信息的国家安全信函经常附带禁言令。收到这类信件的人被禁止谈论此事，即使是泛泛之谈。这使得在法庭上对抗这些信件变得更加困难。

政府也躲在公司的保密协议后面。这就是FBI和当地警方没有透露他们的“黄貂鱼”手机监控系统细节的原因。这就是为什么当地警察部门拒绝透露他们用来部署警察的商业开发的预测性警务算法的细节。

政府保密的第二种表现方式是，它被施加到了极端的程度。美国有一个复杂的保密法律框架，而这个框架正日益被忽视。行政部门滥用其国家机密特权，将信息排除在公众视野之外。行政部门对国会保密。NSA对监督其运作的人(包括国会)保守秘密。某些国会议员对其他国会成员保守秘密。秘密法庭保守自己的秘密，甚至最高法院也越来越多地对文件保密。在

在华盛顿，知识就是货币，而情报机构正在囤积知识。

政府保密的第三个表现是，政府非常严厉地对待那些揭露其秘密的人:告密者。奥巴马总统在起诉揭露政府机构不法行为的个人方面格外热心。自2008年当选总统以来，他已经起诉了8名向媒体泄露机密信息的人。自1917年《间谍法》通过以来，此前只有三起起诉。

在美国，与情报有关的举报不是一种法律辩护;《间谍法》禁止被告解释他泄露机密信息的原因。丹尼尔·埃尔斯伯格(Daniel Ellsberg)是1971年第一个被起诉的人，他被禁止在法庭上解释自己的行为。2011年被起诉的NSA前高级管理人员托马斯·德雷克在审判中被禁止使用“告密”和“过度保密”等词。切尔西·曼宁(Chelsea Manning)被禁止使用类似的辩护。

爱德华·斯诺登称自己是告密者。包括我在内的很多人都同意这一点;也有人不同意。国务卿约翰·克里(John Kerry)坚持认为，斯诺登应该“回到这里，站在我们的司法体系中，为自己辩护”，前国务卿希拉里·克林顿(Hillary Clinton)宣称，“如果他希望回来，知道自己会被追究责任，也能进行辩护，那是他自己的决定。”这两句话都是误导人的政治谎言。现行法律不允许斯诺登为自己辩护。

由于政府监控要求保密，人们失去了辩论和投票政府以他们的名义在做什么，或者告诉他们当选的官员他们认为应该做什么的权力。人们很容易忘记，关于NSA及其监控项目的头条新闻层出不穷，但如果斯诺登没有冒着巨大的个人代价和风险，揭露该机构的所作所为，公众根本不会知道这一切。

滥用职权

2014年初，有人开了一个恶搞伊利诺伊州皮奥里亚市市长吉姆·阿迪斯(Jim Ardis)的推特账号。这是一个非常无礼的模仿，它真的激怒了阿迪斯。他的愤怒引发了一系列事件，当地警方非法获得命令，要求推特提供与该账户相关的同一性信息，然后搜查了推特用户乔恩丹尼尔的家。没有提出指控，主要是因为丹尼尔没有做错任何事，美国公民自由联盟目前正代表他起诉皮奥里亚。

所有的监控系统都容易被滥用。近年来，政客们利用监控来恐吓反对派，正如我们上面看到的那样，骚扰那些惹恼他们的人。一个例子来自2014年:新泽西州的警察经常在州长克里斯·克里斯蒂(Chris Christie)主持的活动上拍摄抗议者，直到州检察长命令他们停止。同样在2014年，我们了解到中央情报局非法入侵了参议院情报委员会工作人员的电脑，这些工作人员负责监督他们。2013年，

我们了解到NSA一直在监视联合国的通讯，这违反了国际法。我们知道，州和地方政府的监控机构也存在各种其他滥用职权的行为。

监控机构内部也存在滥用职权的情况。例如，NSA的雇员经常监听海外美国人的私人电话，拦截电子邮件，在办公室里传阅色情照片。2008年，我们从两名监听人员那里了解到这一点，2014年，我们又从斯诺登那里了解到这一点。我们从NSA那里了解到，它的特工有时会监视他们认识的人;在内部，他们称这种做法为LOVEINT。NSA自己的审计文件指出，从2011年到2012年的12个月里，该机构违反了自己的隐私规定2776次。这是一个很大的数字——每天8次——但实际数字可能要高得多。由于NSA自身的管理方式，它本质上决定了它能发现多少违规行为。

这不是一个新问题，也不局限于NSA。最近的美国历史显示了许多监控被系统滥用的事件:针对第一次世界大战后的劳工组织者和疑似共产主义者，针对民权领袖，针对越南战争抗议者。具体细节并不漂亮，但值得给出其中的几个。

- 通过广泛的监视，j·埃德加·胡佛(J. Edgar Hoover)得知了马丁·路德·金(Martin Luther King)的婚外情，并在1964年写了一封匿名信，试图诱使他自杀:“金，看看你的心。你知道你是个彻头彻尾的骗子，对我们所有黑人来说都是一个巨大的负担。这个国家的白人有足够多的骗子，但我敢肯定，他们目前没有一个像你这样的骗子。你不是牧师，你知道这一点。我再说一遍，你是个大骗子，是个邪恶的、恶毒的骗子。你不能相信上帝... .显然你不相信任何个人道德原则... .国王，你只剩下一件事要做了。你知道是什么。你只有34天的时间去做这件事(这个确切的数字是有特定原因选择的，它有明确的现实意义)。你就完成了。你只有一条出路。你最好在你肮脏、不正常、欺诈的自我暴露给全国之前接受它。”

- 参议院的一项调查是这样描述1976年联邦调查局(FBI)的COINTELPRO监视项目的:“虽然这些项目宣称的目的是保护‘国家安全’或防止暴力，但FBI的证人承认，许多目标都是非暴力的，而且大多数与外国势力没有联系。”事实上，非暴力组织和个人之所以成为目标，是因为该局认为他们代表了暴力的“潜在”，而反对越南战争的非暴力公民之所以成为目标，是因为他们给暴力示威者提供了“帮助和安慰”，给他们的事业带来了尊重... .但COINTELPRO不仅仅是违反了法律或宪法。在COINTELPRO中，调查局秘密地将法律掌握在自己手中，超越了情报收集和执法职能，完全在法律程序之外行事，秘密地破坏、诋毁和骚扰团体和个人。”

一切都没有改变。自9/11以来，美国一直在监视占领运动、支持和反对堕胎的活动家、和平活动家和其他政治抗议者。

- NSA和FBI监视了许多与恐怖主义无关的著名穆斯林美国人，其中包括费萨尔·吉尔(Faisal Gill)，他长期担任共和党特工，曾是公职候选人，拥有绝密安全许可，曾在乔治·w·布什(George W. Bush)总统的国土安全部(Department of Homeland security)任职;曾在恐怖主义相关案件中代理客户的知名律师阿西姆·加富尔(Asim Ghafoor);罗格斯大学(Rutgers University)伊朗裔美国人国际关系教授胡尚·阿米拉马迪(Hooshang Amirahmadi);尼哈德·阿瓦德(Nihad Awad)，他是该国最大的穆斯林民权组织的执行主任。

- 纽约警察局(New York Police Department)潜入少数族裔社区。它监视清真寺，渗透学生和政治团体，监视整个社区。同样，人们因为种族而成为攻击目标，而不是因为任何犯罪指控或不法行为的证据。其中许多行动都是在中情局的帮助下进行的，而法律禁止中情局对美国人进行间谍活动。

除此之外还有很多。波士顿的融合中心监视着和平退伍军人组织，也就是妇女组织

反战组织粉红代码和占领运动。2013年，该市与IBM合作，在音乐节上部署了视频监控系统。在同一时期，五角大楼的反情报现场活动(Counterintelligence Field Activity)监视了各种无辜的美国平民——这是法律禁止国防部这样做的。

呼应胡佛恐吓金的企图，NSA一直在收集穆斯林“激进分子”——不是恐怖分子，而是那些通过政治言论可能使他人激进化的人——观看色情片习惯的数据，目的是勒索他们。

2010年，DEA特工在获得许可的情况下搜查了奥尔巴尼一名妇女的手机，但随后保存了他们发现的私密照片，为她创建了一个虚假的Facebook页面。当他们因这种虐待行为被起诉时，政府似是而非地辩称，该女子同意搜查她的手机，就等于含蓄地同意了同一性被盗。

地方当局也滥用了监控能力。2009年，费城附近的下梅里恩学区(Lower Merion School District)借给高中生笔记本电脑帮助他们做作业。学校管理人员在电脑上安装间谍软件，然后记录学生的聊天记录，监控他们访问的网站，而且——这是最令人毛骨悚然的——偷偷地给他们拍照，通常是在他们的卧室里。当一名副校长拿着学生布莱克·罗宾斯像吃糖一样吃药片的照片质问他时，这一切都曝光了。事实证明，他们是糖果——确切地说，是迈克和艾克——学校因其侵犯性行为被成功起诉。

除了这些明显的权力滥用之外，任何庞大而强大的官僚体系的扩张都不可避免地伴随着权力的扩张:任务蔓延。比如，9·11事件后，中情局和财政部联手收集美国人的金融交易数据，以为可以发现未来恐怖组织的资金来源。事实证明，这是一条死胡同，但扩大的监控网住了一些洗钱者。就这样继续了下去。

在美国，监控比以往任何时候都更频繁，在更多的情况下，针对更多的犯罪行为。在《爱国者法案》中被认为是打击恐怖主义必不可少的监视权力，比如“偷窥”搜查令，在非恐怖主义调查中更常用，比如搜查毒品。2011年，NSA被授权在其传统的国家安全考虑之外，对毒品走私者进行监视。DEA的工作人员被要求在法庭上撒谎，以掩盖NSA向该机构传递数据的事实。

NSA的术语是“平行结构”。接收到NSA信息的机构必须发明一些其他的方法来获取这些信息，这种方法在法庭上是可以接受的。联邦调查局可能获得了逮捕黑客罗斯·乌布里希特(又名恐怖海盗罗伯茨)所需的证据，他通过这种方式运营了一个匿名的丝绸之路网站，人们可以在那里购买毒品和其他东西。

任务蔓延也发生在英国，在那里，旨在抓捕恐怖分子的监控被用于对付政治抗议者，以及各种轻微的刑事案件:针对违反禁烟令、伪造地址、事后不清理的人

他们的狗。这个国家有很多相机，所以尽可能多地使用它们是“有意义的”。

其他国家则提供了更多的例子。例如，以色列为了政治迫害收集无辜巴勒斯坦人的情报。建立监视国家的技术手段，使个人和组织很容易越过界限，滥用权力。当然，不那么讨人喜欢的政府滥用监控是理所当然的——他们的公民没有法律保护。

所有这些都很重要，即使你碰巧信任当前掌权的政府。一个拥有压倒性权力的系统依赖于每个掌权的人都能尽善尽美——为了防止有意义的滥用，必须采取很多正确的措施。坏苹果总是存在的——问题是他们被允许和授权造成多大的伤害，以及他们在多大程度上腐蚀了剩下的桶。我们的控制不仅要在我们支持的政党领导政府的时候起作用，也要在我们不支持的政党领导政府的时候起作用。

限制互联网自由

2010年，时任国务卿希拉里·克林顿发表演讲，宣布互联网自由是美国外交政策的主要目标。为此，美国国务院资助和支持世界各地的各种项目，致力于反对审查、促进加密和实现匿名，所有这些都是为了“确保任何孩子，无论出生在世界任何地方，都能访问全球互联网作为一个开放平台，在这个平台上进行创新、学习、组织、并在不受不当干扰或审查的情况下表达自己的观点。”这一议程遭到了破坏，因为人们尴尬地意识到，美国和其他民主政府在更专制的国家实施了他们所批评的同样类型的监控。

这些专制国家正在抓住这个机会，指出美国的监视是他们自己更严厉的互联网政策的正当化:更多的监视，更多的审查，以及一个更加孤立主义的互联网，使各个国家更多地控制他们的公民看到和说什么。例如，埃及政府为其监控社交媒体的计划提供的辩护之一是，“美国监听电话，并监督任何可能威胁其国家安全的人。”印度人担心他们的政府会引用美国的行为来证明在该国进行监视的正当性。中国和俄罗斯都公开谴责美国的虚伪。

这影响了全世界的互联网自由。从历史上看，互联网的治理——仅有的一点——大部分都留给了美国，因为每个人或多或少都认为我们是在维护互联网的安全，而不是反对它。但现在，美国已经失去了大部分的信誉，互联网治理陷入了混乱。许多影响互联网的监管机构都在试图弄清楚应该采用什么样的领导模式。国际电信联盟(international Telecommunications Union)等老牌国际标准组织正试图增加它们在互联网治理方面的影响力，并制定一套更具民族主义色彩的规则。

这就是网络主权运动，它有从根本上分裂的危险

互联网。这并不新鲜，但美国国家安全局(NSA)的间谍活动被曝光后，它得到了巨大的推动。像俄罗斯、中国和沙特阿拉伯这样的国家正在推动对其境内的互联网部分进行更自主的控制。

简而言之，这将是一场灾难。互联网本质上是一个全球性的平台。虽然各国继续进行审查和控制，但今天，专制政权中的人们仍然可以从世界其他地方阅读信息并与之交流思想。互联网自由是一个人权问题，美国应该支持这个问题。

脸书的马克·扎克伯格公开批评奥巴马政府，他写道:“美国政府应该是互联网的捍卫者，而不是威胁。”他是对的。

8

商业公平与平等

明尼苏达州。增益健康公司负责为医院收取账单和代理收款，许多医院也负责协调调度、入院、护理计划和住院时间。如果这听起来像一个潜在的利益冲突，它是。该机构收集了大量的患者数据，并将其用于自己的目的，而没有向患者披露其参与其医疗保健的性质。它在安排治疗时使用有关患者债务的信息，并在急诊室骚扰患者索要金钱。该公司否认了所有不当行为，但在2012年和解了明尼苏达州的一项诉讼，同意在两到六年内不在明尼苏达州开展业务。一方面，增益公司被抓并受到惩罚的事实表明，这个体系是有效的。另一方面，也说明了我们的数据是多么容易被不当处理和滥用。

这样的故事表明，允许企业进行大规模监控，会给社会带来相当大的风险。正是他们的监视助长了我在前一章中描述的所有侵犯公民自由、社会进步和自由的行为。除了使政府能够进行监视之外，企业监视也有其自身的风险。

基于监视的歧视

从根本上说，企业利用监控数据进行歧视。他们将人们划分为不同的类别，并在这些类别的基础上以不同的方式向他们推销商品和服务。

“红线”是20世纪60年代的一个术语，用来描述一种更古老的做法:银行在少数群体成员试图购买房屋时歧视他们。银行不会批准少数族裔社区的抵押贷款——他们会在地图上划出红线来划定这些区域。或者，只有少数族裔在少数族裔占主导地位的社区买房时，银行才会向他们发放抵押贷款。当然，这是非法的，但在很长一段时间里，银行都没有受到惩罚。更一般地说，“红线”是指用邻居作为种族的代表来拒绝服务或收取更多费用的做法——这在互联网上要容易得多。

2000年，富国银行(Wells Fargo)创建了一个网站来推广其住房抵押贷款。该网站以“社区计算器”为特色，帮助潜在买家寻找社区。计算器收集潜在客户的当前ZIP，并根据该ZIP的主要种族将他们引导到社区。该网站将白人居民推荐给白人社区，将黑人居民推荐给黑人社区。

这种做法被称为“网播”(weblining)，它有可能变得更加普遍

而且比传统的划红线更具歧视性。因为企业收集了如此多关于我们的数据，可以编制如此详细的档案，他们可以用许多不同的方式影响我们。2014年白宫关于大数据的一份报告得出结论，“……大数据分析有可能在个人信息如何在住房、信贷、就业、健康、教育和市场中使用方面超越长期存在的民权保护。”我认为这份报告低估了这种风险。

如今，价格歧视也是一个大问题。这不是像网络歧视那样经典的种族或性别歧视;而是公司向不同的人收取不同的价格，以实现尽可能多的利润。我们最熟悉的这个概念是关于机票的。价格一直在变化，取决于我们提前购买的时间、旅行的日期以及航班的满员程度等因素。航空公司的目标是以度假者愿意支付的便宜价格向他们出售机票，同时从商务旅行者那里榨取*他们*愿意支付的高得多的价格。这种做法并没有什么邪恶之处;这只是一种收入和利润最大化的方式。即便如此，价格歧视也可能*非常*不受欢迎。比如，在暴风雪过后提高雪铲的价格，就会被认为是哄抬价格。这就是为什么它经常以特别优惠、优惠券或回扣等方式隐藏起来。

有些类型的价格歧视是非法的。例如，餐馆不能根据顾客的性别或种族收取不同的价格。但它可以根据一天中的不同时间收取不同的价格，这就是为什么你会看到午餐和晚餐菜单上有相同的项目和不同的价格。提供老年人折扣和特价儿童菜单，是合法的价格歧视。Uber的高峰期定价也是合法的。

在很多行业，你得到的选择、你支付的价格、你得到的服务都取决于你的信息:银行贷款、汽车保险、信用卡等等。互联网监控促进了这种做法的微调。网上商家已经根据你的历史和他们对你的了解向你展示不同的价格和选择。根据你的身份，你可能会在网络汽车广告中看到红色敞篷车或小型货车的图片，当你访问经销商网站时，他们会为你提供不同的融资和折扣选择。根据《*华尔街*日报》2010年的一篇文章，你在史泰博网站上支付的价格取决于你所处的位置，以及竞争对手的商店离你有多近。文章指出，其他公司，如罗塞塔·斯通(Rosetta Stone)和家得宝(Home Depot)，也在根据个人用户的信息调整价格。

更广泛地说，我们都有一个客户评分。数据经纪人把它分配给我们。它就像一个信用评分，但它不是一个单一的数字，它关注的是你买了什么，基于从零售商那里购买的数据、个人财务信息、调查数据、保修卡注册、社交媒体互动、忠诚度卡数据、公共记录、网站互动、慈善捐赠者名单，线上和线下的订阅，以及健康和健身信息。所有这些都用来决定你在浏览互联网时看到的广告和优惠。

2011年，美国陆军制作了一系列招募广告，展示了不同性别和种族背景的士兵。它与一家有线电视公司合作播放这些广告

according to the demographics of the people living in the house.

还有其他的歧视方式。2012年，Orbitz根据观众使用的是Mac电脑还是Windows系统，突出了酒店客房的不同价格。其他旅游网站则根据浏览者的浏览历史向他们展示不同的价格。许多网站估计你的收入水平，并在此基础上向你展示不同的页面。这些都很微妙。这并不是说你看不到某些机票或酒店房间，只是它们的排序是为了让网站想要展示给你的那些更容易看到和点击。我们在第三章看到了关于我们的数据是如何被用来预测年龄、性别、种族、性取向、关系状态以及其他许多事情的。这使得公司比消费者有更大的优势，随着他们积累更多的数据，无论是个人还是阶层的人，这种优势只会增加。例如，营销人员知道，女性在周一感觉不那么有吸引力，这是向她们宣传化妆品的最佳时机。他们也知道不同的年龄和性别对不同的广告反应更好。未来，他们可能会对特定的个体有足够的了解，知道你在早上8点不太容易受到促销的影响，因为你还没有喝咖啡，心情不好，9:30左右你更容易受到促销的影响，因为你已经完全摄入了咖啡因，然后到了11点又变得不那么容易受影响了，因为午餐前你的血糖很低。

人们也会通过他们的社交网络来评判一个人。Lenddo是一家菲律宾公司，通过观察人们在脸书上频繁互动的人的信用状况来评估人们的信用风险。在另一个网络赌博的例子中，美国运通根据人们购物的商店类型降低了人们的信用额度。

1993年，宾夕法尼亚大学法学教授奥斯卡·甘迪(Oscar Gandy)很有先见之明地将这一切描述为“panoptic sort”：“收集、处理和共享个人和群体的信息，这些信息是他们作为公民、雇员和消费者在日常生活中产生的，用于协调和控制他们获得定义现代资本主义经济生活的商品和服务。”掌握这种权力的人，确实拥有巨大的权力。这种权力可以用歧视性的标准来发放不同的机会、准入、资格、价格(主要是特惠和折扣)、关注(正面和负面的)和曝光率。

这种做法可能会变得非常具有侵入性。高端餐厅开始对顾客进行b谷歌，以更好地个性化他们的用餐体验。他们不能给顾客提供不同价格的菜单，但他们当然可以给顾客提供酒单，要么是便宜的那一面朝上，要么是贵的那一面朝上。汽车保险公司正在试验基于使用的保险。如果你允许保险公司监控你开车的时间、距离和速度，你可能会得到更低的保险费率。

如果是雇主和雇员之间的关系，侵犯隐私的可能性就会大大增加。至少有一家公司通过向员工分发fitbit，通过谈判大幅降低了医疗保险成本，这让保险公司对其订户的健康习惯有了前所未有的了解。同样，有几所学校要求学生在体育课上佩戴智能心率监测器;至于这些数据之后会如何处理，目前还不得而知。2011年，惠普(Hewlett-Packard)分析了员工数据，以预测谁可能离开公司，然后通知他们

经理们。
工作场所监控是另一个潜在危害巨大的领域。对我们中的许多人来说，我们的雇主是最危险的力量，它把我们置于监视之下。经常被监视的员工包括呼叫中心工作人员、卡车司机、制造工人、销售团队、零售工人等。我们中更多人的公司电子通讯经常受到监控。这其中很多都来自于一个新的领域，叫做“职场分析”，基本上就是监控驱动的人力资源管理。如果你使用公司的电脑或手机，你几乎肯定赋予了雇主监控你在这些设备上所做的一切的权利。其中一些是合法的;雇主有权确保你没有整天在电脑上玩《Farmville》。但你可能也会在自己的时间使用这些设备，用于个人和工作交流。

任何时候我们被监控和侧写，都有可能出错。这一点你们已经很熟悉了;想想那些你在互联网上看到的不相关的广告，都是基于一些算法误解了你的兴趣。对某些人来说，这没什么;而对另一些人来说，无论分类正确与否，都有低级别的心理伤害。随着判断变得越来越重要，造成伤害的可能性也在上升:我们的信用评级取决于算法;我们在机场安检时受到的待遇，部分取决于企业收集的数据。

这也会产生寒蝉效应。例如，人们不愿查找有关他们可能患有的疾病的信息，因为他们害怕他们的保险公司会放弃他们。

的确，很多企业档案都是从良好的意图开始的。有些人可能会因为他们的脸书朋友赖账而被银行拒绝贷款，但Lenddo的系统旨在使银行能够向没有信用评级的人提供贷款。如果他们的朋友有良好的信用评级，这将是一个对他们有利的标记。使用个人数据来确定保险费率或信用卡消费限额可能会导致一些人得到比他们本来得到的更糟糕的交易，但它也会给很多人带来比他们本来得到的更好的交易。

然而，总的来说，监控数据正在被强大的公司利用，以牺牲消费者的利益为代价来增加自己的利润。消费者不喜欢这样，但只要(1)卖家为了我们的钱互相竞争，(2)软件系统让价格歧视变得更容易，(3)歧视可以对消费者隐藏起来，企业就很难抵制这种行为。

基于监控的操纵行为

了解我们的人对我们有一定程度的控制，了解我们一切的人对我们有很大的控制。监视有利于控制。

操纵不一定要涉及公开的广告。它可以是植入式广告，确保你看到的图片背景中有某个品牌的汽车。或者只是一个

增加你看到那辆车的频率。从本质上讲，这就是搜索引擎的商业模式。在早期，有一种说法是，广告主可以通过付费在搜索结果中获得更好的位置。在公众的强烈抗议和FTC随后的指导下，搜索引擎在视觉上区分了通过算法获得的“自然”结果和付费结果。现在你看到的是b谷歌的付费搜索结果以黄色框框显示，而Bing的付费搜索结果以淡蓝色框框显示。这种做法在一段时间内是有效的，但最近趋势又发生了逆转。谷歌现在接受在搜索结果中插入特定url的费用，而不仅仅是在单独的广告区域。我们不知道这有多广泛，但FTC再次对此感兴趣。

当你浏览Facebook动态时，你不会看到每个朋友的每条帖子;你看到的内容是由自动算法选择的，不会公开。但人们可以通过付费来增加好友或粉丝看到自己帖子的可能性。广告安置费占Facebook收入的很大一部分。同样，很多新闻页面底部的附加文章链接都是付费植入。

这里被操纵的可能性是巨大的。这里有一个例子。在2012年大选期间，Facebook用户有机会发布一个“我投票了”的图标，就像我们许多人在投票后在投票站得到的真正的贴纸一样。关于投票，有一种有据可查的从众效应;如果你相信你的朋友也在投票，你就更有可能去投票。这种操纵产生了全国选民投票率增加0.4%的效果。到目前为止，一切顺利。但现在想象一下，如果Facebook根据党派关系或一些体面的代理来操纵“我投票”图标的可见性:居住地的邮政编码、链接到的博客、喜欢的url等等。它没有这样做，但如果它这样做了，它就会在一个方向上提高选民投票率。这将很难被发现，甚至不会是非法的。Facebook可以通过有选择地操纵用户看到的帖子，轻易地影响一场势均力敌的选举。谷歌可能会对其搜索结果做类似的事情。

一个真正邪恶的社交网络平台可以更有效地操纵公众舆论。通过放大它认同的人的声音，压制它不认同的人的声音，它可能会严重扭曲公共话语。中国的“五毛党”就是这样做的:政府雇佣的人在社交网站上发表支持和挑战反对党的立场的评论。三星(Samsung)也做过类似的事情。

许多公司根据你的用户资料操纵你看到的内容:b谷歌搜索、雅虎新闻，甚至像《*纽约*时报》这样的在线报纸。这是一件大事。谷歌搜索结果中的第一个列表获得了三分之一的点击，如果您不在第一页上，您就像不存在一样。其结果是，你看到的互联网越来越多地根据你的个人资料所显示的你的兴趣来量身定制。这就导致了一种被政治活动家Eli Pariser称为“过滤泡沫”的现象:一个根据你的偏好进行优化的互联网，在那里你永远不会遇到你不同意的观点。你可能觉得这还不算太糟，但从大范围来看，这是有害的。我们不想生活在这样一个社会里，每个人都只会读那些强化他们现有观点的东西，我们从来没有自发的相遇，让人活跃、困惑、

面对并教导我们。

2012年，Facebook进行了一项对照实验。它有选择地操纵了68万用户的新闻推送，向他们展示快乐或悲伤的状态更新。因为Facebook不断地监控它的用户——这就是它把用户变成广告收入的方式——它可以很容易地监控实验对象并收集结果。研究发现，看到更快乐的帖子的人倾向于写更快乐的帖子，反之亦然。我不想过分夸大这个结果。Facebook只做了一个星期，效果很小。但一旦像Facebook这样的网站知道如何有效地做到这一点，他们就能从中获利。女性不仅在周一觉得自己没那么有吸引力;她们在情绪低落的时候也会觉得自己没那么有魅力。我们已经看到一些系统开始通过分析人们的声音和肢体语言来判断情绪;公司希望更好地确定客户何时感到沮丧，以及何时可以进行最有利可图的追加销售。操纵这些情绪来更好地推销产品是广告界可以接受的事情，即使这对我们来说听起来很可怕。

由于我们许多系统的集中式架构，操纵变得更加容易。b谷歌和Facebook等公司是我们交流的中心。这给了他们巨大的操纵和控制能力。

在政治中使用监控数据可能会产生独特的危害。选举政治在很大程度上是一种营销，政治家们开始利用个性化营销的歧视能力来跟踪投票模式，更好地“推销”候选人或政策立场。候选人和倡导团体可以针对特定人群制作广告和筹款诉求:年收入超过10万美元的人群、拥有枪支的人、读过某一特定问题某一方的新闻文章的人、失业退伍军人……任何你能想到的人。他们可以针对一群人投放愤怒的广告，针对另一群人投放深思熟虑的政策性广告。他们还可以在选举日微调他们的投票宣传活动，并在两次选举之间更有效地重新划分选区。这样的数据使用可能会对民主和投票产生根本性的影响。

基于个人信息和对底层系统的控制的心理操纵将变得越来越好。更糟糕的是，它会变得如此之好，以至于我们都不知道自己被操纵了。这是我们难以接受的现实，因为我们都喜欢相信自己太聪明了，不会被任何这样的伎俩所欺骗。我们不是。

侵犯隐私

1995年，黑客凯文·米特尼克(Kevin Mitnick)侵入了一家名为网通的互联网公司的网络，窃取了2万名客户的信用卡号码。2004年，黑客侵入了数据经纪公司ChoicePoint的网络，窃取了超过10万人的数据，并利用这些数据进行诈骗。2014年底，黑客侵入家得宝的企业网络，窃取了超过6000万张信用卡号码;一个月后，我们得知摩根大通(JPMorgan Chase)窃取了8300万户家庭的联系信息。互联网发展了二十年，除了规模，似乎什么都没变。

一个合理的问题是:互联网公司、数据经纪人和我们的政府在保护我们的数据方面做得怎么样?从某种意义上说，这个问题没有什么意义。在美国，任何愿意为数据付费的人都能获得数据。在某些情况下，犯罪分子合法购买并使用数据进行欺诈。

网络犯罪的历史比互联网还要悠久，而且是一门大生意。具体数字很难统计，但美国的损失很容易达到数百亿美元。有了这么多钱，网络犯罪是有组织的，也是国际化的。

这种犯罪大多涉及某种形式的同一性盗窃，这是互联网时代对假冒欺诈的花哨术语。犯罪分子侵入某个地方的数据库，窃取你的账户信息，也许还有你的密码，然后用它们来冒充你，以你的名义获得信贷。或者他窃取你的信用卡号码，并向你支付购物费用。或者他以你的名义提交虚假的纳税申报表，然后得到退款，而你以后要为此负责。

这不是针对你个人的。罪犯并不是真的想要你的私密信息;他们只是想要足够的关于你财务账户的信息来访问它们。或者需要足够的个人信息来获得贷款。

十几年前，风险是犯罪分子会侵入你的电脑并窃取你的个人数据。但数据盗窃的规模一直在增加。如今，犯罪分子更有可能侵入大型企业数据库，窃取你的个人信息，以及其他数百万人的个人信息。这只是更有效率了。政府数据库也经常遭到黑客攻击。我们一次又一次地了解到，我们的数据没有得到很好的保护。盗窃事件时有发生，比新闻机构报道的要频繁得多。我认识的隐私律师告诉我，数据漏洞和泄露事件比报道的要多得多——许多公司甚至都没有意识到他们的网络被黑客入侵，他们的数据被盗。事实上，企业安全的糟糕程度令人惊讶。而且因为机构合法地拥有你的数据，如果他们丢失了，你往往没有追索权。

有时候，黑客并不是为了钱。加州人路易斯·米汉格斯(Luis Mijangos)于2010年因“性勒索”被捕。他会侵入女性受害者的电脑，搜索她们的性和犯罪照片和视频，偷偷打开摄像头，自己拍下，然后威胁说，如果她们不向他提供更多的色情照片和视频，他就要公布这些照片和视频。做这种事的人被称为“ratters”，即RAT，即远程访问木马。这是他们用来接管你的电脑的恶意软件。最阴险的rat可以在不打开指示灯的情况下打开你电脑的摄像头。并不是所有的rat都会勒索受害者;有些人只是互相交换照片、视频和文件。

远程监视他人的不仅仅是黑客。在第七章中，我谈到了一个学区通过电脑监视学生。2012年，联邦贸易委员会(Federal Trade Commission)成功起诉了7家通过网络摄像头监视客户的电脑租赁公司。

在写这本书的时候，我从两个不同的人那里听到了类似的故事。在一个朋友——或者朋友的女儿——申请大学几年后，她收到了一封来自

她从未申请过的大学——每个故事里都写着不同的大学。这封信基本上是说，学校一直在存储她的个人数据，黑客侵入并窃取了所有数据;建议她向各大征信机构对自己的账户设置欺诈警报。在每一个案例中，学院都是在她高三的时候从经纪人那里购买了这些数据，并一直试图诱使她考虑入学。在这两种情况下，她甚至都没有申请这所大学。然而，几年后，这些大学仍在存储这些数据。两所大学都没有很好地保护这些数据。

只要我们的个人数据还像这样到处乱窜，我们的安全就有风险。

9

商业竞争力

1993年，电子商务;互联网是一个非常广泛的不同的地方，从它的婴儿期。它是今天。当时没有技术人员和学者的交流工具，我们使用电子邮件、新闻组和一种叫做IRC的聊天协议。计算机是原始的，计算机安全也是原始的。在大约20年的时间里，NSA通过将加密软件归类为军需品并限制其出口，成功地将其排除在主流之外。具有强大加密技术的美国产品无法销往海外，这意味着美国的硬件和软件公司将弱的——我指的是容易被破解的——加密技术植入他们的国内和国际产品中，因为这比维护两个版本要容易得多。

但世界正在发生变化。密码学的发现无法被撤销，学术界正在追赶NSA的能力。1993年，我写了第一本书《应用密码学》(*Applied Cryptography*)，让更普通的读者可以接触到这些发现。这是一件大事，我分两版卖出了18万册。《*连线*》杂志称它为“美国国家安全局希望永远不要出版的书”，因为它向非专家传授了加密专业知识。研究是国际化的，非美国公司如雨后春笋般涌现，在他们的产品中提供强大的加密技术。1993年的一项研究发现，在美国以外生产和销售的加密产品超过250种。美国公司担心，由于现行的出口限制，他们将无法与之竞争。

与此同时，FBI开始担心强大的加密技术会使该局更难窃听罪犯的谈话。它担心的是电子邮件，但它最担心的是可以安装在电话上的语音加密盒。这是FBI首次使用“暗化”一词来描述其想象中的无处不在的加密未来。这是一个没有正当化支持的恐怖故事，就像今天一样——但立法者相信它。他们通过了我在第六章提到的CALEA法律，FBI推动他们禁止所有没有后门的加密技术。

相反，克林顿政府想出了一个解决方案:克利伯芯片。这是一个加密系统，内置了联邦调查局和国家安全局的监控功能。据称，这种加密算法足够强大，可以防止窃听，但有一个后门，可以让知道特殊密钥的人获得明文。这被称为“密钥托管”，并被宣传为一个伟大的妥协;值得信赖的美国公司可以凭借强大的加密技术在世界市场上竞争，联邦调查局和国家安全局可以保持他们的窃听能力。

第一个内置克利伯芯片的加密设备是AT&T的安全电话。

它不是手机;那是1993年。它是一个小盒子，插在有线电话和有线听筒之间，对语音对话进行加密。在当时，它还算简洁。语音质量只能说还行，但还是管用的。

没人买。

回想起来，这是相当明显的。没有人想要内置美国政府后门的加密技术。注重隐私的个人不想要它。美国公司也不想要。美国以外的人不想要它，尤其是当有非美国的替代品可用时，它们具有强大的加密技术，没有后门。美国政府是AT&T设备的唯一主要客户，其中大部分设备甚至从未使用过。

在接下来的几年里，政府尝试了其他的关键托管计划，这些计划都是为了让美国政府能够通过后门访问所有加密，但市场也完全拒绝了所有这些计划。

克利伯芯片(Clipper Chip)和密钥托管的消亡，预示着美国政府对强密码学限制的终结。在接下来的几年里，出口管制逐渐取消，首先是1996年对软件的出口管制，几年后对大多数硬件的出口管制也取消了。这一变化来得并不早。到1999年，来自美国以外35个国家的800多种加密产品占据了市场。

杀死克利伯芯片和加密出口管制的不是消费者对隐私的要求。相反，它们是被外国竞争的威胁和美国工业界的要求扼杀的。电子商务需要强大的密码学，即使是FBI和NSA也无法阻止它的发展和采用。

政府监控让企业付出代价

我们这些打过“加密货币战争”(我们这么称呼它们)的人，以为自己在上世纪90年代赢得了这场战争。斯诺登文件向我们展示的是，NSA和FBI并没有放弃通过后门进入政府的想法，而是一直在秘密地这么做。现在这件事已经公开，美国公司正在失去海外业务，因为他们的非美国客户不希望他们的数据被美国政府收集。

美国国家安全局(NSA)的监控正以三种不同的方式让美国公司损失业务:人们逃离美国云提供商，人们不再购买美国的计算机和网络设备，以及人们不再信任美国公司。

2013年，NSA直接从美国云提供商处获取用户数据的“棱镜”项目曝光后，相关企业面临着严重的公关反弹。几乎立即就有文章指出，美国云计算公司正在失去业务，而瑞士等被视为中立的国家的同行正在获得业务。2014年对英国和加拿大公司的一项调查发现，25%的公司正在将数据转移到美国以外，即使这意味着性能下降。另一项针对公司的调查发现，NSA的爆料让高管们更加担心他们的数据存储在哪里。

对于美国云服务提供商将损失多少业务，各方估计不一。2013年

信息技术与创新基金会(Information Technology and Innovation Foundation)的一项研究预计，未来三年的收入损失将达到220亿至350亿美元;这相当于美国云服务提供商海外市场份额的10%到20%。互联网分析公司弗雷斯特研究公司(Forrester Research)认为这一比例很低;该公司估计，由于一些美国公司也将转向外国云提供商，三年的损失将达到1800亿美元。

美国的计算机和网络公司也受到了严重的打击。思科报告称，2013年第四季度收入下降了8%至10%。AT&T也出现了盈利亏损，其欧洲扩张计划也出现了问题。IBM在中国的销售额也出现了下滑。高通也是如此。威瑞森失去了一份德国政府的大合同。还有更多。我曾参加过一些非公开会议，美国大型软件公司在会上抱怨海外销售大幅减少。思科首席执行官约翰·钱伯斯致信奥巴马政府，称NSA对美国设备的黑客攻击“将破坏人们对我们行业的信心，以及科技公司向全球交付产品的能力。”

钱伯斯的言论呼应了斯诺登事件后美国企业面临的竞争力问题的第三个方面:它们不再被信任。全世界现在都知道，美国电信公司允许NSA访问互联网骨干，美国云提供商允许其访问用户账户。全世界现在都知道，NSA在运输途中拦截美国出售的计算机设备，并秘密安装监控硬件。全世界都知道，有一个秘密法庭迫使美国企业向美国国家安全局(NSA)提供窃听服务，然后命令它们在公开场合撒谎。还记得第五章里拉瓦比特的故事吗?

奥巴马政府一再保证，只有非美国人才是NSA大部分工作的重点，这加剧了所有这些不信任。许多云计算公司一半以上的收入来自美国以外。脸书的马克·扎克伯格(Mark Zuckerberg)在2013年的一次采访中说得最好:“政府的回应是，‘哦，别担心，我们没有监视任何美国人。’哦，太好了:这对那些试图为世界各地的人们服务的公司来说真的很有帮助，这真的会激发人们对美国互联网公司的信心。”

公平地说，我们不知道这种反弹有多少是暂时的，因为NSA的监视活动上了新闻，又有多少是永久性的。我们知道有几个国家——德国是其中最大的一个——正试图建立国内云基础设施，以使他们的国家数据不被NSA掌握。德国法院最近对谷歌、脸书和苹果的数据收集行为做出了裁决，德国政府正在考虑禁止所有与NSA合作的美国公司。数据隐私正逐渐成为国际商务的新公共安全要求。

这也是一项新的合同要求。越来越多的美国大公司要求其IT供应商签署合同，保证其IT系统不存在后门。更具体地说，合同语言要求供应商保证没有任何允许第三方访问其公司数据的内容。这使得IT公司更难与NSA或任何其他政府机构合作，因为这会使它们对最大、最复杂的客户承担直接的合同责任。在某种程度上，他们不能签署这样的保证，他们是

他们的生意就会被那些有能力的公司抢走。

我们也不知道世界上其他国家的竞争性产品和服务会有什么样的增长。欧洲、亚洲和南美的许多公司都在利用这种新的警惕态度。如果上世纪90年代的加密货币战争有什么借鉴意义的话，那么数以百计的非美国公司将提供超出美国法律管辖范围的IT产品:软件产品、云服务、社交网站、网络设备，应有尽有。不管这些新产品是否真的更安全——其他国家可能会在他们可以控制的产品中建立后门——或者甚至超出NSA的范围，NSA的监控对美国企业的成本将是巨大的。

企业监控成本商业

没有人会为隐私买单，这几乎已经成为一个公理。这种概括可能曾经是正确的，但人们的态度正在发生变化。

人们现在更加清楚谁可以访问他们的数据，多年来有迹象表明，他们已经准备好为隐私付费。2000年的一项研究发现，如果消费者在购物时感到他们的隐私得到了保护，美国的互联网支出每年将增加60亿美元。2007年的一项研究发现，消费者愿意支付更多的钱来保护他们的隐私:每件价值15美元的商品支付0.60美元。斯诺登事件后，许多公司都在宣传保护自己免受政府监控。

大多数公司不会把隐私作为一种市场差异化特征来提供，但也有例外。DuckDuckGo是一家搜索引擎，其商业模式围绕着不跟踪用户展开。Wickr提供加密消息。Ello是一个不跟踪用户的社交网络。这些社交网络的规模远不及它们的老牌竞争对手，但它们是可行的业务。而且新公司也一直在开业。

我们看到，越来越多的公司设立了首席隐私官，即负责管理公司持有的个人数据的法律和声誉风险的高级管理人员，这使得客户和用户隐私变得越来越重要。这些高管有自己的组织，即国际隐私专业人员协会，即使在没有政府推动的情况下，他们也在制定规章制度。他们这么做，是因为这对企业有利。

10

隐私

希德。“如果你对隐私没有任何错误的误解，那么你就没有什么要隐藏的，”这句话是这么说的，很明显，隐私只会帮助不法分子。

然而，如果你仔细想想，这是没有道理的。我们做爱、上厕所、洗澡唱歌，都没有做错什么。我们在找工作时没有告诉现在的雇主，也没有做错什么。当我们寻找私人空间进行反思或交谈时，当我们选择不谈论情感或个人的事情时，当我们用信封寄信时，或者当我们向朋友倾诉而不向任何人倾诉时，我们并没有做错什么。

而且，即使那些这么说的人也并不真的相信。在2009年的一次采访中，谷歌CEO埃里克·施密特这样说:“如果你有不想让任何人知道的事情，也许你一开始就不应该做这件事。”但在2005年，施密特禁止员工与CNET的记者交谈，因为一名记者在一篇文章中披露了施密特的个人信息。Facebook的马克·扎克伯格(Mark Zuckerberg)在2010年宣布，隐私不再是一种“社会规范”，但为了确保自己的隐私，他买下了位于帕洛阿尔托(Palo Alto)家附近的四套房子。

很少有秘密是我们不会告诉*别人的*，即使我们已经告诉了那个人，我们仍然相信有些事情是隐私的。我们给爱人和朋友写亲密的信，和医生说一些我们不会告诉别人的事情，在商务会议上说一些我们不会在公开场合说的话。我们使用假名是为了将职业上的自我与个人生活中的自我区分开来，或者是为了安全地尝试新事物。

Facebook的CEO马克·扎克伯格(Mark Zuckerberg)表示:“你只有一个同一性。你对你的工作朋友或同事以及你认识的其他人有不同形象的日子可能很快就要结束了。拥有两个身份是缺乏诚信的一个例子。”

对我们认识的每个人来说，我们都是不一样的。当我们与家人、朋友、同事等在一起时，我们的行为也会有所不同。我们在家和在餐馆有不同的餐桌礼仪。我们给孩子讲的故事和给酒友讲的故事不一样。这并不一定是我们在说谎，尽管有时我们确实在说谎;而是我们向不同的人展示了自己不同的一面。这是人类与生俱来的特质。隐私让我们在任何环境下都能做出适当的行为。在家里或卧室的私密空间里，我们可以以一种别人在身边时无法做到的方式放松。

隐私是一项与生俱来的人权，是维护人类尊严和尊重的必要条件。这是一种选择，并有能力控制如何去做

你向世界展示你自己。互联网人种学家danah boyd是这样说的:
“隐私不仅仅取决于机构;能够实现隐私是代理的一*种*表现。”

当我们失去隐私时，我们就失去了对自己表现方式的控制。当我们在脸书上对一群人说的话意外地被另一群人分享时，我们就失去了控制;当我们的数据被政府收集时，我们就失去了完全的控制。“他是怎么知道的?我们问道。我是如何失去控制的，不让谁知道我创伤的童年、我对粗俗幽默的嗜好，或者我去多米尼加共和国度假的经历?你可能知道这种感觉:当你妈妈在脸书或其他社交网站上加你为好友时，你会有这种感觉，而这些网站以前只有你和你的朋友。侵犯隐私是一种侵犯。

隐私有很强的生理基础。生物学家彼得·沃茨(Peter Watts)指出，对隐私的渴望是与生俱来的:哺乳动物对监视的反应尤其不好。我们认为这是一种身体上的威胁，因为自然界的动物会受到捕食者的监视。监视让我们觉得自己是猎物，就像它让监视者的行为像捕食者一样。

心理学家、社会学家、哲学家、小说家和技术专家都写过关于持续监控的影响，甚至只是对持续监控的感知。研究表明，无论是身体上还是情感上，我们都不那么健康。我们会感到自卑、抑郁和焦虑。监视剥夺了我们的尊严。它威胁着我们作为个体的自我。这是一种在世界各地的监狱和拘留营中使用的非人性化策略。

侵犯隐私的行为并不都是平等的。情境很重要。运输安全管理局(TSA)的官员在你的行李箱里发现色情片和你的配偶发现色情片是有区别的。警察知道你吸毒和你的朋友知道你吸毒是有区别的。侵犯隐私的伤害并不都是一样的。我们这些处于社会经济边缘的人，以及被边缘化的种族、政治、民族和宗教群体，受到的影响更大。我们这些身居要职、受制于人们持续认可的人受到的影响更大。我们中的一些人的生活依赖于隐私。

我们的隐私正受到不断监视的侵犯。了解这种情况是如何发生的，对于理解什么是利害攸关的至关重要。

短暂的

在历史的大部分时间里，我们的互动和对话都是短暂的。这是我们对对话的自然思考方式。例外情况非常罕见，值得注意:保存下来的日记，速记员抄录的法庭诉讼程序，政治候选人录制的演讲。

这种情况已经发生了变化。公司面对面的会议减少了。朋友们在网上社交。我和妻子通过短信进行亲密对话。我们都表现得好像这些对话是短暂的，但事实并非如此。它们以我们所没有的方式保存着

无法控制。

记录在案的对话很难删除。奥利弗·诺斯(Oliver North)早在1987年就明白了这一点，当时他以为已经删除的信息，结果却被白宫的PROFS Notes系统保存了下来，这是电子邮件的一种早期形式。十年后，比尔·盖茨也明白了这一点，当时他的对话电子邮件作为微软反垄断诉讼发现过程的一部分，被提供给了对方律师。2014年，100多名女名人也知道了这一点，当时她们的iCloud账户上的私密自拍——其中一些据说已被删除——被窃取，并被分享到比她们预想的更广泛的地方。

想要短暂存在越来越难了。语音对话在很大程度上仍未被录制，但这种情况能持续多久?零售商店的监控系统会记录下我们的存在，即使我们除了浏览什么都不做，即使我们买什么都用现金支付。有些酒吧会记录每一个进来的人的身份证。甚至在飞机上用现金买一杯酒都不行了。无处不在的生活记录仪会让情况变得更糟。

科幻作家查尔斯·斯特罗斯(Charles Stross)将此描述为史前时代的终结。我们不会忘记任何事情，因为我们总能从某些计算机的内存中检索到它。这对我们人类来说是全新的，对未来的历史学家和现在想要更好的数据进行自我评估和反思的我们来说都是一个福音。

把所有的东西都记录下来并永久地获取，将会改变我们个人和整个社会。我们的感知和记忆并不像我们想象的那么敏锐。我们无法注意到一些事情，即使是重要的事情。我们记错了，即使是我们确信自己记对的事情。我们会忘记一些我们确信自己永远不会忘记的重要事情。写日记的人知道这一点;旧的条目读起来就像别人写的一样。我已经注意到，拥有20年来所有电子邮件的记录，会让我对个人过去的看法发生很大变化。

四分之一的美国成年人有犯罪记录。即使是轻微的违法行为也可能永远跟着人们，并对他们的生活产生巨大的影响——这就是为什么许多政府都有在一段时间后删除犯罪记录的程序。失去短暂性意味着你所说的和所做的一切将永远与你联系在一起。

有一出现就消失的对话是一种社会规范，它能让我们更放松、更舒服，也能说一些如果录音机开着可能不会说的话。长此以往，遗忘——以及记错——就是我们处理历史的方式。遗忘是宽恕的重要促成因素。个人和社会的记忆会褪色，过去的伤痛会变得不那么尖锐;这有助于我们原谅过去的错误。我不相信我的婚姻会因为有能力记录过去的争吵而得到改善。失去转瞬即逝的东西将是一个巨大的社会和心理变化，我认为我们的社会还没有做好准备。

算法监控

对大规模监控的常见防御之一是，它是由算法而不是人来完成的，所以它不会损害我们的隐私。这是完全错误的。

人类监控和计算机监控之间的区别在政治上很重要。自从斯诺登向记者提供了大量绝密文件以来，我们已经了解了NSA的各种文字游戏。根据美国国防部的说法，“收集”这个词有一个非常特殊的定义。它的意思不是收集;它的意思是一个人看，或者分析数据。2013年，美国国家情报总监詹姆斯·克拉珀(James Clapper)将NSA积累的大量数据比作一座图书馆。所有这些书都被存放在书架上，但真正被阅读的却很少。“因此，为了维护安全，维护公民自由和隐私，我们的任务是在图书馆寻找我们需要打开并真正阅读的书籍时尽可能精确。”

想想你的朋友，他家里有成千上万本书。根据这个荒谬的定义，他唯一能自称收藏的书就是他读过的书。

这就是为什么克拉珀在参议院听证会上对“NSA是否收集数百万或数亿美国人的任何类型的数据”的问题回答“不”时声称他没有撒谎的原因。从军方的角度来看，即使国防人员或承包商开发和实施的算法已经对这些数据进行了多次分析，但在有人看到这些数据之前，这也不是监视。

这并不是我们第一次听到这样的说法。在Gmail早期，这是Gmail捍卫其上下文敏感广告的核心。b谷歌的计算机检查每封电子邮件，并在页脚插入与内容相关的广告。但是没有人会读那些Gmail信息，只有电脑会读。正如Gmail早期的一位高管私下告诉我的那样，“担心电脑阅读你的电子邮件，就像担心你的狗看到你的裸体一样。”

但事实并非如此，狗的例子说明了其中的原因。当你被狗注视时，你不会过度担心，原因有三。狗不能像其他人一样理解或处理它所看到的东西。狗不会像其他人那样记住或根据它所看到的东西做出未来的决定。而且狗不能告诉任何人——无论是人还是另一只狗——它看到了什么。

当你被一台电脑监视时，狗的类比就不适用了。计算机正在处理它所看到的东西，并根据它采取行动。你可能被告知计算机没有保存数据，但你不能保证这是真的。你可能会被告知，如果计算机感知到感兴趣的东西，它不会提醒一个人，但你无法知道这是否是真的。你无法确定没有人会察觉到计算机做出的任何决定，也无法确定你不会因为计算机看到的东西而受到评判或歧视。

此外，当计算机存储你的数据时，总是存在被暴露的风险。隐私政策可能明天就会改变，允许在没有你明确同意的情况下对旧数据进行新的使用。一些黑客或犯罪分子可能会闯入并窃取你的数据。拥有你的数据的组织可以以某种新的和公开的方式使用它，或者把它卖给另一个组织。联邦调查局可以向数据所有者发出国家安全信函。另一方面，世界上没有一个法庭可以得到你裸体的描述

从你的狗嘴里。

电脑和狗的主要区别在于，电脑能与人交流，而狗不能——至少，不能很好地与人交流。计算机算法是由人编写的，其输出是供人使用的。而当我们想到计算机算法在监视我们或者分析我们的个人数据时，我们需要考虑这些算法背后的人。无论是否有人真的在看我们的数据，(1)他们可以，(2)他们指导算法这样做的事实，使它成为监视。

你知道这是真的。如果你相信克拉珀所说的话，那么你就不会反对在你的卧室里装摄像头——只要有规定规定警察什么时候可以看录像。你不会反对被强迫佩戴政府发放的全天候监听设备，只要你的官僚监控人员遵守同样的规则。如果你真的反对，那是因为你意识到隐私损害来自于自动收集和算法分析，而不管一个人是否直接参与了这个过程。

识别和匿名性

我们都有过在互联网上证明自己身份的经历。一些网站将你的在线同一性与你的真实同一性捆绑在一起:银行、一些政府服务网站等等。有些将你的在线同一性与支付系统(通常是信用卡)绑定，有些则与你的银行账户或手机绑定。有些网站并不关心你的真实同一性，只允许你为该网站保留一个唯一的用户名。更多的网站可能以这种方式运作。例如，苹果的iTunes可以被设计成不知道你的真实身份，只知道你被授权访问一组特定的音频和视频文件。

执行身份识别和认证的手段包括密码、生物识别技术和令牌。包括我在内的许多人都写过大量关于各种系统及其相对优缺点的文章。我就不赘述了;结论是，这些系统都不是完美的，但总的来说，它们的应用都足够好。身份验证基本上是有效的。

它起作用是因为参与的人想要被识别。你想让Hotmail相信这是你的账户;你想让你的银行相信这是你的钱。虽然你可能不希望AT&T能够将你在智能手机上浏览的所有互联网信息与你的同一性联系起来，但你确实希望电话网络将你的电话传输给你。所有这些系统都试图回答以下问题:“这是她声称的那个人吗?”这就是为什么在网上很容易收集到我们的数据;这些数据大多来自于我们有意标明自己身份的来源。

将匿名活动归因于特定的人是一个更难的问题。在这种情况下，这个人不一定想要被识别出来。他是在网站上匿名发表评论。或者他在对你的网络发起网络攻击。在这种情况下，系统必须回答一个更难的问题:“这是谁?”

在非常基本的层面上，当恶意对手试图逃避检测时，我们无法识别单个硬件和软件。我们无法将识别信息附加到互联网上传输的数据包上。我们无法验证一个人的同一性他坐在地球上某个地方的随机键盘前。解决这个问题不是克服一些工程挑战的问题;这种无能是互联网固有的工作方式。

这意味着我们无法确定是谁在博客上留下了匿名评论。(它可能是用公共计算机发布的，或者是共享的IP地址。)我们无法确定电子邮件的发件人。(这些邮件头可以被欺骗;垃圾邮件发送者一直都在这么做。)我们无法最终确定谁是一系列登录你的银行账户失败的幕后黑手，或者是针对我们国家基础设施的网络攻击的幕后黑手。

我们甚至不能确定某一特定攻击的源头是犯罪还是军事，或者哪个政府是幕后主使。2007年针对爱沙尼亚的网络攻击，常被称为第一次网络战，其主谋要么是与俄罗斯政府有关联的组织，要么是心怀不满的22岁青年。

当我们设法将攻击归罪于一个淘气的高中生，一个银行抢劫犯，或者一个国家认可的网络战士团队时，我们通常是在进行了广泛的法医分析之后才这样做的，或者因为攻击者以其他方式暴露了自己。分析人士花了几个月的时间才确定中国是2012年《*纽约*时报》遭受攻击的最终来源，直到美国承认了这一点，我们才确切地知道谁是Stuxnet的幕后黑手。这是一个非常困难的问题，我们不太可能在短期内解决这个问题。

多年来，有很多建议要消除互联网上的匿名性。他们的想法是，如果任何人做的每件事都是可归因的——如果所有的行为都可以追溯到他们的来源——那么就很容易识别罪犯、垃圾邮件制造者、跟踪者和网络喷子。基本上，每个人都将获得相当于驾照的互联网证书。

这是一个不可能实现的目标。首先，我们没有现实世界的基础设施来提供基于其他身份识别系统的互联网用户证书——护照、国民同一性卡、驾驶执照等等——而这正是我们所需要的。我们当然也没有在全球范围内做到这一点的基础设施。

即使我们有，也不可能保证安全。我们现有的每一个同一性系统都已经被试图买酒的青少年颠覆了——这是一种面对面的交易。一个新的系统也不会更好。即使有，它也不会起作用。在同一性系统之上建立匿名服务总是可能的。这一事实已经惹恼了像中国这样的国家，它们想要识别在其领土上使用互联网的每个人。

这似乎与我在第三章中写的内容相矛盾，即在互联网上很容易识别出那些试图保持匿名的人。这是可以做到的，如果你已经捕获了足够的数据流来关联，并愿意投入调查时间。有效减少互联网匿名性的唯一方法是通过大规模监控。第三章的例子都依赖于拼凑不同的线索，

而且都需要时间。追踪单个互联网连接的来源要困难得多:一封电子邮件，一个网络连接，一次攻击。

悬而未决的问题是，通过关联和分析进行识别的过程能否实现自动化。我们能否构建足够智能的计算机系统，像我们在第3章看到的例子那样，在大规模的基础上分析监控信息以识别个人?目前还不行，但也许很快就能实现。

正在研究中。像中国和俄罗斯这样的国家想要自动系统在互联网上搜寻持不同政见的声音。娱乐业也希望有类似的系统来识别电影和音乐盗版。美国政府希望用同样的系统来识别它认为是威胁的个人和组织，从单独的个人到外国政府。

2012年，美国国防部长利昂·帕内塔公开表示，美国“在识别网络攻击来源方面取得了重大进展”。我的猜测是，我们还没有发展出一些新的科学或工程，从根本上改变互联网可识别性和匿名性之间的平衡。相反，更有可能的是，我们已经深入渗透到对手的网络中，以至于我们可以监视和了解他们的计划过程。

当然，匿名是有利有弊的，因为它也可以保护仇恨言论和犯罪活动。但是，虽然身份识别可能很重要，但出于我在本章讨论的所有原因，匿名是有价值的。它保护隐私，它赋予个人权力，它是自由的基础。

11

安全

维护网络空间安全。很重要。它们是犯罪，而不是恐怖主义，只有威胁和外来威胁，侵略，我的威胁只是在最后四章描述了其他人。

我们需要防御一系列的威胁，这就是我们开始遇到问题的地方。为了保护我们自己不受恐怖主义的侵害而忽视警察过于激进或政府暴政的风险，就像为了保护我们自己不受警察越权的侵害而忽视恐怖主义的风险一样没有意义。

不幸的是，作为一个社会，我们往往一次只关注一种威胁，而把其他威胁最小化。更糟糕的是，我们倾向于关注罕见和壮观的威胁，而忽略了更频繁和普通的威胁。所以比起开车，我们更害怕坐飞机，尽管前者安全得多。或者我们更害怕恐怖分子而不是警察，尽管在美国，你被警察杀死的可能性是被恐怖分子杀死的9倍。

我们让我们的恐惧阻碍了智能安全。以牺牲其他威胁为代价来防御某些威胁是一种失败的策略，我们需要找到平衡所有威胁的方法。

防范恐怖分子和犯罪分子的安全

美国国家安全局反复使用“连点”的比喻来为其监控活动辩护。一次又一次，在9/11之后，在内衣炸弹袭击者之后，在波士顿马拉松爆炸案之后，政府被批评没有把这些点联系起来。

然而，这是一个极具误导性的比喻。把彩色画册上的点连起来很容易，因为它们都有编号，而且是可见的。在现实生活中，这些点只有在事后才能被识别出来。

这并不妨碍我们要求知道为什么当局不能把这些点联系起来。胡德堡枪击案、波士顿马拉松爆炸案和维斯塔岛枪击案留下的警示信号事后看来很明显。风险工程专家纳西姆·塔勒布(Nassim Taleb)将这种倾向称为“叙事谬误”。人类天生就是讲故事的人，故事的世界比现实要整洁、可预测、连贯得多。数以百万计的人举止怪异，足以引起FBI的注意，而且几乎所有人都是无害的。美国运输安全管理局的禁飞名单上有2万多人。恐怖分子身份数据集市环境，也被称为观察名单，有68万人，其中40%的人“没有公认的恐怖组织隶属关系”。

数据挖掘是作为一种技术提供的，它将使我们能够将这些点连接起来。但是，虽然公司成功地挖掘我们的个人数据，以便定位广告、检测金融欺诈和执行其他任务，但三个关键问题使数据挖掘成为寻找恐怖分子的不合适工具。

第一个，也是最重要的一个问题是错误率。对于广告来说，即使错误率很高，数据挖掘也能取得成功，但发现恐怖分子需要比数据挖掘系统所能提供的准确度高得多的精度。

当你在搜索一个定义良好的个人资料时，当每年有合理数量的事件发生时，当误报的成本较低时，数据挖掘的效果最好。检测信用卡欺诈是数据挖掘的安全成功案例之一:所有信用卡公司都会挖掘他们的交易数据库，寻找表明被盗卡的消费模式。美国有超过10亿张活跃的信用卡在流通，其中每年有近8%的信用卡被欺诈使用。许多信用卡盗窃案都有一个共同的模式——在持卡人通常不常去的地方购物，购买旅游、奢侈品和容易交易的物品——在许多情况下，数据挖掘系统可以通过防止欺诈交易来最大限度地减少损失。虚惊一场的唯一代价就是给持卡人打个电话，让她核实几笔消费。

同样，美国国税局用数据挖掘来识别逃税者，警方用它来预测犯罪热点，银行用它来预测贷款违约。基于数据和应用，这些应用成败参半，但它们都在数据挖掘所能完成的范围内。

恐怖主义的阴谋是不同的，主要是因为尽管欺诈很常见，但恐怖袭击却非常罕见。这意味着，即使是高度准确的恐怖主义预测系统也会充斥着假警报，以至于它们将毫无用处。

究其原因，在于探测的数学。所有的检测系统都有误差，系统设计者可以对它们进行调整，以最小化假阳性或假阴性。在恐怖分子检测系统中，当系统错误地将无害的东西识别为威胁时，就会出现假阳性。当系统错过了实际的攻击时，就会出现假阴性。根据你如何“调优”你的检测系统，你可以增加误报的数量来保证你不太可能错过一次攻击，或者你可以以错过攻击为代价来减少误报的数量。

因为恐怖袭击是如此罕见，假阳性完全压倒了系统，无论你如何调整。我的意思是完全:如果系统发现任何真正的恐怖主义阴谋，数百万人将被错误地指控。

如果误报的代价很小，我们也许能够处理所有被系统标记的无辜者。想想机场的全身扫描仪吧。它们在扫描人的时候一直处于警戒状态。但是运输安全管理局的工作人员可以通过简单的搜身检查假警报。这并不适用于更通用的基于数据的恐怖主义探测系统。每一个警报都需要经过漫长的调查才能确定其真假。这需要时间和金钱，还会妨碍情报人员从事其他富有成效的工作。或者，更简洁地说，当你在监视一切时，你什么也没看到。

美国情报界也把发现恐怖主义阴谋比作大海捞针。正如前美国国家安全局局长基思·亚历山大所说，“大海捞针”。这句话完美地说明了问题

大规模监控和大量收集。当你在找针头的时候，你最不想做的就是在上面堆更多的干草。更具体地说，没有科学依据认为，增加与无辜民众无关的数据会更容易发现恐怖袭击，而且有大量证据表明，事实并非如此。你可能增加了稍微多一点的信号，但你也增加了多得多的噪音。尽管NSA有“收集一切”的心态，但它自己的文件也证明了这一点。军事情报界甚至谈到了“从消防水管里喝水”的问题:有太多不相关的数据，根本不可能找到重要的部分。

我们在NSA的窃听项目中看到了这个问题:误报使系统不堪重负。在9/11之后的几年里，NSA每月向FBI提供数千条线索;结果每一条都是虚惊一场。成本是巨大的，最终让有义务调查所有线索的FBI特工感到沮丧。我们在可疑活动报告(sar)数据库中也看到了这一点:数以万计的报告，却没有实际的结果。NSA收集的所有电话元数据只导致了一次成功:一名出租车司机被定罪，他向一个对美国没有直接威胁的索马里组织汇了8500美元——这可能是捏造出来的，这样NSA在国会面前就能有更好的谈话点。

使用数据挖掘技术试图揭露恐怖主义阴谋的第二个问题是，每一次袭击都是独一无二的。谁能想到两个高压锅炸弹会被一个波士顿的大学生和他的哥哥放在背包里送到波士顿马拉松终点线?每一个实施恐怖袭击的罕见个体，都会对判定谁可能是恐怖分子的标准产生不成比例的影响，导致侦查策略失效。

第三个问题是，NSA试图寻找的人都很狡猾，他们试图避免被发现。在个性化营销的世界里，典型的监控对象并不是试图隐藏自己的活动。在警察或国家安全的背景下，这是不正确的。一种对抗性的关系使问题变得更加困难，也意味着大多数商业大数据分析工具根本不起作用。商业工具可以简单地忽略那些试图隐藏的人，并假设其他人的行为是良性的。政府的数据挖掘技术做不到这一点，因为这些人正是他们要找的人。

对手躲避监视的能力复杂程度各不相同。遗憾的是，大多数罪犯和恐怖分子——以及政治异见者——都相当无知，犯了很多错误。但这并不是数据挖掘的正当化;有针对性的监控也有可能识别出他们。问题在于，大规模监控的效果是否比定向监控好到足以证明其极高的成本是合理的。对NSA所有努力的几项分析表明，事实并非如此。

上面列出的三个问题无法解决。数据挖掘根本不是这项工作的正确工具，这意味着为其提供所需的所有大规模监控都是不合理的。基思·亚历山大将军(Keith Alexander)担任NSA局长时曾辩称，无所不在的监控将使NSA能够阻止9/11事件的发生。这似乎不太可能。他没能阻止2013年的波士顿马拉松爆炸案，尽管其中一名袭击者

在恐怖分子观察名单上，两人都有马虎的社交媒体记录——这是在9/11事件后的十几年磨练技术之后。NSA在爆炸案发生前收集了萨纳耶夫夫妇的数据，但并没有意识到这些数据比他们收集的数百万其他人的数据更重要。

这一点在《9/11委员会报告》中也有提及。该报告描述了未能“连接这些点”，大规模监控的支持者声称需要收集更多数据。但报告实际上说的是，情报部门在*没有*大规模监控的情况下掌握了有关阴谋的所有信息，而这些失误是分析不足的结果。

2006年，尽管阿卜杜勒穆塔拉布的父亲曾多次警告美国政府他很危险，但大规模监控并没有抓到他。液体炸弹袭击者(他们是政府禁止乘客在随身行李中携带大瓶液体，面霜和凝胶登机的原因)于2006年在伦敦的公寓被抓获，不是因为大规模监视，而是通过传统的调查警察工作。每当我们得知NSA的成功时，它总是来自有针对性的监控，而不是大规模的监控。一项分析表明，FBI从可疑活动报告、阴谋报告和其他不相关犯罪的调查中识别潜在的恐怖主义阴谋。

这是一个临界点。无处不在的监控和数据挖掘并不适合用来寻找专门的罪犯或恐怖分子。我们纳税人在大规模监控项目上浪费了数十亿美元，却没有得到我们所承诺的安全。更重要的是，我们浪费在这些无效监控项目上的钱，没有花在调查、情报和应急响应上，而这些都是已被证明有效的策略。

大规模监控和数据挖掘更适合于人口歧视的任务:寻找具有特定政治信仰的人，与某些人是朋友的人，秘密社团的成员，以及参加某些会议和集会的人。这些都是像中国这样意图控制社会的政府感兴趣的个人。数据挖掘之所以能找到他们，是因为和信用卡诈骗犯一样，持不同政见者很可能有一个明确的个人资料。此外，在威权统治下，不可避免的假警报不是什么问题;以煽动罪指控无辜的人会给民众带来恐惧。

美国国家安全局的监视工作不仅是无效的，实际上还让我们更不安全。为了理解其中的原因，我需要解释一下互联网安全、加密和计算机漏洞。下面的三个部分很短，但很重要。

互联网攻击与防御

在任何安全形势下，攻击与防御之间都有一场基本的军备竞赛。一方可能在一段时间内占据优势，然后技术发生变化，给另一方带来优势。然后又变回来。

想想军事技术和战术的历史。在19世纪初，军事防御者有优势;向防线冲锋要比防守危险得多。拿破仑首先想出了如何利用当时的武器进行有效的进攻。到第一次世界大战时，火器——尤其是机枪——已经变得如此强大，防守方再次占据了优势;堑壕战对进攻方来说是毁灭性的。在第一次世界大战中，随着闪电战的发明，潮流再次转变，攻击者再次获得优势。

现在，无论是在互联网上还是在一般的计算机上，攻击者都占据了优势。这是正确的，有几个原因。

- 破坏事情比修复事情容易。
- 复杂性是安全最大的敌人，我们的系统一直在变得越来越复杂。
- 计算机化系统的本质使得攻击者更容易在系统中找到一个可利用的漏洞，而防御者却很难找到并修复系统中的*所有*漏洞。
- 攻击者可以选择一个特定的攻击并集中精力，而防御者必须防范每一种可能性。
- 软件安全性普遍较差;我们根本不知道如何编写安全的软件，创建安全的计算机系统。是的，我们在不断改进，但我们做得还不是很好。
- 计算机安全技术含量很高，普通用户很容易出错，破坏他们可能拥有的任何安全措施。

这并不是说网络安全毫无用处，远非如此。攻击可能更容易，但防御仍然是可能的。良好的安全性使许多类型的攻击更加困难、代价更高、风险更大。面对不够熟练的攻击者，良好的安全性可以完全保护您。

在安全领域，我们是从风险管理的角度来思考的。你确定你的风险是什么，你应该采取什么合理的预防措施。所以，作为家里有电脑的人，你应该安装一个好的杀毒程序，打开自动更新，使你的软件保持最新，避免可疑的网站和陌生人发来的电子邮件附件，并做好备份。这些加上其他几个相当容易实施的基本步骤，将使你足够安全，免受普通罪犯和黑客的攻击。另一方面，如果你是中国、叙利亚或乌克兰的持不同政见者，试图避免被捕或暗杀，你的预防措施必须更全面。如果你是一个试图躲避警察的罪犯，一个试图阻止商业间谍活动的商人，或者一个试图挫败军事间谍活动的政府大使馆，同样如此。如果你特别担心公司收集你的数据，你就需要一套不同的安全措施。

对于许多组织来说，安全归根结底是基本的经济问题。如果安全成本低于因缺乏安全而可能造成的损失成本，那么安全就是赢家。如果安全成本大于可能损失的成本，那就接受损失。对个人来说，很多心理因素和经济因素混杂在一起。很难用金钱来衡量侵犯隐私或被列入政府观察名单的行为。但总体思路是一样的:成本vs收益。

这种分析的关键是随机攻击和目标攻击之间的区别。

大多数犯罪袭击都是机会主义的。2013年，黑客闯入零售商塔吉特公司的网络，窃取了4000万人的信用卡和其他个人信息。这是当时已知的同类事件中最大的一起，对该公司来说也是一场灾难——该公司首席执行官格雷格·斯坦哈费尔(Gregg Steinhafel)因此事件辞职——但犯罪分子并没有因为任何意识形态上的原因专门选择塔吉特公司。他们感兴趣的是获取信用卡号码来实施欺诈，任何公司的数据库都可以做到。如果塔吉特有更好的安全措施，犯罪分子就会去别的地方。这就像典型的入室盗窃。他想抢劫人家。虽然他可能对社区和家庭类型有一些选择标准，但他并不特别在意自己选择哪一个。作为房主，你的工作是让你的家对窃贼的吸引力低于你邻居的家。面对无定向的攻击，需要好的安全措施是相对的。

与2012年中国黑客对*《纽约*时报》的攻击相比，这些黑客可能与政府有关。在这起事件中，攻击者试图监控记者与中国持不同政见者的通信。他们特别针对*纽约时报*的电子邮件和内部网络，因为他们想要的信息就在那里。针对有针对性的攻击，重要的是你的绝对安全水平。你的邻居有什么样的安全措施是无关紧要的;你需要对攻击者的特定能力保持安全。

另一个例子:谷歌扫描所有Gmail用户的电子邮件，并使用从中收集的信息来定位广告。当然，不是b谷歌的员工在做这件事;电脑会自动完成。因此，如果您用谷歌无法自动翻译的晦涩语言编写电子邮件，那么您将不会受到谷歌算法的攻击——因为谷歌不值得手动翻译您的电子邮件。但如果你突然受到联邦调查局的针对性调查，官员们就会利用这段时间翻译你的电子邮件。

记住大规模监视和定向监视之间的安全区别;我们会一次又一次地回到这个问题上。

加密的价值

我刚才把互联网安全描述为一场军备竞赛，攻击者比防御者有优势。优势可能很大，但仍然是程度上的优势。除了在电影和漫画书中，永远不会出现一方拥有某些强大的技术，而另一方不可能获胜的情况。

加密技术，以及一般的密码学，是唯一的例外。不仅防御比攻击容易;防守比进攻容易得多，进攻基本上是不可能的。

与试图破解加密相比，加密有着巨大的内在数学优势。从根本上说，安全性是基于密钥的长度;密钥长度的微小变化会给攻击者带来巨大的额外工作量。难度呈指数级增长。64位密钥可能需要攻击者一天的时间才能破解。a

同样的攻击者需要两倍的时间来破解65位的密钥，也就是两天。128位的密钥——最多是加密工作的两倍——将花费同一个攻击者264倍的时间，或者100万亿年的时间来破解。(相比之下，地球已有45亿年的历史。)

这就是为什么你会听到这样的说法:“在宇宙热寂之前，这是不可能被打破的，即使你假设攻击者用地球上所有的原子建造了一台巨大的计算机。”奇怪的是，这些话并不是夸大其词。它们只是加密和破解之间数学失衡的结果。

至少，理论上是这样的。问题是，加密只是一堆数学，而数学没有代理。要把那个加密数学变成可以真正为你提供一些安全性的东西，就必须用计算机代码来写。而这些代码需要在一台电脑上运行:一台有硬件、操作系统和其他软件的电脑。这台计算机需要由人操作，并连接到网络上。所有这些都会不可避免地引入漏洞，破坏数学的完美，并使我们回到前面讨论的安全状况——一个强烈倾向于攻击的状况。

NSA当然有一些机密的数学和大规模的计算能力，让它更容易破解某些类型的加密。为此，它在田纳西州橡树岭建立了多程序研究设施(Multiprogram Research Facility)。尽管nsa的密码分析能力非常先进，但我们从斯诺登的文件中了解到，nsa主要是利用计算机、人员和网络上的其他漏洞来规避加密，而不是直接解决加密问题。NSA入侵系统，就像网络罪犯做的那样。它的“量身定制访问行动”(Tailored Access Operations)小组侵入网络并窃取密钥。它利用用户选择的错误密码，以及默认或弱密钥。它获取法院命令并要求获得加密密钥的副本。它秘密地在产品和标准中插入漏洞。

斯诺登在2013年的一次在线问答中是这样说的:“加密有效。正确实施的强大加密系统是你可以依赖的少数东西之一。不幸的是，端点安全性非常薄弱，NSA经常可以找到绕过它的方法。”

但NSA可以用来获取加密数据的其他方法恰恰说明了加密为何如此重要。通过利用这种数学上的不平衡，密码学迫使攻击者追求这些其他路线。攻击者可能不得不闯入特定的计算机系统并获取明文，而不是被动地窃听通信通道并收集每个人的数据。与大量收集未加密数据相比，这些绕过加密的路径需要更多的工作、更大的暴露风险和更大的针对性。

记住大数据的经济学原理:就像保存所有东西比找出保存什么更容易一样，监视每个人比找出谁值得被监视更容易。广泛的加密技术有可能使大规模监控失效，并迫使窃听者选择监听目标。这对隐私来说是一个巨大的胜利，因为攻击者没有足够的预算来选择每个人。

漏洞的普遍性

漏洞就是错误。它们是设计或实现上的错误——代码或硬件上的小故障——允许未经授权的入侵系统。因此，例如，网络犯罪分子可能会利用一个漏洞闯入你的电脑，窃听你的网络连接，并窃取你用于登录你的银行账户的密码。政府情报机构可能会利用漏洞闯入外国恐怖组织的网络并破坏其运作，或窃取外国公司的知识属性。另一个政府情报机构可能会利用一个漏洞来窃听持不同政见者、恐怖组织或敌对政府领导人。军方可能会利用漏洞发射网络武器。这都是黑客行为。

当有人发现一个漏洞时，她既可以用来防御，也可以用来进攻。防御意味着提醒供应商并对其进行修补——并将其发布，以便社区可以从中吸取教训。许多漏洞是由供应商自己发现的，并在没有任何宣传的情况下进行修补。还有一些是由研究人员和有道德的黑客发现的。

攻击包括利用漏洞攻击他人。未公布的漏洞被称为“零日”漏洞;对于攻击者来说，它们非常有价值，因为没有人受到保护，它们可以在全球范围内使用而不受惩罚。最终，受影响软件的供应商发现——时间取决于漏洞被利用的范围——并发布补丁来关闭它。

如果进攻性军事网络部队或网络武器制造商发现了这一漏洞，它将对其保密，以便将来用于制造网络武器。如果很少被秘密使用，这个漏洞可能会在很长一段时间内保密。如果不使用，它将一直保密，直到其他人发现它。

发现者可以出售漏洞。以攻击为目的的零日漏洞有一个强大的市场——政府和向政府出售网络武器的制造商都是买家——而在黑市上，发现者可以向罪犯出售漏洞。一些供应商为漏洞提供赏金，以刺激防御研究，但赏金要低得多。

未被发现的零日漏洞很常见。每一个商业软件——你的智能手机，你的电脑，运行核电厂的嵌入式系统——都有数百甚至数千个漏洞，其中大多数未被发现。编程的科学和工程技术还不足以生产出完美无瑕的软件，而且这种情况短期内不会改变。软件开发的经济学优先考虑的是功能和上市速度，而不是安全性。

这一切意味着，黑客攻击的威胁不会消失。在可预见的未来，一个足够熟练的攻击者总是有可能在防御者的系统中找到漏洞。对于制造网络武器的军队、试图侵入系统进行窃听的情报机构，以及各种犯罪分子来说，都将是如此。

维护一个不安全的互联网

在第6章中，我讨论了NSA如何使用现有的和专门创建的漏洞来入侵系统。它的行为将监视置于安全之上，最终使我们所有人都不那么安全。根据《*卫报*》关于斯诺登文件的一篇文章，NSA和政府通信总部是这样想的:“两家机构之间的机密简报庆祝他们成功地‘击败了网络安全和隐私....’。”

政府到底是如何打败安全和隐私的呢?我们知道NSA主要采用以下四种做法。假设俄罗斯、中国和其他各种国家也在使用类似的方法。网络犯罪分子也不甘落后。

在**我们每天使用**的**商业软件**中**囤积漏洞，而不是确保这些安全漏洞得到修复**。当NSA发现(或购买)一个漏洞时，它可以通知供应商并修复一个仍然保密的漏洞，或者它可以抓住它并利用它来窃听目标计算机系统。这两种策略都支持美国的重要政策目标，但NSA必须在每种情况下选择哪一种。

现在，美国——无论是NSA还是美国网络司令部——都在储备零日漏洞。目前尚不清楚有多少个。2014年，白宫曾试图在一篇博客文章中澄清美国在这方面的政策，但并没有真正解释清楚。我们知道，单一网络武器震网(Stuxnet)就使用了四个零日漏洞。在一次网络攻击中使用这么多零日攻击意味着政府的库存有数百个。

在国会作证时，前NSA局长迈克尔·海登介绍了该机构术语NOBUS，即“除了我们没有人”——也就是说，除了我们没有人可能发现或使用的漏洞。NSA有一个机密程序来决定它应该如何处理漏洞。该机构声称，它公开并关闭了它发现的大多数漏洞，但保留了一些——不知道有多少——它认为是nobus。

这种方法似乎是合适的一般框架，但在实践中是不可能应用的。我们安全领域的许多人都不知道如何做出NOBUS决策，我们担心政府也不会。

这种囤积让每个人都处于危险之中。未修补的漏洞会让我们更不安全，因为任何人都可以独立地发现它们，并利用它们来攻击我们。它们本质上是不稳定的，尤其是因为它们只在有限的时间内有效。更糟糕的是，每次使用都有风险，其他人会知道这个漏洞，并将其用于自己。它们以家庭的形式出现;保守一个秘密，可能意味着一整类漏洞都没有被发现，也没有被修补。美国和其他西方国家非常容易受到零日攻击，因为我们的关键电子基础设施、知识属性和个人财富。像中国和俄罗斯这样的国家不那么容易受到攻击——朝鲜更少——所以他们修复漏洞的动力要小得多。

在**广泛使用**的**计算机硬件和软件产品中植入后门**。后门并不新鲜。长期以来，安全行业一直担心黑客在软件中留下后门，并花费了相当多的精力来寻找和修复后门。

但现在我们知道，美国政府正在故意将后门植入硬件和软件产品中。

斯诺登披露的一份NSA文件描述了“SIGINT启用项目”，其中一项策略是“在商业加密系统、IT系统、网络和目标使用的端点通信设备中插入漏洞”。我们对这个项目了解不多:其中有多少是在相关制造商知情并同意的情况下完成的，又有多少是由秘密为政府工作的员工或秘密操纵公司主源代码文件秘密完成的。我们也不知道它的成功程度如何——文件没有给我们很多细节——但我们知道它的资金是每年2.5亿美元。我们也不知道还有哪些国家对受其政治控制的公司设计的系统做同样的事情。

我们知道一些例子。在第6章中，我谈到了微软为NSA削弱Skype。NSA还向微软施压，要求其在其硬盘加密软件BitLocker中设置后门，尽管该公司似乎拒绝了。想必还存在其他涉及其他产品的努力;我私下也听说过几次不成功的尝试。

故意制造漏洞是非常危险的，因为没有办法对任何系统实施后门访问，以确保只有政府可以利用它。政府授权的访问会迫使企业降低产品和服务对所有人的安全性。

例如，在2004年6月到2005年3月之间，有人窃听了100多个希腊政府成员的手机——包括总理、国防部长、外交部长和司法部长——以及其他重要的希腊公民。瑞典电信供应商爱立信(Ericsson)在沃达丰的产品中植入了这种窃听功能，但只对提出要求的政府开放。希腊政府不在其中，而是某个尚不为人知的政党——敌对的政治团体?有组织犯罪?-弄明白了如何偷偷地打开这个功能。

这不是一个孤立的事件。2006年，意大利也发生过类似的事件。2010年，中国黑客利用b谷歌安装在Gmail上的拦截系统，以满足美国政府的监控要求。2012年，我们了解到，卖给美国国防部的每一台手机交换机，其监控系统都存在安全漏洞;我们不知道这些漏洞是无意插入的，还是故意插入的。

NSA经常利用其他国家系统内置的后门来达到其他目的。例如，它利用百慕大电话系统内置的窃听功能，秘密截获了该国*所有*的电话。为什么它相信同样的事情不会发生在我们身上呢?

破坏加密算法和标准。另一个目标是SIGINT启用项目旨在“影响商业公钥技术的政策、标准和规范”。同样，细节很少，但我认为这些努力更多地集中在手机安全等专有标准上，而不是公共标准

比如加密算法。例如，NSA影响了GSM手机加密算法的采用，它很容易破解。我们所知道的一个公开例子是NSA将一个后门的随机数生成器插入到一个通用的互联网标准中，然后努力使该生成器得到更广泛的使用。其目的是破坏人们用来保护互联网通信和网页浏览的加密技术，但并不是很成功。

黑客攻击互联网。在第五章中，我谈到了NSA的TAO小组及其黑客任务。除了直接侵入电脑和网络设备外，NSA还伪装成脸书和LinkedIn(可能还有其他网站)，渗透目标电脑，将互联网流量重定向到自己的虚拟网站，以达到窃听目的。英国政府通信总部(GCHQ)可以在脸书上找到你的私人照片，人为增加网站流量，干扰网站视频，删除电脑账户，入侵在线投票，等等。

除了所有这些策略在互联网用户中引起的极度不信任之外，它们还要求NSA确保监视优先于安全。NSA不是为了每个人的利益而提高互联网的安全性，而是为了自己的方便而确保互联网仍然不安全。

这伤害了我们所有人，因为NSA并不是唯一一个依靠不安全感而茁壮成长的机构。其他政府和犯罪分子也从颠覆安全中获益。斯诺登披露的大量秘密监控技术并非NSA所独有，甚至也不是其他国家情报机构所独有。它们只是资金更充裕的黑客工具。学者们讨论了用开源和商业系统重建NSA收集和分析工具的方法。

例如，当我与《卫报》合作处理斯诺登文件时，NSA极力不希望我们曝光的一个绝密项目是QUANTUM。这是NSA所谓的信息包注入项目，基本上，这是一种允许该机构侵入计算机的技术。然而，事实证明，并不是只有NSA在使用这项技术。中国政府使用数据包注入来攻击计算机。网络武器制造商黑客团队向任何愿意购买的政府出售数据包注入技术。犯罪分子使用它。也有黑客工具让个人也有这种能力。这些在我写《QUANTUM》之前就已经存在了。NSA利用其知识来攻击他人，而不是建立互联网防御，以确保任何人都可以使用数据包注入来入侵计算机。

即使在NSA内部开发了技术，它们也不会长期保持排他性。今天的绝密项目，就会变成明天的博士论文，第二天的黑客工具。最初为军事网络武器震网病毒开发的技术最终被用于犯罪恶意软件。Elcomsoft出售给政府的密码破解软件也曾被黑客用来从iCloud账户中窃取名人照片。曾经秘密使用的监控人们手机的技术现在也被广泛使用。

美国政府对不受约束的监控的渴望已经影响了互联网的运作方式。当监控变成多国合作时，这些需求

将越来越优先于其他需求。而网络工程师为满足政府监控要求而做出的架构选择可能会持续几十年，原因很简单，因为继续做同样的事情比改变更容易。通过将监视置于安全之上，NSA确保了我们所有人的不安全。

网络攻击的附带损害

随着各国继续相互攻击，使用互联网的公众越来越成为附带损害的一部分。大多数时候，我们不知道细节，但有时足够的信息浮出水面，我们知道。

三个例子:震网的目标是伊朗，但恶意软件意外感染了印度、印度尼西亚、巴基斯坦和其他地方的5万多台电脑，包括雪佛龙公司(Chevron)拥有的电脑和德国的工业工厂;它可能是2010年印度卫星故障的罪魁祸首。斯诺登声称，NSA在2012年意外导致了叙利亚的互联网中断。同样，中国的防火长城使用了一种名为DNS注入的技术来阻止对某些网站的访问;这种技术经常会中断与中国或被审查链接无关的通信。

越多的国家通过全球互联网相互攻击——无论是为了获取情报还是造成破坏——越多的民用网络将成为附带损害。

损害国家利益

在第9章中，我讨论了NSA的活动如何损害美国的经济利益。它也损害了美国的政治利益。

政治学家伊恩·布雷默(lan Bremmer)认为，NSA活动的公开披露“严重损害了美国在许多盟友中的信誉”。美国在世界舞台上的利益受到了严重损害，因为一个又一个国家知道了我们对其公民或领导人的窥探行为:欧洲、拉丁美洲和亚洲的友好国家。自从美国国家安全局(NSA)监听德国总理安格拉·默克尔(Angela Merkel)的手机一事曝光以来，美国和德国之间的关系变得尤为紧张。巴西总统迪尔玛·罗塞夫(Dilma Rousseff)拒绝了美国的国宴邀请——这是世界各国领导人第一次拒绝美国的国宴邀请——因为她和巴西其他国家的人对美国国家安全局(NSA)的监视行为感到愤怒。

在幕后，通过更多的私人外交渠道，发生了更多的事情。如果美国正以其咄咄逼人的监控项目破坏其全球地位和领导地位，那就无可避免了。

PART THREE

WHAT TO DO ABOUT IT

12

原理

大规模监控带来的危害是多方面的，对个人和整个社会造成的损失不成比例地超过了好处。我们能够而且必须做些什么来控制它。在提出具体的法律、技术和社会建议之前，我想以一些一般原则作为本节的开始。这些都是关于监控以及我们应该如何应对的普遍真理，适用于政府和企业。

阐明原则是比较容易的部分。在具体情况下应用这些原则要困难得多。“生命、自由和追求幸福”是我们都同意的原则，但我们只需要看看华盛顿特区，就会知道实施这些原则有多困难。我参加过许多小组讨论和辩论，在这些讨论和辩论中，这个问题的各方都同意关于数据收集、监视、监督、安全和隐私的一般原则，尽管他们在如何将这些原则应用到手头的世界上存在激烈的分歧。

安全和隐私

通常争论的特点是“安全与隐私”。这种过于简单化的观点要求我们在两者之间做出某种根本性的取舍:为了变得安全，我们必须牺牲自己的隐私，让自己受到监控。而如果我们想要某种程度的隐私，我们必须认识到，为了得到它，我们必须牺牲一些安全。

这是一种虚假的取舍。首先，有些安全措施要求人们放弃隐私，但有些根本不侵犯隐私:飞机上的门锁、高围栏、警卫、加固的驾驶舱门。其次，隐私和安全从根本上是一致的。当我们没有隐私时，我们会感到暴露和脆弱;我们会觉得不那么安全。同样，如果我们的个人空间和记录不安全，我们的隐私就会减少。美国宪法第四修正案谈到了“人民享有人身、房屋、文件和财产安全的权利”(斜体mine)。它的起草者认识到，隐私对于个人安全至关重要。

将对话框定为以安全换取隐私，会导致不平衡的评估。通常，这种权衡是以货币成本的形式呈现的:“你愿意为隐私支付多少钱?”或者“你愿意为安全支付多少钱?”但这也是一种错误的权衡。不安全感的代价是真实的、发自内心的，即使是抽象的;隐私丧失的成本在抽象中是模糊的，只有当有人面对其后遗症时，才会变得有形。这就是为什么我们在拥有隐私的时候会低估它的价值，而只有在失去隐私的时候才会认识到它的真正价值。这也是为什么我们经常听到没有人愿意为隐私付费，因此安全绝对胜过隐私的原因。

当安全与隐私的权衡被框定为生死抉择时，所有理性的辩论都结束了。当生命危在旦夕时，谁还能谈论隐私呢?害怕的人会更容易为了安全感而牺牲隐私。这就解释了为什么美国政府在9/11事件后可以如此自由地进行大规模监控。政府基本上是说，我们所有人都必须放弃自己的隐私，以换取安全;我们大多数人都不知道，因此接受了浮士德式的交易。

问题是，不安全感的全部重量与对隐私的增量侵犯进行了比较。美国法院经常这样做，说的是这样的话:“我们同意在这个或那个政府项目中存在隐私损失的风险，但在纽约引爆核弹的风险太大了。”这是对这种取舍的草率描述。这并不是说，如果我们监视，核爆炸就不可能发生，或者如果我们不监视，核爆炸就不可避免。这种可能性已经非常小了，正在考虑的理论上侵犯隐私的安全计划只能将这个数字略微降低。这就是需要考虑的取舍。

更一般地说，我们的目标不应该是在安全和隐私之间找到一个可以接受的权衡，因为我们可以也应该把两者都维护在一起。

安全重于监控

安全和监视是相互冲突的设计要求。为安全而构建的系统更难被监控。相反，为方便监控而构建的系统更难确保安全。系统中内置的监控能力是不安全的，因为我们不知道如何构建一个只允许*适当*类型的人进行监控的系统。我们在第11章已经看到了这一点。

我们需要认识到，对于整个社会来说，安全比监控更重要。也就是说，我们需要选择一个能够抑制监控的安全的信息基础设施，而不是一个允许容易监控的不安全的基础设施。

这个推理适用于一般情况。我们的基础设施既有好的用途，也有坏的用途。银行劫匪在高速公路上开车，用电，在五金店购物，在通宵餐厅吃饭，就像诚实的人一样。无辜者和罪犯一样使用手机、电子邮件和Dropbox。正义和不正义都在下雨。

尽管如此，社会仍在继续运转，因为对基础设施的诚实、积极和有益的使用远远超过了不诚实、消极和有害的使用。我们高速公路上的司机中银行抢劫犯的比例可以忽略不计，电子邮件用户中罪犯的比例也可以忽略不计。为我们大多数人设计所有这些系统更有意义，因为我们需要罪犯、电话推销员，有时甚至是我们自己的政府提供安全保障。

通过优先考虑安全问题，我们将保护世界的信息流——包括我们自己的信息流——免受窃听以及盗窃和破坏等更具破坏性的攻击。我们将保护我们的信息流不受政府、非国家行为体和犯罪分子的侵犯。我们将使整个世界更加安全。

Tor就是一个很好的例子。它是免费的开源软件，你可以用它来浏览

在互联网上匿名浏览。首先由美国海军研究实验室资助，然后由国务院资助，它被世界各地的持不同政见者用来逃避监视和审查。当然，犯罪分子也会出于同样的目的使用它。Tor的开发人员不断更新该程序，以逃避中国政府的禁令。我们知道，NSA一直在试图破解它，至少从斯诺登披露的2007年NSA文件来看，一直没有成功。我们知道联邦调查局在2013年和2014年入侵了电脑，因为它无法破解Tor。与此同时，我们相信在NSA和GCHQ工作的个人都在匿名帮助保持Tor的安全。但这是一个困境:Tor要么强大到足以保护我们喜欢和不喜欢的人的匿名性，要么它不够强大到足以保护两者的匿名性。

当然，永远不会有一个没有人监视的未来。那就是naïve。从历史开始，政府就一直在监视;甚至在旧约中也有一些间谍的故事。问题是我们想要走向什么样的世界。我们是否希望通过限制政府的监督、审查和控制能力来减少权力失衡?还是允许政府对我们拥有越来越大的权力?

当然，“安全高于监视”并不是绝对的规则。有时候，有必要设计一个系统来保护我们中少数不诚实的人。飞机安全就是一个例子。与非恐怖分子相比，乘坐飞机的恐怖分子数量微不足道，但我们围绕着这几个人设计整个机场，因为飞机上的安全故障比任何地方的恐怖主义炸弹都要致命。不过，我们(还)没有围绕预防恐怖主义来设计我们的整个社会。

有时候，我们也需要在系统中设计适当的监控。我们希望航运服务能够实时跟踪包裹。我们希望急救人员能够知道紧急手机电话来自哪里。当然，在这些情况下，我们不会使用“监视”这个词;我们会用一些不那么情绪化的术语，比如“包裹追踪”。

这里的一般原则是，系统应该在设计时尽可能少地进行必要的监视，以使其发挥作用，而在需要监视的地方，系统应该收集尽可能少的必要信息，并在尽可能短的时间内保留这些信息。

透明度

透明对于任何开放和自由的社会都是至关重要的。政府公开法和信息自由法让公民知道政府在做什么，并使他们能够履行监督政府活动的民主义务。公司信息披露法在私人领域也发挥着类似的作用。当然，公司和政府都有一定的保密需求，但它们越能公开，我们就越能明智地决定是否信任它们。现在在美国，我们有强有力的开放政府和信息自由法，但太多的信息不受它们的约束。

对于个人数据，透明度是相当直接的:人们应该有权知道关于他们的哪些数据被收集了，关于他们的哪些数据被存档了，关于他们的数据是如何被使用的——以及被谁使用的。在一个国际互联网与各国有关监视和控制的具体法律相结合的世界里，我们需要知道关于我们的数据被存储在哪里。如果我们知道这些事情，我们就更有可能对任何级别的监视感到舒服。隐私政策应该提供这些信息，而不是太长，故意混淆，以至于它们没有揭示什么。

我们还需要让那些根据我们的数据来判断我们的算法透明化，要么公布代码，要么解释它们是如何工作的。现在，我们无法判断TSA算法的公平性，这些算法会选择我们中的一些人进行“特殊筛选”。我们也无法判断IRS选择我们中的一些人进行审计的算法。搜索引擎算法决定我们看到哪些网页，预测性警务算法决定带谁来问话，哪些社区需要巡逻，信用评分算法决定谁可以获得抵押贷款，这些都是一样的。其中一些保密是必要的，这样人们就不会想出如何与系统博弈，但大部分不是这样。《欧盟数据保护指令》已经要求披露其中的大部分信息。

这似乎让我自相矛盾。一方面，我主张保护个人隐私，而不是强制监控。另一方面，我主张政府和企业透明，而不是机构保密。我之所以对两者都说“是”，是因为人与机构之间现存的权力失衡。制度自然比人拥有更大的权力。制度保密增加了制度权力，这种权力差距就会扩大。这本质上不利于个人自由。个人隐私增加了个人权力，从而减少了这种权力差异。这有利于自由。透明度和监督也是一样。制度的透明减少了权力的不平衡，这是好事。对个人的制度性监督加剧了权力的不平衡，这是不好的。

透明度来之不易。有权有势的人不喜欢被监视。例如，警察越来越不喜欢被监视。在美国各地，警察骚扰并起诉那些对他们进行录像的人，一些司法管辖区已经裁定这是非法的。芝加哥的警察故意遮挡摄像头，显然是为了掩盖自己的行为。圣地亚哥警察局则拒绝了所有提供警方录像的要求，声称这是正在进行的调查的一部分。在2014年密苏里州弗格森的抗议活动中，在警察杀死一名手无寸铁的黑人男子之后，警察经常阻止抗议者录制他们的视频，有几名记者因记录事件而被捕。洛杉矶警方甚至在巡逻车上破坏法院授权的录音设备。

政府和企业经常抵制各种透明度法律。但保密的世界正在发生变化。隐私法学者彼得·斯维尔(Peter Swire)写了一篇关于秘密半衰期的文章。他观察到的是，一般来说，秘密比以前暴露得更快。科技让秘密更难被保守，而互联网的本质让秘密更难被长期保守。按下“发送”按钮就能传递信息

千兆字节的信息瞬间传遍互联网。一个u盘每年可以存储更多的数据。政府和组织都需要假设，他们的秘密比以往任何时候都更有可能被曝光，而且曝光得更快。

秘密半衰期缩短的影响之一是，它们的披露更具破坏性。斯诺登的一份文件显示，NSA监听了德国总理安吉拉·默克尔的手机。这份文件没有注明日期，但显然是最近几年的内容。如果这份文件在20年后公布于众，德国的反应将与2013年发生的公众骚动大不相同，当时默克尔仍在执政，该事件是当前事件，而不是历史事件。

文化的变化也让保密变得更加难以保守。在过去，保守机构机密是一种终身文化的一部分。情报界会在人的职业生涯早期招募他们，并给他们提供终身工作。这是一个私人的男人俱乐部，充满了暗语和秘密知识。企业界也到处都是终身工作者。那些日子已经一去不复返了。情报部门的许多工作现在都外包了，企业界也不再有终身工作的文化。劳动力是灵活的，工作是外包的，人是可以牺牲的。从一个雇主换到另一个雇主是现在的常态。这意味着秘密会被更多的人分享，而那些人对秘密的关心就更少了。回想一下，美国有500万人拥有安全许可，其中大多数是承包商，而不是政府雇员。

人们也更加信仰开放的价值，尤其是在年轻人中。年轻人在分享个人信息方面比他们的长辈要自在得多。他们认为信息想要自由，安全来自于公众的知识和辩论。他们在网上说过非常私人的事情，也在社交网站上晒过自己的尴尬照片。他们在公开的网络论坛上被恋人甩过。他们以最妥协的方式被掩盖，却完好无损地活了下来。要说服这群人相信政府的保密胜过公众的知情权，难度更大。

这些技术和社会趋势是一件好事。只要有可能，我们就应该争取透明度。

监督和问责

为了让大多数社会正常运转，人们必须赋予他人管理自己的权力。让出权力本身就是一件危险的事情，几千年来，我们在这样做的同时，已经形成了一个保护自己的框架:透明度、监督和问责制。如果我们知道人们是如何使用我们赋予他们的权力的，如果我们能确保他们没有滥用权力，如果我们能在他们滥用权力时惩罚他们，那么我们就能更安全地将权力托付给他们。这是民主的基本社会契约。

监督有两个层面。第一个层面是战略层面:我们实施的规则是否正确?例如，NSA可以实施自己的程序来确保遵守规则，但它不应该决定应该遵守哪些规则。这个

前NSA局长迈克尔·海登(Michael Hayden)很好地解释了这一点:“给我一个你允许我在里面操作的盒子。”我将在这个框框的边缘发挥作用... .你们，美国人民，通过你们选出的代表，给我一个发挥的空间，我将非常积极地发挥。”从某种意义上说，他是对的;制定规则并不是他的职责。但另一方面他是错的，我会在第13章讨论这个。

无论哪种情况，我们都需要在战略监督方面做得更好。我们需要就应该对政府和政府监督施加哪些限制展开更公开的辩论。我们需要立法机构进行有意义的监督，并制定前瞻性的应对措施。我们还需要公开、独立的法院执行法律，而不是橡皮图章机构的做法，定期报道政府行为，充满活力的公共部门媒体和监督团体分析和辩论掌权者的行为，是的，还有一个举报的法律框架。以及一个关心的公众。我也会在第13章中讲到这个。

另一种监督是战术上的:规则被遵守了吗?这种监督的机制包括程序、审核、审批、故障排除协议等等。例如，美国国家安全局(NSA)对其分析师进行管理其工作的法规培训，审核系统以确保这些法规得到切实遵守，并在他们没有遵守这些法规的情况下建立报告和纪律处分程序。

不同的组织会对彼此进行战术监督。授权程序就是一个例子。当然，我们可以相信警察只在他们应该进行搜查时才进行搜查，但相反，我们要求他们将他们的请求提交给中立的第三方——法官——他确保他们在发布法院命令之前遵守规则。

强有力的监督的关键是独立性。这就是为什么我们总是对内部审查持怀疑态度，即使这些审查是由一个强有力的倡导者进行的。这是DHS首席隐私官的一个关键问题。我记得玛丽·艾伦·卡拉汉(Mary Ellen Callahan)，她从2009年到2012年担任该职位。她是隐私的伟大倡导者，并建议该机构取消几个项目，因为隐私问题。但她向DHS部长珍妮特·纳波利塔诺(Janet Napolitano)汇报，而她所能做的就是提出建议。如果卡拉汉不在DHS工作，她就会有更正式的监管权力。由人手充足、知识渊博的外部评估人员进行监管，效果会好得多。

你可以把战术监督和战略监督的区别看作是正确做事和正确做事的区别。两者都是必需的。

没有问责制，这两种监督都无法发挥作用。那些被赋予权力的人不能随意滥用权力而不受惩罚;滥用权力必须受到惩罚。没有问责制的监督意味着什么都改变不了，这是我们一次又一次学到的。或者，正如风险分析师纳西姆·塔勒布(Nassim Taleb)所指出的那样，当人们参与其中时，组织滥用权力的可能性就会降低。

说“透明、监督和问责”很容易，但要让这些原则在实践中发挥作用要困难得多。尽管如此，我们必须尝试——我将在下一章讨论如何做到这一点。这三点使我们有信心信任强大的机构。如果

如果我们要让他们拥有凌驾于我们之上的权力，我们需要保证他们会为我们的利益行事，不会滥用这种权力。

弹性设计

在系统架构中，为弹性而设计是一个重要的、近乎哲学的原则。技术解决方案通常被认为是完美的。然而，我们都知道，完美是不可能的——人、组织和系统本质上是有缺陷的。从政府机构到大型跨国公司，所有组织都存在缺陷。

这些不完美并不仅仅是良好系统内的不良行为者的结果。不完美可能是平凡的、普通的、官僚主义的随波逐流。不完美的一种形式是任务蠕变。另一种是来自组织内部的人，他们只关注组织的狭隘需求，而不关注他们行为的广泛影响。不完美也来自社会变革:随着时间的推移，我们的价值观发生了变化。先进的技术给现有系统增加了新的扰动，造成了不稳定。

如果系统性缺陷是不可避免的，我们就必须接受它们——无论是法律、政府机构、企业、个人还是社会。我们必须设计出能预料到缺陷并能在缺陷存在的情况下正常工作的制度。如果某件事将要失败或中断，我们需要它以一种可预测的方式失败。这就是韧性。

在系统设计中，弹性来自于多种要素的组合:容错、缓解、冗余、适应性、可恢复性和可生存性。在我在本书中描述的复杂且不断变化的威胁环境中，这是我们所需要的。

我提倡为我们的监视系统和控制监视的系统提供几种不同的弹性:对硬件和软件故障的弹性，对技术创新的弹性，对政治变革的弹性，以及对胁迫的弹性。安全架构提供了应对不断变化的政治突发事件的弹性，这可能使政治监视合法化。多个重叠的权力机构提供了应对强制压力的弹性。适当的成文法律提供了应对不断变化的技术能力的弹性。自由为威权主义提供弹性。当然，要完全抵御这些事情中的任何一件，更不用说所有的事情，都是不可能的。但我们必须尽我们所能做好，甚至要假设我们的复原力不完美。

同一个世界，同一个网络，同一个答案

美国目前关于监控的争论主要围绕NSA的权力，以及限制NSA是否在某种程度上授权了其他人。这种争论是错误的。如果NSA停止监视，我们不能选择一个中国、俄罗斯和以色列停止监视的世界。我们必须决定的是，我们是要发展一个易受所有攻击者攻击的信息基础设施，还是一个对所有用户都安全的信息基础设施。

自1952年成立以来，NSA一直肩负着双重使命。首先，信号情报(SIGINT)涉及拦截美国敌人的通信。第二，通信安全，或COMSEC，涉及保护美国人

军方和一些政府通信不被拦截。将这两项任务结合起来是有道理的，因为了解如何窃听是保护自己不被窃听所必需的，反之亦然。

这两个任务是互补的，因为不同的国家使用不同的通信系统，军事人员和平民也使用不同的通信系统。但正如我在第五章所描述的那样，那个世界已经不复存在了。今天，NSA的两项任务发生了冲突。

法律可能决定哪些监视方法是合法的，但技术决定哪些是可能的。当我们考虑应该实施什么样的安全技术时，我们不能只看我们自己的国家。我们必须放眼世界。

我们不能在削弱敌人网络的同时保护自己的网络。情报机构用来互相监视的漏洞，也被犯罪分子用来窃取你的金融密码。因为我们都在使用同样的产品、技术、协议和标准，我们要么让每个人都更容易监视每个人，要么让任何人都更难监视任何人。这是自由与控制的较量，我们都是同甘共苦。哈佛大学法学教授、乔治·w·布什时期的前助理司法部长杰克·戈德史密斯(Jack Goldsmith)写道，“每一种进攻性武器都是我们防御的(潜在)漏洞——反之亦然。”

例如，美国的CALEA法要求电话交换机允许窃听。我们或许可以接受让美国警方拥有这种能力，因为我们通常信任司法授权程序，并认为警方不会滥用权力。但是那些电话交换机在世界范围内销售——还记得第十一章中关于希腊手机窃听的故事吗?它们具有同样的技术窃听能力。这是我们的选择:要么每个人都拥有这种能力，要么没有人拥有。

截取手机通话和元数据的imsi -catch也是如此。StingRay可能曾经是FBI的秘密，但这项技术已经不再是秘密了。有几十个这样的设备分散在华盛顿特区和国家其他地方，由谁知道什么政府或组织运营。下一个是犯罪用途。通过确保手机网络易受这些设备的攻击，这样我们就可以利用它们来破案，我们必然会允许外国政府和犯罪分子利用它们来对付我们。

我在第11章给出了更多的例子。总的来说，我们要决定如何建立我们的通信基础设施:安全与否，监控与否，隐私与否，恢复与否。然后*每个人都*可以使用这个基础设施。

13

政府的解决方案

斯诺登事件曝光后，奥巴马建议对NSA的情报进行改革。监控，2013年，奥巴马总统没有出现短缺，成立了一个关于监控和国家情报的审查委员会;该委员会提出了46项NSA政策建议。2014年，包括我在内的全球500个组织、专家和官员签署了《将人权应用于通信监控的国际原则》，通常被称为“必要和相称”原则。美国国会就几项法案进行了辩论，提出了一些小的改革;你读到这篇文章的时候，可能已经有一两个法案通过了。

在本章中，我将着眼于国家安全和执法，并提出一般性的政策建议，而不是详细的立法规定。其中一些很容易实现，而另一些则更有抱负。所有这些都是我认为政府需要长期努力的方向。

我并不是说政府永远不应该被允许进行监视或破坏。我们已经赋予警察广泛的权力来侵犯公民的隐私和获取我们的数据。我们这样做是明知故犯的，也是心甘情愿的，因为这有助于破案，从而使我们更安全。诀窍在于既要赋予政府机构这种权力，又不能让他们滥用这种权力。我们需要政府提供的安全保障，也需要政府提供的安全保障。这就是像美国宪法和欧洲宪章这样的文件试图做到的，这就是授权程序所做的，这就是我们在9/11袭击后疯狂争夺安全以对抗恐怖分子的平衡。

通信监控适用人权的国际原则-摘要(2014)

合法性:对隐私权的限制必须在法律中明确而准确地规定，并应定期进行审查，以确保隐私保护跟上快速的技术变革。
合法目的:通信监控应该只允许用于追求最重要的国家目标。

必要性:国家有义务证明其通信监控活动对于实现合法目标是必要的。

充分性:通信监督机制在实现其合法目标方面必须是有效的。

相称性:通信监视应被视为一种高度侵入性的行为，它干涉隐私权和意见和言论自由权，威胁到民主社会的基础。相称性的通信监控通常需要获得主管司法机关的事先授权。

主管司法机关:与通信监视有关的决定必须由公正和独立的主管司法机关作出。

正当程序:正当程序要求任何对人权的干涉都受到法律的约束

公开的程序，并在公平和公开的聆讯中持续适用。**用户通知:**应将授权监视其通信的决定通知个人。除非主管司法机关发现通知会损害调查，否则应向个人提供机会，在监视发生之前对其提出质疑。**TRANSPARENCY:**政府有义务向公众提供足够的信息，以便公众能够了解其监视活动的范围和性质。政府一般不应阻止服务提供商公布他们自己与国家进行的与监视有关的交易的范围和性质的细节。

公共监督:各国应建立独立的监督机制，以确保通信监控的透明度和问责制。监督机制应有权获取有关国家行动的所有可能相关的信息。

通信和系统的完整性:不应强迫服务提供商或硬件或软件供应商在其系统中建立监视能力或后门，或收集或保留纯粹用于国家监视目的的特定信息。

国际合作的SAFEGUARDS:有时，国家可能会寻求外国服务提供者的帮助来进行监视。这必须由明确和公开的协议来管理，以确保在每个情况下都依赖最适用的隐私保护标准。**防止非法访问的SAFEGUARDS:**应对非法电子监视的任何责任方施加民事和刑事处罚，受监视影响的人必须能够利用必要的法律机制进行有效补救。对揭露威胁人权的监视活动的举报人也应给予强有力的保护。

我主要针对的是美国，尽管本章中的建议适用于其他地方。在美国，总统可以通过行政命令单方面实施其中一些建议，有些建议需要国会批准，还有一些建议需要通过新的立法。其他国家有自己的三权分立和自己的规则。当然，在许多国家，实施上述任何一项建议都需要政府进行彻底变革。

少一些保密，多一些TRANSPARENCY

自9/11事件以来，布什和奥巴马政府一再坚持认为，为了防止敌人知道我们在做什么，极端的保密是必要的。我们在第一次世界大战期间看到的保密水平仍然有道理。战术事实在有限的时间内可能非常有价值，在那段时间内保密也很重要。有时我们需要保守更大的秘密:我们与其他国家的谈判立场、外国特工的身份、军事规划，以及国家情报的某些领域。回到间谍和监视的重要区别上来，我们的间谍系统比我们的监视系统需要更多的保密性。

然而，我们在很多领域可以做到更加透明。将围绕国安局监控的高度保密与一个非常相似的领域进行比较，在这个领域，我们通常管理得相当好，没有太多的保密:警察和打击犯罪。第四修正案规定了警察进行监视的能力，所有与此相关的法院裁决都是公开的。犯罪分子可以阅读所有这些内容，或者聘请了解这些内容的律师，然后制作一份详细的手册，说明如何精确地利用法律漏洞。法律上有很多漏洞，也有很多知道如何钻这些漏洞的辩护律师。然而，警方的工作仍在继续，罪犯经常被逮捕和定罪。

更普遍的是，几乎所有关于警察和打击犯罪的事情都是公开的。我们知道我们国家所有警察部队的预算。我们了解他们的能力。我们知道他们有多有效。我们知道他们在做什么，以及他们做得有多好。我们不知道便衣警察的身份，但我们大致知道他们是如何被利用的，他们能做什么，不能做什么。所有这些都是公开的，我们这些授予警察权力的人以及我们这些想要犯罪的人都知道。然而，警察经常设法破案。

这表明，我们目前在反恐方面的保密程度过高。它将军事级别的保密应用于一直以来的国内事务。恐怖分子并不比有组织犯罪更聪明、更可怕。恐怖分子不会造成更大的破坏，也不会杀死更多的人;我们只是更害怕他们。我们需要将传统的执法透明原则转移到国家安全上，而不是像我们不幸开始做的那样，增加执法的保密性。我们必须设计出能够保证我们安全的系统，即使他们的细节是公开的，被敌人知道。如今，秘密更难保守，所以我们最好限制它们的数量。

在20世纪80年代，美国放弃了对密码学研究保密的尝试，因为这样做只会让我们的数学家和工程师相对于其他国家的同行处于不利地位。最近，美国放弃了阻止制造生物病毒研究的尝试，因为无论我们做什么，总会有人在某处公布这些信息。军事思想家现在意识到，由于卫星图像和其他技术的无处不在，许多战略军事机密更难保守。我们需要以同样的方式思考围绕监视的政府保密问题。

美国已经有关于监控透明度的法律。1968年最初的窃听法要求对政府使用窃听的情况进行广泛的公开报道。年度窃听报告长达200多页，包含大量细节。这使得人们有可能核实联邦调查局在做什么，并确保该机构没有滥用职权。问题是，当其他监视机构在9/11事件后扩大时，并没有建立类似的报告要求。我们需要解决这个问题。

美国政府应该公布有关情报收集范围和规模的详细、非机密描述。它应该公布所有情报项目的法律依据。它应该公布在这些不同权限下收集的数据的类型和数量，以及最小化程序和数据保留规则的细节。它应该解密外国情报监视法庭的所有一般意见，该法庭根据外国情报监视法和《外国情报监视法修正案》监督NSA的监视活动。被监视的个人和组织的名字是合法保密的;而组织运作的规则则不是。

更多更好的监督

为了控制NSA的监视，我们需要对国家情报和执法部门进行更好的监督。

战略监督是第一位的。NSA以国会的监督为其行为辩护。其领导人声称，该机构的工作人员只是遵循国会通过的法律或总统签署的命令。根据一份官方新闻稿，“NSA的所有活动都是按照适用的法律、法规和政策进行的。”事实并非如此。事实上，这是非常虚伪的。我们从最近解密的外国情报监视法庭的意见，特别是约翰·贝茨法官的意见中得知，NSA经常向法院作出虚假陈述，不遵守最小化要求，并经常超越其法律授权。

NSA玩弄了国会监督的规则，以确保没有实际的理解或关键的审查发生。NSA提供给国会的文件要么是旨在说服国会的宣传材料，要么是旨在混淆视听的术语文件。国会议员不能从存放这些文件的安全房间中移除这些文件，也不能删除他们做的任何笔记。他们只能带着经过安全审查的工作人员来帮助他们理解这些材料的含义和重要性，但很少有议员雇佣既具有绝密审查级别又具有适当专业知识的工作人员。此外，他们还受到NSA的大力游说。参议员罗恩·怀登(Ron Wyden)表示，高级情报官员在国会听证会上多次发表“误导性和欺骗性言论”。参议院情报特别委员会主席、长期支持政府监控的参议员黛安·范斯坦(Dianne Feinstein)遗憾地得出结论，她的委员会“没有得到情报界关于其活动的令人满意的通知”。佛罗里达州国会议员艾伦·格雷森称国会对NSA的监督是一个“笑话”。

2014年，我应六名国会议员的邀请——来自两党的议员——向他们简要介绍了NSA的活动。因为我看过很多斯诺登未公开的文件，所以我比他们更了解NSA的活动。当国会所能得到的关于NSA所作所为的最好信息都来自我的时候，我们的民主制度如何生存?

另一方面，许多立法者不想履行分配给国会的监督职能。这种不情愿部分源于对合理推诿的渴望。让行政部门做决定，然后在出现问题时让它承担责任，在政治上更安全。对抗执法部门也存在政治风险。很少有国会委员会成员真正冒险进入那个安全的房间。

NSA对其权力的解释非常咄咄逼人，而且非常自私。在第五章中，我讨论了NSA用来为其监视活动辩护的三种不同的权力:行政命令12333、爱国者法案第215条和外国情报监视修正案第702条。

1981年的总统文件《行政命令12333》授权了NSA的大部分监视活动，这是令人难以置信的宽松。该法案本应主要允许NSA在美国境外进行监视，但它赋予了该机构收集美国人数据的广泛权力。它对在美国境外收集的美国人数据提供的保护微乎其微，对数亿无辜的非美国人的数据保护就更少了

偶然收集的数据。因为这是总统指令而不是法律，法院没有管辖权，国会的监督也很少。此外，至少在2007年，总统认为他可以随意和秘密地修改或忽略它。因此，我们对NSA内部如何解读行政命令12333知之甚少。

《爱国者法案》(PATRIOT Act)第215条从未打算授权进行大规模监视，而且可以提出强有力的论点，认为该法案的措辞不允许这样做。当时的想法是，FBI将能够从比以前更广泛的来源获得“与授权的(国家安全)调查相关”的信息——即关于特定调查主题的信息。政府提到的例子是，嫌疑人从图书馆借了什么书;也许他在读*《无政府主义者的食谱》*之类的书。事实上，当该法案被辩论时，它被称为“图书馆条款”。它只授权FBI要求获得它可以通过大陪审团传票获得的信息——所有元数据，没有内容——但它允许它在不召集大陪审团的情况下这样做。这是有道理的;在国家安全调查中并没有真正的大陪审团。

然而，在2001年《爱国者法案》通过后，司法部的国家安全律师梳理了这部法律，寻找漏洞。尽管该法的本意是为了方便有针对性的监控，但他们认为，该法可以延伸为授权进行大规模监控。尽管它只授权了FBI，但他们决定FBI可以要求将信息发送给NSA。起初，他们这样做根本没有得到任何法院的批准。最终，他们决定在秘密的外国情报监视法庭上为自己的案子辩护。因为没有人持反对立场，所以他们能够说服法官，*一切都*与调查“相关”。这是对“相关”一词的一种新的解读，甚至连嗅探测试都没通过。如果“相关”并不因为一切都是相关而限制收集，那么当初为什么要把限制写进法律呢?即使是国会议员吉姆·森森布伦纳，美国爱国者法案的起草人，当他得知NSA用它作为收集大量美国人监控数据的合法正当化时，也感到惊讶。他说:“这就像舀起整个海洋来保证你能抓到一条鱼。”

《外国情报监视修正案》第702条略有不同。该条款本应解决一个非常具体的问题。政府官员会绘制图表:沙特阿拉伯的一名恐怖分子与古巴的一名恐怖分子交谈，数据流经美国，但NSA必须在美国境外进行窃听。它辩称，这是低效的，而第702条允许它从美国境内的监听中获取那段对话。

同样，第702条中没有任何内容授权大规模监视。NSA通过滥用“偶然”这个词来为使用这个词辩护。一切都被拦截，包括元数据和内容，并自动搜索感兴趣的项目。NSA声称，只有它想要保存的东西才算搜索。其他一切都是偶然的，只要它的预定“目标”不在美国，就没关系。一个有用的类比是，允许警察在没有任何合理理由或搜查令的情况下搜查城市里的每一所房子，寻找一个通常住在保加利亚的人。他们会保存他们碰巧发现的任何犯罪证据，然后争辩说其他搜查都不算数

因为他们什么也没找到，而他们找到的东西可以作为证据，因为这是寻找保加利亚人的“偶然”。第四修正案明确禁止这种不合理的搜查，而且有充分的理由。

我的猜测是，到2008年《FISA修正案》出台时，NSA知道自己在做什么，并故意对法案进行措辞修改，以允许自己喜欢的解释。它的领导层甚至可能已经向参议院和众议院情报委员会简要介绍了它将如何解释这些语言。但他们肯定没有向全体国会通报情况，也从未告诉过美国人民。

我相信，其中很大一部分最终会被发现是违宪的。第四修正案不仅保护不受不合理的搜查，也保护不受不合理的扣押。我在第10章中指出，电脑搜查也是搜查。仅仅从威瑞森(Verizon)等公司获得大量数据副本的行为也是一种非法扣押。

问题在于，这三个政府部门都放弃了自己的监督职责。制定一项法律，把它变成规则，然后把这些规则变成程序，这种正常的民主过程，每一步都是可以解释的，因此每一步都需要监督。没有监督，机构就会滥用权力。我们在20世纪70年代看到了这一点，当时联邦调查局和NSA在三叶草和尖塔项目下非法监视美国人，以及在一个不知名的项目下，这是禁毒战争的一部分。今天，我们又看到了这种情况。

为了避免你认为这只是美国的现象，2000年UK通过《调查权力监管法案》(Regulation of Investigatory Powers Act)时也发生过同样的事情。该法案在辩论时基本未被注意到的第16(3)条，已被GCHQ用来监视英国公民。它是故意这样起草的，一些国会议员也参与其中，顽固地为这种晦涩难懂的语言辩护，这种语言实际上并没有使大规模监视合法化，但最终却被用来为其辩护。我相信FAA第702条的想法来自RIPA第16(3)条。

2013年，奥巴马总统试图让美国人放心，NSA的监控项目是由政府所有三个部门审查和批准的。他的声明严重误导了民众。在斯诺登之前，政府的全部监视活动只有少数行政部门的成员知道，部分披露给了立法部门的几名高级成员，并得到了FISA法庭(FISA court)一名法官的批准。1979年至2013年，该法院在3.4万份搜查令申请中，只驳回了11份。这并不是真正的监督。然而，公平地说，它比你在其他国家，包括法国、德国和UK等欧洲民主国家发现的监督要多得多。

一些国会议员正试图对NSA施加限制，他们的一些建议具有实际效力，可能会有所作为。即便如此，我现在对有意义的国会改革也不抱任何希望，因为所有的提案都集中在具体的项目和权力上:第215条下的电话元数据收集项目，第702条下的批量记录收集，等等。这是一种零敲碎打的方法，行不通。我们现在已经超越了简单的法律干预可以产生

改变。有太多的秘密，太多的项目在不同的法律理由之间转移。当公司拒绝国家安全信函时，政府会以第215条的命令回来。NSA一再威胁说，如果国会根据第215条和第702条限制它的权力，它将把被削减的项目转移到更宽松、监管更少、更保密的《行政命令》12333号授权上。

还有其他监管方面的尝试。总统2013年成立的NSA审查小组对该机构的能力和活动有广泛的了解。他们提出了一份出色的报告，概述了46项政策建议，奥巴马总统同意实施其中的许多建议。现在的关键问题是他是否会这样做。2004年，国会根据9/11委员会的建议成立了隐私和公民自由监督委员会，负责监督国家安全问题。该委员会在2012年之前基本没有人员和资金，权力有限。(该组织2014年的报告只讨论了NSA根据第702条收集的信息。该报告被普遍批评为不充分。)

更多的国会议员必须承诺对NSA进行有意义的改革。我们需要独立的政府机构在完全透明的基础上进行全面的战略监督。我们需要有意义的规则来最大限度地减少收集和存储的关于美国人的数据，这些规则要求NSA删除它不应该访问的数据。在20世纪70年代，丘奇委员会调查了NSA、中央情报局和FBI的情报收集。经过广泛的研究和发现，它才能够改革这些机构。我们现在需要一个类似的委员会。我们需要说服奥巴马总统采纳他自己的NSA审查小组的建议。我们需要赋予隐私和公民自由监督委员会真正的调查权。

这些建议都与大规模监控的战略监督有关。接下来，让我们考虑战术监督。对政府监视进行战术监督的一个主要机制是搜查令程序。与许多政府官员的说法相反，搜查令并不会损害安全。它们是一种安全机制，旨在保护我们免受政府越权的侵害。

秘密搜查令的效果就差远了。监督NSA行动的法官来自秘密的FISA法庭。与传统法院相比，FISA法庭在签发搜查令之前的证据标准要低得多。它的案件是秘密的，它的裁决是秘密的，从来没有另一方的人在它面前出庭。考虑到这个过程是多么不平衡，令人惊讶的是，FISA法庭在与NSA对抗时表现出了同样的骨气(尽管几乎从未拒绝过搜查令请求)。

有些监视令完全绕过了这一程序。例如，我们知道，2012年US Cellular只收到了两份司法批准的窃听令，而在没有任何司法监督的情况下，还收到了10801份针对相同类型信息的传票。所有这些问题都需要解决。

先从FISA法庭说起。它应该更加公开。FISA法庭的首席法官应该成为一个需要参议院批准的职位。该法院应尽可能公布其意见。一个官方的公共利益倡导者应该被指派反对监视申请的任务。国会应该制定一个对FISA裁决提起上诉的程序，要么向上诉法院上诉，要么向最高法院上诉

最高法院。

但需要采取更多措施，将NSA置于可信的战术监督之下。它的内部程序更适合于发现无意和不正确的监视目标等活动，而不是发现故意规避监视控制的人，无论是个人还是整个组织。为了纠正这一点，外部审计员是必不可少的。让政府官员亲自为越权和违法行为负责也很重要。没有一个NSA的间谍被解雇，更不用说被起诉了。当斯诺登试图在内部表达他对NSA对美国人的监控程度的担忧时，他一再遭到拒绝。

其他执法机构，如FBI，也有自己的内部监督机制。在这方面也是一样，透明度越高越好。我们一直赋予警方调查犯罪的非凡权力。我们在知情的情况下这样做，我们作为一个社会也因此更安全，因为我们规范了这些行为，并有一些追索权来确保警察不会滥用这些权力。我们可以争论这些在美国和其他国家的运作情况如何，但总的想法是合理的。

保护举报人

哥伦比亚大学法学教授David Pozen认为，民主需要有漏洞——漏洞和举报本身就是防止政府越权的安全机制。在他看来，泄密是对过度保密趋势的一种对抗，最终是政府赢回因过度保密而失去的信任的一种方式。

民族学家丹娜·博伊德(danah boyd)将告密称为信息时代的非暴力反抗;它使个人能够反击权势者的虐待。非政府组织人权观察(Human Rights Watch)写道，“那些揭露官方不法行为的人……在民主社会中发挥了重要作用... .”

在这种思维方式下，举报人提供了另一种监督机制。你可以把他们看作是一次随机的突击检查。正如我们有保护企业举报人的法律一样，我们也需要保护政府举报人的法律。一旦这些法律到位，我们就可以为合法的举报人建立一个框架和规则。

这并不意味着任何人都可以通过声称自己是举报人来自由泄露政府机密。这只是意味着，出于良心而披露政府的不法行为将是一个有效的辩护，泄密者可以在法庭上使用——陪审团将不得不决定这是否合理——而记者将在法律上能够对他们的消息来源保密。这样做的聪明之处在于，它回避了定义“举报人”的难题，并允许法院根据具体情况来决定某人的行为是否符合举报人的资格。像斯诺登这样的人将被允许返回美国，并在法庭上陈述他的案件，正如我在第七章中解释的那样，目前他不能这样做。

此外，我们需要法律来保护获得机密信息的记者

信息。公开披露本身并不是间谍活动，将新闻视为犯罪对民主极为有害。

在第7章中，我提到了奥巴马政府对举报人的过度起诉。这一政策既虚伪又危险。我们鼓励个人举报私营企业的违法行为;我们也需要保护政府内部的检举行为。

目标范围要更小，而且必须得到司法部门的批准

电子监控是执法和情报收集的宝贵工具，也是我们应该继续使用的工具。问题是对整个人口的电子监控，尤其是在狭窄的法院命令之外进行的大规模监控。正如我们在第11章看到的那样，它并没有让我们更安全。事实上，它把资源和注意力从真正让我们更安全的事情上转移开，让我们更不安全。解决的办法是限制数据收集，回到有针对性的——而且只有针对性的——监控。

网络安全和信息法律研究员阿克塞尔·安巴克(Axel Arnbak)谈到政府监控时说:“前门受法律管辖;后门由博弈论管理。”他的意思是，有针对性的监视过程受制于合理的理由、授权、范围限制以及其他旨在保护我们的安全和隐私的法律。大规模监控受制于一个组织的冷静分析，即它可以收集什么，以及它逃脱惩罚的可能性有多大。当我们赋予NSA逃避搜查令程序进行大规模监视的能力时，我们就允许NSA的工作人员更多地考虑什么是可能的，而不是什么是合法的。我们让他们变得傲慢和贪婪，我们为此付出了代价。

大规模监控颠覆了传统的调查过程。在正常的行动顺序下，执法部门有理由怀疑一个人，并申请搜查令来监视那个人。大规模监视允许执法部门监视每个人——以形成怀疑的理由。这是美国宪法明文禁止的，而且是有充分理由的。这就是为什么2014年联合国的一份报告得出结论，大规模监控威胁到国际法。

我们需要立法来迫使情报机构和执法部门有针对性地进行监视:包括新的立法和现有立法的新执行。这种结合将只给执法部门提供所需的信息，并防止滥用。

2013年，美国最高法院在这个方向上迈出了一小步，要求警察在嫌疑人的车上安装GPS跟踪设备之前必须获得搜查令，2014年又要求警察在搜查他们拦下或逮捕的人的手机之前必须获得搜查令。

在美国，我们需要推翻过时的第三方原则，并认识到即使我们将信息委托给在线服务提供商，信息仍然可以是私人的。警察应该需要一份搜查令才能查看我的邮件，无论是我家里的纸质邮件、我工作的电脑上的邮件，还是b谷歌在世界某个地方的服务器上的邮件。

其中许多问题是国际性的。要做到这一点，就意味着要认识到政府不仅有义务保护本国公民的权利和自由，而且有义务保护世界上每一位公民的权利和自由。这是新的;美国针对监控的法律保护不适用于美国境外的非美国公民。国际协议需要承认，一个国家的义务并不完全止于其边境。为什么我们应该这样做，有基本的道德理由，但也有务实的理由。保护外国人的隐私权有助于保护我们自己的隐私权，而第9章讨论的经济危害源于践踏这些隐私权。

修复几乎所有的漏洞

正如我在第11章中所讨论的，一场关于美国政府——特别是NSA和美国网络司令部——是应该储存互联网漏洞，还是应该披露并修复它们的辩论正在进行。这是一个复杂的问题，它赤裸裸地说明了在网络空间中区分攻击和防御的困难。

网络空间军备竞赛正如火如荼地进行着。中国、俄罗斯和许多其他国家也在囤积漏洞。如果我们不修补一个漏洞，我们就有可能被另一个国家独立发现，并将其用于针对我们和我们的盟友的网络武器。但如果我们修补我们发现的所有漏洞，我们的武器库就会消失。

一些人认为，NSA应该披露并修复它发现的每一个漏洞。另一些人则声称，这相当于单方面裁军。奥巴马总统的NSA审查小组建议采取中间立场:只有在极少数情况下，才能在短时间内囤积漏洞。这一点我自己也说过。这就是NSA，延伸到美国网络司令部，声称它正在做的事情:平衡几个因素，比如是否有其他人可能发现这个漏洞——还记得第11章的NOBUS吧——以及它对美国的战略意义。然而，有证据表明，它囤积的信息远比它公开的要多。

这是一种倒退。我们不得不在披露方面犯错。这将特别有利于那些严重依赖互联网基础设施的国家，比如美国。它将通过展示我们将安全置于监视之上来恢复信任。虽然储存的漏洞需要保密，但我们越能公开决定储存什么样的漏洞的过程，就越好。要正确地做到这一点，我们需要一个具有适当技术专长的独立政府组织来做决定。

在当今的网络战军备竞赛中，世界各国军队在寻找和购买漏洞方面投入的资金，超过了商业世界在修复漏洞方面投入的资金。它们的库存影响着我们所有人的安全。无论网络犯罪分子做什么，无论其他国家做什么，我们美国人都需要在安全方面犯错，修复我们发现的几乎所有漏洞，并使披露过程更加公开。这将使我们更安全，同时使人们对美国的政策和互联网的技术基础产生信任。

不要颠覆产品或标准

信任对社会至关重要。它是个人的、相对的、情境的、流动的。它支撑着我们作为一个物种所完成的一切。我们必须能够彼此信任，我们的机构——包括政府和企业——以及使社会运转的技术系统。当我们建立系统时，我们需要确保它们既值得信赖又有效。

互联网信任的确切性质很有趣。我们这些技术人员从来没有幻想过互联网是安全的，也没有幻想过政府、罪犯、黑客和其他人如果有足够的技术和动机就无法闯入系统和网络。我们从不相信程序员是完美的，代码是没有错误的，甚至我们的加密数学是牢不可破的。我们知道，互联网安全是一场军备竞赛，攻击者占据了大部分优势。

我们所相信的是，这些技术将取决于它们自己的优点。由于斯诺登的爆料，我们现在知道这种信任是错误的。这就是为什么NSA和GCHQ的监视项目在世界范围内引起如此强烈的抗议，也是为什么技术社区对NSA对互联网产品、协议和标准的颠覆尤其愤怒。这些机构的行为削弱了世界对互联网背后技术的信任。

我在第6章中讨论过，FBI一直在试图通过法律，强制要求后门进入安全系统。我在第11章中讨论了NSA如何秘密地在互联网产品和协议中插入后门，以便进行间谍活动。我们还必须假设，其他国家也一直在对自己的产品(以及彼此的产品)做同样的事情。不少观察人士得出的结论是，拥有以色列开发团队的公司，如Verint、narendra、Amdocs等，与以色列政府勾结，华为的设备是中国政府的后门。我们信任中国制造的美国产品吗?我们信任在微软工作的以色列人吗?还是俄罗斯的硬件和软件?法国?德国?任何地方的东西?

这种不信任是毒药。安全要放在第一位，窃听要放在第二位。执法部门可以获得搜查令并尝试窃听，但不应该强迫通信公司保证窃听尝试会成功。我们真正需要做的是废除CALEA，重新回到保护电话网络和互联网安全的事业中来。

执法人员对此的反应是试图用绑架者、恋童癖者、毒贩和恐怖分子逍遥法外的幻想来吓唬我们，因为他们无法解密他们的电脑和通信。我们在2014年底看到了这一点，当时苹果公司最终加密了iPhone的数据;执法人员一个接一个地提出了绑架和儿童掠夺者的幽灵。这是一种常见的危言耸听的说法，但没有人指出任何实际案例中这是一个问题。2013年，在3576起被授权进行通讯拦截的重大犯罪中，只有一起涉及绑架，而且受害者不是儿童。更重要的是，没有证据表明加密会以任何严重的方式阻碍刑事调查。2013年，加密失败了

警方破获了9次，高于2012年的4次，而且调查以其他方式进行。

执法机构拥有大量可供使用的调查工具。他们可以获得存储在云中的数据和大量元数据的搜查令。他们有权利和能力渗透目标嫌疑人的计算机，这可以在不削弱每个人的安全性的情况下为他们提供所需的数据。良好的安全性并不会让我们处于危险之中。

无论是公开还是秘密，我们的情报机构都不应该故意在外国专门的军事和政府系统之外的任何东西中插入漏洞;他们应该与学术界和商界合作，确保更多敌对方插入的任何漏洞都能被发现、揭露和消除。

我们永远无法让世界上的每一个大国都同意不颠覆它所控制的互联网部分，但我们可以停止颠覆我们所控制的部分。大多数让互联网运转的高科技公司都位于美国，所以我们的影响力不成比例。一旦我们停止玩颠覆游戏，我们就可以可靠地将我们的资源用于检测和防止他人的颠覆行为——从而增加全世界的信任。

将间谍活动与监视活动分开

2013年，我们得知NSA窃听了德国总理安格拉·默克尔的手机。我们了解到，NSA对世界各地的大使馆和使团进行了监视: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、斯洛伐克、南非、韩国、台湾、委内瑞拉和越南。我们了解到NSA在监视联合国。自然，这些爆料使国际关系紧张，但真的有人感到惊讶吗?监视外国政府是NSA应该做的。

政府间的间谍活动和政府本身一样古老。这是一项重要的军事任务，无论在和平时期还是战争时期，它都不会消失。它是有针对性的。它是专注的。它实际上是稳定的，减少了各国对彼此意图的不确定性。

无论是在美国还是在国际上，间谍活动都与NSA的大规模监视项目有着根本的不同。在第五章中，我指出，NSA活动的这种转变是其使命转向预防恐怖主义的结果。9/11之后，反恐监视的主要任务被交给了NSA，因为它拥有可以轻易改变用途的现有能力，尽管这项任务本来可以交给FBI。

由于NSA被赋予了反恐监视任务，其间谍活动的军事规范和法律框架得以延续。我们对全体人民(包括我们自己的国民)的监视行动就像我们对政府的间谍活动一样保密。

我们需要把这两项任务分开。政府间谍活动应该留在

国务院和军方的职权范围作为三军统帅，总统应该决定窃听哪些大使馆和谁的手机，而NSA应该执行这些命令。大规模监视，无论是国内的还是国外的，几乎从来都是不合理的。政府对普通公民的监视有时是正当的，但只是作为刑事调查活动。这些监视活动不应该局限于NSA和军方。相反，他们应该在FBI和司法部的支持下，在常规的公开法庭上应用警方关于合理原因、正当程序和监督监视活动的规则。

这并不是说我们不需要在美国进行重大的警察改革。我们已经在第七章讨论过警察保密问题。警察日益军事化和许多部门倾向于种族歧视的做法也是严重的问题。但这是另一本书的话题了。反恐怖主义过去是，现在仍然是FBI的主要任务。

2014年1月，奥巴马总统就NSA发表了一次演讲，其中他提出了两点非常重要的观点。他承诺，NSA将不再监听安格拉·默克尔的手机。虽然他没有将这种礼貌扩展到其他8200万德国公民，但他确实表示，他将把美国宪法对未经授权的监视的一些保护扩展到世界其他地方。将政府对人口的监视置于平民领导和警察规则之下，将大大有助于实现这一理想。

限制军方在网络空间的角色

19世纪后期的一项伟大的政治成就是文官政府与军队的分离。历史和当前的政治都表明，当将军掌管一个国家时，会产生巨大的社会损害。正如世界上许多自由民主国家所做的那样，将两者分开，为自由和民主的蓬勃发展提供了空间。

问题在于，网络空间并不容易被传统的划分为民用和军事领域。当你受到人身攻击时，你可以呼吁各种组织为你辩护:警察、军队、在你的国家负责反恐安全的人、你的律师。辩护的法律制度取决于两件事:谁在攻击你，为什么要攻击你。不幸的是，当你在网络空间受到攻击时，有两件事你不知道，那就是谁在攻击你，为什么要攻击你。

此外，互联网没有与现实世界相比的边界——你可以说它根本没有边界——因此，国外和国内之间的区别就更难适用了。攻击者的范围可以从无聊的青少年到职业罪犯再到民族国家，也许使用相同的战术和武器，所以很难确定攻击者类型之间的区别。攻击发生在几毫秒内，可能会产生广泛的影响。

很容易的反应是把所有这些未知的攻击都归为

“网络战争”，这是军事规划中的热门新事物。我已经提到，大约有30个国家在军队中设有网络战部门。“网络围攻”的心态正在成为新的常态。

考虑到这个战场是如此的新鲜和未知，考虑到一切都发生得如此之快，考虑到军方默认的信仰是其使命的正义性，无论它是如何构建的，军队往往会匆忙进入，填补他们认为的安全空白。相应的危险是人们感知我们有军事问题，需要军事解决办法。这些问题最坏的情况往往是极权主义，最好的情况是法外解决。

我们需要解决这个问题。

在美国，一系列法律阻止军队在正常和平时期的国内事务中发挥作用，同时确保他们准备好应对外国威胁。1878年的《军务委员会法》(Posse Comitatus Act)和其他指令禁止军队参与国内安全事务。因为我们把军队的作用限制在对外国列强发动战争，所以我们有信心允许它有更大的行动自由度。例如，适用于执法部门的正常搜查和扣押规则不适用于军队，因为这样的规则在战争中就是没有意义。

网络空间的进攻性军事行动，无论是间谍活动还是攻击，都应该留在军方的职权范围内。在美国，这是网络司令部。如果我们要攻击另一个国家的电子基础设施，我们应该像对待其他对外国的攻击一样对待它。不是简单的间谍活动(网络或现实世界)，而是作为一种攻击。此类行动应被视为进攻性军事行动，相应得到行政部门最高层的批准，并应遵守与管理线下世界战争行为相同的国际法标准。

解散NSA

我刚刚提议将NSA的间谍任务与其监视任务分开，并将军方在网络空间中的角色限制在针对外国军事目标的行动上。为了实现这一目标，我主张拆分NSA，恢复和加强9/11之前存在的各种机构的职责:

- 作为国防部的一部分，NSA应该专注于针对外国政府的间谍活动。
- 司法部应该负责执法和恐怖主义调查。为此，它应该只进行有针对性的、法律允许的国内和国外监视活动，并且应该根据联邦调查局特工的专业知识而不是NSA的数据库来追查线索。
- NSA在密码学、计算机安全和网络防御方面的防御能力应该剥离出来，变得更加突出和公开。美国国家标准与技术研究院(NIST)是美国国防部之外的一个民间机构，它应该重申对网络安全技术标准开发的控制。1987年的《计算机安全法》明确规定nist(当时称为国家标准局)在建立技术安全标准方面具有领导地位，试图将NSA排除在国内安全事务之外。我们需要加强这项法律并确保它得到遵守。
- 美国的进攻性网络能力应保留在美国网络司令部手中。这个组织应该包括NSA的黑客能力(也就是TAO)。负责美国网络司令部的将军不应该兼任NSA局长。

这是一个长远的计划，但却是正确的计划。与此同时，我们应该把NSA的资金削减到9/11之前的水平。这本身就会带来巨大的好处。

打击网络主权运动

20年前，几乎没有政府出台任何监管互联网的政策。今天，每个国家都有，其中一些还相当严厉。这并不奇怪;互联网变得太大了，政府无法忽视。但这种变化让许多互联网观察人士感到意外，并将继续如此。

越来越多的世界各国政府正在与互联网固有的国际性作斗争。如果一个政权想要监视其人民，限制他们可以阅读的内容，审查他们可以发表的言论，那么互联网的国际自由和开放性质就会出现问题。

出于这个原因，俄罗斯、中国和沙特阿拉伯等国多年来一直在推动对国内互联网进行更多的国家控制。通过国际电信联盟这样的国际组织——这是联合国控制电话标准的机构——他们正试图从目前掌管互联网的更非正式的多方利益相关者国际组织手中夺取对互联网的控制权。他们的论点听起来是善意的，但他们的动机并非如此。他们想要一个既承认国家边界，又承认政府在这些边界内施加控制的权利的互联网:在这种情况下，这会导致更多的监视和审查。

美国国家安全局(NSA)监控活动的曝光，极大地推动了这一地位。一些国家的政府反对美国在互联网上的主导地位，因为他们担心本国公民的隐私。巴西和德国等国呼吁将更多公民数据存储在本国境内。持相反议程的其他国家也利用了同样的说辞。2014年，俄罗斯通过了一项法律，要求在线企业在俄罗斯境内存储公民的数据，这超出了NSA的范围，但俄罗斯政府很容易就能得到。

对此，我持有不同的观点。一方面，我希望拥有更严格隐私法的国家通过要求公民数据受其管辖来保护公民数据。另一方面，我不认为这将保护这些数据免受NSA的监视。至少NSA对其在美国境内可以访问的内容有一些限制。如果同样的数据存储在巴西和德国的服务器上，这些法律限制就不适用了。鉴于我们对NSA技术能力的了解，我毫不怀疑该机构无论如何都会获得访问权限。

互联网本质上的国际性，对生活在实行监视和审查制度的国家的人们来说是一个巨大的好处。网络主权往往是政治领导人在不受外国政府或公司干涉的情况下监视和控制其公民的愿望的烟幕。而反对网络主权的斗争通常被视为NSA获取更多全球通信信息的烟幕。我们需要重申我们对自由、开放和全球互联网的支持，然后努力确保其继续存在。

为共享资源提供保障

无主公共空间具有巨大的社会价值。我们的公园，我们的人行道，我们的道路不属于任何私人企业，我们的法律反映了这种公共所有权。在互联网上，所有的东西都属于私人实体;就连你朋友独立运营的那个网站，也托管在某个地方的某个企业服务器上。没有公地。

我们并不这样看待我们的在线体验。在脸书上聊天感觉就像面对面聊天一样，当该公司行使删除帖子和封杀用户的权利时，我们感到很惊讶。当我们得知自己无权上诉——甚至无权对自己的数据上诉时，我们就更惊讶了。是的，当我们点击最终用户许可协议时，我们同意交出所有这些权利。但因为我们没有阅读它，所以我们没有意识到这一点。

公共空间的概念很重要，因为我们在线下世界的很多自由都是基于这个概念。在美国，第一修正案保护公共场所的言论自由。其他法律限制公共场所醉酒和猥亵等行为。这些法律不适用于互联网，因为那里的一切都是私人空间。这些法律不适用于我们在脸书、推特、Instagram或媒体上发表的言论，也不适用于我们在新闻网站上发表的评论，即使这些评论是公开可读的。

在互联网诞生之初，公共讨论论坛是在一个叫做Usenet的地方进行的。这是一个去中心化的系统，没有一家公司可以控制谁能说话，谁能说什么。随着讨论论坛转移到网站和企业自有平台，这种自由消失了。

我们需要互联网上不受私人党派控制的地方——说话的地方、交谈的地方、集会的地方、抗议的地方。它们可以是政府管理的，也可以是企业管理的，并有特殊的规则将它们视为真正的公共场所。类似于电信公司不允许区别对待不同类型的流量的公共运营商规则，可能存在公共运营商不允许其所有者监控或审查的社交网络领域。

无论解决方案是什么，公共网络对社会都至关重要。我们应该有意识地努力确保我们在网络空间中始终拥有它们。

14

企业解决方案

当我们从企业数据收集、监控和使用中寻找限制的好处时，重要的是要记住，数据收集给我们带来了许多我们都能获得的好处和便利，这是以前不可能的:基于实际拥堵数据的实时驾驶方向，记得我们上次买了什么的购物清单，即使你没有保存收据也能获得商店退款的能力，远程验证你关了灯和锁了门的能力，与世界上任何地方的任何人即时通信的能力。未来还会有更多的应用。看看任何科幻电影或电视节目，关注一下完全电脑化的世界的奇迹;其中很大程度上假定计算机知道、响应并记住人们在做什么。这种监视就是我们的未来，这个未来充满了让我们的生活更美好、更愉快的东西。

同样，不受限制地获取技术也是有价值的。虽然这本书的大部分内容都集中在技术的阴暗面上，但我们必须记住，技术给我们所有人带来了巨大的好处。技术使我们能够更快、更容易、更准确地完成复杂的任务，其目的有很多:开发更耐用的建筑材料;发现和传播信息;精确描绘物理现象;不受地域限制地与他人交流;记录事件;种植更多的粮食;活得更久。如果没有互联网，我不可能写出这本书。当然，它并不完美。技术在地球上的分布是不均匀的，有富人也有穷人，但总的来说，技术越多越好。

我们最不愿意做的就是让这样的未来脱轨。我们根本不知道未来会出现什么样的发明，也不知道它们将能够解决哪些主要的人类问题。我们需要能够试验新技术和基于这些技术的新业务，这包括监控技术。诀窍在于将公司收集、存储和分析我们的数据所带来的好处最大化，同时将危害降到最低。

有很多解决方案可供考虑。1980年的经合组织隐私框架是一个很好的起点;它列出了数据收集、数据存储和数据使用方面的限制。1995年，欧盟通过了《欧盟数据保护指令》，对企业收集的个人数据进行了规范。习惯了美国宽松得多的法律制度的美国企业，不断与欧洲法律发生冲突。目前正在讨论如何进行改革，使欧洲法律与现代技术保持同步。

本章提供的解决方案都是针对私人收集和使用我们的数据。这些变化有时会受到市场的刺激，但大多数时候会受到法律的推动。这确实是政府需要做的事情的清单，这在

Turn实际上是公民需要要求政府做的事情的清单。因为它们影响公司，所以它们在这一章中。

让供应商对隐私泄露负责

提高收集数据安全性的一种方法是让公司对数据泄露负责。

企业在不断平衡成本和收益。在这种情况下，成本包括保护他们收集和保存的数据的成本，如果出现违规的不安全成本，以及他们收集的数据的价值。目前，不安全的成本很低。除了一些非常公开的违规行为——比如塔吉特(target)——企业发现，把钱花在宣传良好安全性的公关活动上，在被证明是错误的情况下经受住偶尔的媒体风暴和一轮又一轮的诉讼，并在问题公开后修复问题，成本更低。

OECD Privacy Framework (1980)

COLLECTION LIMITATION PRINCIPLE: There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

DATA QUALITY PRINCIPLE: Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

PURPOSE SPECIFICATION PRINCIPLE: The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

USE LIMITATION PRINCIPLE: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except: a) with the consent of the data subject; or b) by the authority of law.

SECURITY SAFEGUARDS PRINCIPLE: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

OPENNESS PRINCIPLE: There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

INDIVIDUAL PARTICIPATION PRINCIPLE: Individuals should have the right: a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to them; b) to have communicated to them, data relating to them i. within a reasonable time; ii. at a charge, if any, that is not excessive; iii. in a reasonable manner; and iv. in a form that is readily intelligible to them; c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and d) to challenge data relating to them and, if the challenge is successful to have the data erased, rectified, completed or amended.

ACCOUNTABILITY PRINCIPLE: A data controller should be accountable for complying with measures which give effect to the principles stated above.

This is because most of the cost of privacy breaches falls on the people whose data is exposed. In economics, this is known as an externality: an effect of a decision not borne by the decision maker. Externalities limit the incentive for companies to improve their

安全。

你可能期望用户的反应是更喜欢安全的服务，而不是不安全的服务——毕竟，他们是在相同的市场模式的基础上做出自己的购买决定的。但这通常是不可能的。在某些情况下，软件垄断限制了可用产品的选择。在其他情况下，专有文件格式、现有基础设施、兼容性要求或软件即服务所产生的“锁定效应”使得转换变得更加困难。在很多情况下，我们不知道是谁在收集我们的数据;回想一下第二章中关于隐藏监视的讨论。在所有情况下，买家都很难评估任何数据服务的安全性。而且，不只是非技术买家;甚至我也不能告诉你是否应该把你的隐私委托给任何特定的服务提供商。

责任改变了这一点。通过提高隐私泄露的成本，我们可以让公司接受外部性的成本，并迫使他们花更多的精力来保护那些他们获得数据的人的隐私。我们已经在美国对医疗数据采取了这种做法;该行业的隐私侵犯行为会被处以高额罚款。

在这里，这种情况也开始发生在商店的数据上。塔吉特因2013年的数据泄露事件面临多起诉讼。在其他案件中，银行因未能充分保护客户隐私而被起诉。一种帮助的方法是要求公司告知用户他们所拥有的*所有*可能被泄露的信息。

这些案件可能会很复杂，因为有多家公司卷入了一起特定事件，分摊责任将会很困难。法院一直不愿意找到隐私的价值，因为人们愿意放弃隐私，换取的东西太少了。而且由于很难将隐私丧失带来的伤害与造成这些伤害的具体行为联系起来，这类案件很难胜诉。

有一个更好的方法来解决这个问题:把损害的重点放在隐私泄露上，而不是随之而来的伤害上。必须迫使公司遵守1973年的《公平资讯实务守则》和其他类似的隐私法规，这些法规目前不是强制性的;那么，违规行为就变成了未能遵守法规。

这与美国环保署监管环境污染物的方式类似。工厂有法律义务限制它们排放到环境中的微粒数量。如果他们超过这些限制，他们将受到罚款。没有必要等到癌症病例意外激增时才采取行动。问题是可以理解的，法规已经到位，企业可以决定是建煤炉还是太阳能电池板的工厂，如果他们不遵守本质上最好的做法，制裁就等着他们。这是我们需要走的方向。

美国公平资讯实务守则(1973年)

《公平资讯实务守则》以五项原则为基础:

1. 不得存在保密的个人资料记录系统。
2. 必须有一种方法让一个人知道记录中有关于他的哪些信息，以及这些信息是如何被使用的。

3. 一个人必须有一种方法来防止为一个目的而获得的关于该人的信息在未经该人同意的情况下被用于或用于其他目的。
4. 一个人必须有一种方法来纠正或修改关于他的可识别信息的记录。
5. 任何创建、维护、使用或传播可识别个人数据记录的组织都必须确保数据用于其预期用途的可靠性，并必须采取预防措施防止数据被滥用。

可以肯定的是，使系统更安全需要花钱，如果可能的话，公司会以更高价格的形式将这些成本转嫁给用户。但用户已经在为不安全的系统支付额外的成本:隐私泄露的直接和间接成本。让公司为违规行为承担责任，将这些成本转嫁给了他们，作为副产品，会促使公司提高其安全性。经济学中的相关术语是“最小成本规避者”(least cost avoider):将责任分配给拥有数据的实体在经济上是有效的，因为它处于最大限度降低风险的最佳位置。想想看——如果你想让Facebook更好地保护你的数据，你能做些什么?不多。经济学理论认为，这就是为什么公司应该承担不良安全措施的成本。

规范数据使用

与欧盟不同，在今天的美国，关于你的个人信息不是你的属性;它归收集者所有。法律保护特定类别的个人数据——金融数据、医疗信息、学生数据、录像带租赁记录——但我们没有像欧洲国家那样广泛的隐私保护法律。但广泛的法律保护确实是唯一的解决方案;让市场来解决这个问题，会导致更具侵入性的大规模监控。

举个例子。Dataium是一家跟踪你在网上买车的公司。它会监控你对不同制造商网站的访问:你在看什么类型的车，你点击了哪些选项来获取更多信息，你研究了哪种融资选项，你在任何给定页面上停留了多长时间。经销商为这些关于你的信息付费——不仅仅是关于他们出售的汽车的信息，还有你看的其他制造商出售的汽车。他们为这些信息付费，这样当你走进展厅时，他们就能卖给你一辆更有利可图的车。

想想这里的经济学。当你买车的时候，这些信息可能会让你(大概估计)在最终价格上多花300美元。这意味着它的价值不超过300美元，可以保护你免受Dataium的攻击。但美国每年售出1600万辆汽车。即使你假设Dataium只拥有与其中2%相关的客户信息，这也意味着它对公司来说价值约1亿美元，以确保其策略有效。

这种不对称就是市场解决方案往往失败的原因。这是一个集体行动的问题。保护我们免受Dataium的侵害对我们所有人来说价值1亿美元，但我们不能有效地协调。Dataium自然会把汽车经销商团结在一起，但我们消费者团结起来的最佳方式是通过集体政治行动。

使用点是一个合理的监管点，因为很多信息

我们的信息之所以被收集，是因为我们希望如此。当这些信息被以我们不希望的方式使用时，我们会反对:当它被存储、共享、出售、关联，并以某种隐秘的方式操纵我们时。这意味着我们需要限制我们的数据如何被使用，特别是限制与收集数据的目的不同的方式。

当企业将其底层算法视为商业机密时，就会出现其他问题:谷歌的PageRank算法(它决定了你看到的搜索结果)和信用评分系统就是两个例子。这些公司对保密性的担忧是合理的。他们既担心竞争对手会模仿他们，也担心人们会想出如何利用他们。但我相信，当算法对公众产生直接影响时，透明度比专利主张更重要。与目前相比，更多的算法可以公开——或者重新设计以使它们能够公开。多年来，借贷真相法和公平借贷法要求金融机构确保他们使用的算法既可解释又具有法律上的可辩护性。强制性的透明度需要扩展到算法对人有影响力的其他领域:它们必须是开放的。此外，有一些方法可以在不公开的情况下审计算法的公平性。

企业往往是理性的风险评估者，并且会遵守监管。要做到这一点，关键在于监督和问责。这并不是什么不寻常的事情:在我们的社会中有许多受监管的行业，因为我们知道他们所做的事情既重要又危险。个人信息和用于分析它的算法也没有什么不同。一些定期的审计机制将确保企业遵守规则，如果他们不遵守规则，就会受到惩罚。

这一切在理论上讲得通，但实际上很难做到。我们最不希望看到的，就是政府开始对我们的数据说，“你只能做这个，不能再做别的”。以许可为基础的监管会扼杀技术创新和变革。我们想要基于权利的监管——基本上，“你可以做任何你想做的事，除非它被禁止。”

也要规范数据收集

规范数据使用是不够的。隐私需要在很多地方得到规范:收集时、存储时、使用时、争议时。经合组织隐私框架很好地阐述了它们，它们都是必不可少的。

美国公司多年来一直在努力说服世界，我们不需要对数据收集进行监管，只需要对数据使用进行监管。公司试图消除对数据收集的任何限制，因为他们知道任何使用限制的定义都很狭隘，一旦他们掌握了我们的数据，他们就可以慢慢扩大这些限制。(反对任何特定数据使用监管的一个常见论点是，这是一种审查形式。)他们知道，如果收集限制已经到位，要改变它们就困难得多。但就像政府的大规模监控一样，对隐私的伤害来自于数据的简单收集，而不仅仅是数据的使用。还记得第10章关于算法监控的讨论吗?不受限制的公司收集将导致广泛的收集，与政府的广泛共享，以及缓慢地削弱

必须严格定义使用限制。

我们需要对抗这一运动。数据收集方面的限制并不新鲜。未来的雇主不允许询问求职者是否怀孕。贷款申请也不允许询问申请人的种族。“禁箱”是一项旨在使雇主询问申请人犯罪记录成为违法行为的运动。前美国同性恋军人的妥协方案“不问不说”是对数据收集的限制。美国人口普查局可以问什么问题是有限制的。

将这一点扩展到一个我们所做的一切都由计算机调解的世界并不容易，但我们需要开始讨论哪些数据永远不应该被收集。有一些明显的地方可以开始。我们在网上阅读的内容应该像在纸媒世界中一样隐私。这意味着我们应该在法律上限制记录我们阅读的网页、我们点击的链接和我们的搜索结果。我们的行动也是如此;不应该成为拥有手机的条件，让我们让自己受到持续的监控。我们的交往——我们和谁交流，我们在街上遇到谁——不应该受到持续的监视。也许公司可以被允许立即使用其中的一些数据，然后必须清除它。也许他们会被允许保存一小段时间。

迈阿密大学法学院教授迈克尔·弗鲁姆金(Michael Froomkin)提出了一个有趣的想法:要求从事大规模数据收集的政府机构和私营公司以环境影响报告为蓝本，提交隐私影响通知。这将有助于告知公众收集的内容和原因，以及如何存储和使用这些数据。这将鼓励决策者在任何项目开发的早期就考虑隐私问题，并征求公众的反馈。

一个开始的地方是要求用户选择加入。基本上，获得同意有两种方式。Opt-in是指在你的数据被收集和使用之前，你必须明确同意。Opt-out则相反;除非您明确表示反对，否则您的数据将被收集和使用。像Facebook这样的公司更喜欢选择退出，因为他们可以让这个选项很难找到，而且知道大多数人不会费心。选择加入更公平，服务的使用不应该以允许数据收集为前提。

目前来看，收集和保存所有数据并没有什么坏处。通过限制公司可以收集什么和他们可以用他们收集的数据做什么，通过让公司对他们控制下的数据负责，通过强迫他们向客户坦白他们实际收集了什么和他们用这些数据做了什么，我们将影响他们只收集和保存他们知道有价值的关于我们的数据。

国会需要开始更新美国隐私法的艰苦工作，停止为不作为找借口。法院也可以通过执行现行的隐私法，在保护消费者隐私方面发挥重要作用。监管机构，如联邦贸易委员会和联邦通信委员会，在某些领域有一定的权力保护消费者隐私。但美国今天需要的是一个独立的数据保护机构，可以与世界上其他国家的数据保护机构相媲美。而我们必须做得更好，而不是在问题变得足够有害之后才去修补。这些挑战是巨大的，而且

我们需要一个拥有专业知识和资源的机构来产生有意义的影响。

用更少的数据凑合一下

总的来说，与现在相比，组织可以收集更少的数据，并将其存储更短的时间。关键是要了解为了什么目的需要多少数据。

例如，许多收集身份信息的系统并不真正需要这些信息。通常，只需要授权就可以了。社交网站不需要知道你的真实同一性。云存储公司也不需要。

有些类型的数据分析需要你有很多人的数据，但不是每个人的数据。想想Waze。它使用监控数据来推断交通流量，但并不需要每个人的数据来做到这一点。如果它有足够多的汽车被监控，可以对主要道路进行广泛的覆盖，那就足够了。许多零售商依靠无所不在的监控来衡量广告的有效性，推断购买模式，等等;但同样，他们并不需要所有人的数据。一个有代表性的样本对于这些应用来说已经足够好了，而且在数据收集成本很高的时候很常见。

其他应用程序更喜欢拥有每个人的数据，只是因为这使它们更有效。当然，如果谷歌只拥有一半用户的数据，或者只保存所有用户的一半搜索查询，它也可以做得很好，但这将是一项利润较低的业务。还有一些应用程序实际上需要所有的数据。如果你是一家试图提供移动电话服务的手机公司，你需要知道每个用户的位置，否则系统将无法工作。

公司需要存储数据的时间长短也存在差异。Waze和你的手机公司只需要实时的位置数据。广告商需要一些历史数据，但更新的数据更有价值。另一方面，有些数据对于研究来说是无价之宝。例如，推特正在将其数据提供给美国国会图书馆。

我们需要法律来迫使公司收集他们需要的最少数据，并在他们需要的最短时间内保存这些数据，并且比目前更安全地存储这些数据。正如人们所预料的那样，德语中有一个词来形容这种做法:*Datensparsamkeit*。

赋予人们对自己数据的权利

美国是唯一没有基本数据保护法的西方国家。我们确实对某些类型的信息有保护，但这些都是孤立的领域。总的来说，我们对自己数据的权利参差不齐。b谷歌“记得”我早已忘记的事情。这是因为谷歌有我一生的搜索历史，但我无法访问它来刷新我的记忆。美敦力坚持认为，其心脏除颤器的数据是公司专有的，不会让植入除颤器的患者获得这些数据。在欧盟，人们有权知道公司掌握了他们的哪些数据。这就是为什么奥地利人马克斯·施雷姆斯(Max Schrems)能够迫使Facebook把他所有的钱都给他

公司拥有的个人信息。我们这些在美国的人没有这种权利。

要弄清楚这些权利应该如何发挥作用并不容易。例如，这里是你在社交网站上产生的不同类型数据的列表。

- 服务数据:你为了使用社交网站而提供给该网站的数据。根据网站的不同，这些数据可能包括你的法定姓名、年龄和信用卡号码。
- 公开的数据:您在自己的页面上发布的内容，如博客条目、照片、信息和评论。
- 委托数据:你在别人的页面上发布的内容。它基本上和公开的数据是一样的，但不同的是，一旦你发布了数据，你就无法控制这些数据——另一个用户可以控制。
- 附带数据:其他人发布的关于你的信息。可能是别人写的关于你的一段话，或者是别人拍的你的照片发上去的。你不仅对它没有任何控制权，甚至它都不是你创造的。
- 行为数据:网站通过监控你做了什么以及和谁一起做这些事来收集关于你习惯的数据。
- 衍生数据:从所有其他数据中推断出的关于你的数据。比如，如果你80%的朋友都自认为是同性恋，那么你很可能也是同性恋。

对于这些类型的数据，你应该拥有哪些权利呢?如今，这一权利已经遍布全球。有些类型永远是私有的，有些可以设为私有，还有一些永远是公开的。有些可以编辑或删除——我知道有一个网站允许在24小时内编辑或删除委托数据——有些则不能。有些可以查看，有些则不能。在美国，没有相关规定;持有数据的人有权决定——当然，他们有完全的访问权限。

不同的平台给你不同的能力来限制谁可以看到你的通信。直到2011年，你可以让你的Facebook帖子只有你的朋友可以读，或者所有人都可以读;那时，Facebook允许你有自定义的朋友群，你可以让你的帖子被你的一些朋友读到，但不是所有的朋友。推文要么是直接的消息，要么是向全世界公开的。Instagram的帖子既可以是公开的，也可以是仅限于特定关注者的，也可以是秘密的。Pinterest页面有公开或秘密选项。

标准化这一点很重要。2012年，白宫发布了《消费者隐私权利法案》。2014年，一个总统大数据和隐私审查小组建议将这份权利法案作为立法的基础。我同意。

这个概念很容易走得太远。计算机科学家和技术评论家杰伦·拉尼尔(Jaron Lanier)提出了一个方案，任何使用我们数据的人，无论是使用我们的数据为我们提供广告的搜索引擎，还是使用我们的数据来确定实时道路拥堵的地图应用，都会自动向我们支付版税。当然，这将是一笔小额支付，甚至可能是纳米支付，但随着时间的推移，它可能会累积到几美元。要做到这一点将是非常复杂的，最终需要持续的监控，即使它试图把这种监控变成每个人的收入来源。更根本的问题是，隐私的概念应该以这种方式受到商业的影响。隐私应该是一项基本权利，而不是一项属性权利。

我们应该有删除的权利。我们应该能够告诉我们将数据委托给的任何公司，“我要离开。删除你掌握的所有关于我的数据。”我们应该

可以去找任何数据经纪人说:“我不是你的产品。我从未允许你收集我的信息并将其出售给他人。我想把我的数据从你的数据库中删除。”这就是欧盟目前正在努力解决的问题:被遗忘权。2014年，欧洲法院(European Court of Justice)裁定，在某些情况下，搜索引擎需要从搜索结果中删除个人信息。这导致一大批人要求谷歌删除对他们不利的搜索结果:政治家、医生、恋童癖者。我们可以争论案件的细节，以及法院是否取得了正确的平衡，但对于企业从中获利的个人数据，这是公民的一项重要权利。

US Consumer Privacy Bill of Rights (2012)

INDIVIDUAL CONTROL: Consumers have a right to exercise control over what personal data companies collect from them and how they use it.

TRANSPARENCY: Consumers have a right to easily understandable and accessible information about privacy and security practices.

RESPECT FOR CONTEXT: Consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data.

SECURITY: Consumers have a right to secure and responsible handling of personal data.

ACCESS AND ACCURACY: Consumers have a right to access and correct personal data in usable formats, in a manner that is appropriate to the sensitivity of the data and the risk of adverse consequences to consumers if the data is inaccurate.

FOCUSED COLLECTION: Consumers have a right to reasonable limits on the personal data that companies collect and retain.

ACCOUNTABILITY: Consumers have a right to have personal data handled by companies with appropriate measures in place to assure they adhere to the Consumer Privacy Bill of Rights.

MAKE DATA COLLECTION AND PRIVACY SALIENT

We reveal data about ourselves all the time, to family, friends, acquaintances, lovers, even strangers. We share with our doctors, our investment counselors, our psychologists. We share a lot of data. But we think of that sharing transactionally: I’m sharing data with *you*, because I need you to know things/trust you with my secrets/am reciprocating

因为你刚刚告诉了我一些私人的事情。

作为一个物种，我们已经进化出了各种各样的心理系统来应对这些复杂的隐私决定。这些系统异常复杂，高度协调，微妙的社交。你可以走进一个派对，立刻知道该怎么做。你跟谁说话，跟谁说什么，谁在你身边，谁在听:我们大多数人都能很好地驾驭这一切。问题是，科技抑制了这种社交能力。把同样的聚会搬到Facebook上，我们的直觉突然开始失灵。我们忘记了谁在看我们的帖子。我们不小心把一些私人的东西发到了公共论坛。我们不明白我们的数据是如何在后台被监控的。我们没有意识到我们使用的技术能做什么，不能做什么。

在很大程度上，这是因为在线环境中的隐私程度并不突出。当关于隐私的想法消失在背景中时，直觉就会失效。一旦我们无法直接

感知人，我们做得不太好。我们不会想，“有一家营利公司把我说的每句话都录下来，然后想把它变成广告。”我们不会认为，“美国和其他国家的政府正在记录我所说的一切，试图找到恐怖分子、罪犯、毒贩，或者这个月的坏人。”这并不是显而易见的。显而易见的是，“我在这个虚拟派对上，和我的朋友和熟人在一起，我们在谈论私人的事情。”

所以我们不能把人们在这些网站上不断暴露自己的私人数据作为他们同意被监控的证据。他们所同意的是他们头脑中真实世界的模拟，他们并没有完全理解将这个系统转移到网络空间的后果。

像Facebook这样的公司更喜欢这种方式。他们不遗余力地确保你在他们的网站上不会想到隐私，他们还会使用认知技巧，比如向你展示朋友的照片，来增加你的信任。政府甚至走得更远，将他们的大部分监控保密，所以人们甚至不知道正在发生的事情。这就解释了人们声称隐私很重要，而他们的行动证明隐私并不重要之间的脱节:我们使用的系统是故意设计的，这样隐私问题就不会出现。

我们需要给人们真正的在线隐私选择，以及理解和选择这种选择的能力。如果公司必须向客户和用户证明自己的合理性，他们就不会那么倾向于用我们的数据做令人毛骨悚然的事情。如果用户知道真正的成本，他们就不太可能被“免费”所诱惑。这就需要“产品真实”的法律来规范企业，也需要类似的法律来规范政府。

首先，网站应该被要求披露哪些第三方在跟踪他们的访问者，智能手机应用程序应该披露他们记录的用户信息。监控被隐藏的地方太多了;我们也需要把它凸显出来。

再说一次，这很难。通知、选择和同意是处理这个问题的正确方式，但我们知道，冗长的法律隐私政策——那些你没有阅读就点击“我同意”的通知和同意用户协议——是行不通的。它们故意写得又长又详细，因此会让人感到无聊和困惑;而且它们也不会得到用户方面任何有意义的同意。我们可以非常肯定的是，每当你在Facebook上发布内容时，弹出一个窗口说，“你写的东西将被Facebook保存并用于营销，并将按需提供给政府”，也不会奏效。我们需要一些中间路线。我的猜测是，它将涉及标准化的政策和某种第三方认证。

建立信息受托人

在我们生活的一些领域，我们经常让专业人士接触到我们的个人信息。为了确保他们只为了我们的利益而使用这些信息，我们建立了受托责任的概念。医生、律师和会计师都受到规则的约束，这些规则要求他们把客户的利益放在首位

高于自己的利益。这些规则规定了他们何时以及如何使用我们给予他们的信息和权力，一般不允许他们将其用于无关的目的。对于何时可以要求受托人提供个人信息，警方有相关规定。信托关系创造了一种高于其他义务的注意义务。

我们需要信息受托人。他们的想法是，他们将成为一类持有个人数据的组织，受到特殊的法律限制和保护。公司可以决定是否成为这一类组织的一部分。这与投资顾问有信托责任，而经纪人没有信托责任相当。为了激励公司成为受托人，政府可以为那些愿意承担额外责任的公司提供一定的税收减免或法律豁免。也许某些类型的企业会被自动归类为受托人，仅仅是因为它们自然收集了大量的个人信息:互联网服务提供商、手机公司、电子邮件提供商、搜索引擎、社交网络平台。

受托人监管会让人们相信，他们的信息不会被交给政府，出售给第三方，或者以其他方式被用来对付他们。它将为委托给受托人的信息提供特殊保护。它还要求信息提供者承担一定的注意义务:特定级别的安全、定期审计等等。这将使信任成为可能。

与此类似，互联网安全专家丹·吉尔(Dan Geer)建议互联网服务提供商选择他们是内容公司还是通信公司。作为内容公司，他们可以使用这些数据并从中获利，但也要对这些数据负责。作为通信公司，他们不会对数据负责，但也不能看数据。

在中世纪，天主教会对在忏悔中披露的所有罪行规定了严格的保密义务，认识到如果人们担心自己的信任可能被神父背叛，就不会参加圣礼。今天，我们在网上也需要类似的信心。

激发新的商业模式

监控之所以成为互联网的商业模式，是因为它是最容易赚钱的东西，而且没有规则来监管。它一直是互联网的商业模式，因为成本低，潜在收益巨大，而且(至少在美国)*仍然*没有监管它的规则。

通过既规范我们数据的收集和使用，又提高保留我们数据的成本，我们自然会激发不依赖于监控的新商业模式。技术能力已经存在。有很多研究从一开始就把隐私融入到产品和服务中:通过设计来保护隐私。信用卡公司不必为了给我们开账单和防止欺诈而跟踪我们的每一笔消费。手机供应商不必为了让我们打电话和发短信而永久记录我们的位置。互联网可以建立在强大的匿名保护之上。电子现金既安全又匿名。所有这些都是可能的;我们

只要想要它们。

诚然，这将是一个缓慢的过程。最广泛收集我们数据的公司相信广告收入有巨大增长的潜力。互联网广告在全球范围内可能是一个价值1250亿美元的行业，但它仍然只占广告市场的25%。b谷歌和Facebook等公司关注的是花在电视(40%)和报纸杂志(36%)上的广告费。他们在大数据的价值上投入了大量资金——收集一切，然后再想办法处理这些数据——而且不会轻易改变方向。记者詹姆斯·昆斯特勒(James Kunstler)把这种现象称为“先前投资的心理”，这也是为什么我们经常把坏钱丢在好钱之后。承认自己的错误是很难的，尤其是在数据收集和存储成本如此之低的情况下。

在市场经济中，如果一家公司不能找到一个盈利的商业模式，其他公司就会出现。如果我们成功地提高了监控和数据收集的成本，不依赖于它的新企业就会崛起，取代目前依赖于它的企业。

反对政府监控

到目前为止，斯诺登泄密事件最重要的影响是，它打破了我在第6章中讨论过的公私监控伙伴关系。在斯诺登事件之前，与NSA合作的公司没有任何不利因素。如果NSA要求你提供所有互联网流量的副本，或者在你的安全软件中安装后门，你可以认为你的帮助将永远保密。公平地说，并不是每个人都愿意合作。有些人上了法庭。但似乎他们中的许多人，尤其是政府监管的垄断电信公司和骨干运营商，都很乐意让NSA不受限制地获得它所要求的一切。这很容易，他们在冷战期间一直这样做，然后在9/11之后立即做到了，没有大惊小怪。

这种情况正在改变。现在，保护隐私和对抗美国国家安全局(NSA)有了商业价值，合作也有了商业损害。基本上，企业可以通过四种手段来对抗:透明度、技术、诉讼和游说。

许多计算机公司——雅虎、b谷歌、微软和其他公司——现在定期发布“透明度报告”，让我们大致了解这些公司收到了多少政府数据请求，又遵守了多少。这在很大程度上是出于公关动机，让我们放心，只有很小一部分用户数据被发送给了政府。例如，b谷歌在2013年表示，它向美国政府移交了1至2000名用户的互联网元数据，以及1.8万至2万名用户的通信内容。这些范围是受监管的;这些公司不允许报告确切的数字，尽管许多公司正在向政府施压，要求政府能够披露更精确的信息。(b谷歌已经更准确地报道了世界各地其他政府的要求。)

甚至一些电信公司和有线电视公司也在发布透明度报告，

从2014年初的CREDO Mobile开始。这些都没有什么价值。例如，威瑞森(Verizon)报告称，该公司在2013年收到了32万份索取数据的“执法要求”。我们知道，威瑞森每三个月就会收到一封国家安全信函，要求它交出2.9亿用户的元数据，那么这32万是什么意思呢?

一些公司正试图走得更远。2014年，苹果公司宣布，它将告知个人用户政府对其数据的所有要求，而这些要求并没有被法律明确禁止披露。微软和b谷歌联合起诉美国政府，要求提高透明度。雅虎也在做同样的事情。

其他公司也在雇佣“权证金丝雀”(warrant canary)，试图绕开法律上的禁言令。从2013年开始，苹果的透明度报告中包含了这样一句话:“苹果从未收到过《美国爱国者法案》第215条下的命令。”这个想法是，如果苹果收到这样的命令，它将被禁止披露，但它可以删除这句话，作为对警惕的读者的一个信号。法院从未对这种做法的合法性做出过裁决，我个人对这种做法是否有效持怀疑态度，但这是一种勇敢而聪明的努力。

在技术方面，许多公司正在加强对加密的使用:对他们与用户和客户的互联网连接，对他们自己的网络，对他们的数据库。在b谷歌得知NSA正在窃听其数据中心之间的干线通信链路后，它对这些链路进行了加密。在雅虎得知NSA正在窃听其用户与雅虎网站之间的网络连接后，雅虎和微软(假设其用户也被窃听)都开始对其进行加密。几家大型电子邮件提供商现在也开始对在其数据中心之间传输的电子邮件进行加密。其他公司正在采取更多措施对它们与用户和客户之间的通信进行加密。iphone和安卓手机默认都是加密的。谷歌现在提供端到端的Gmail加密，尽管我猜测这将是一个很少使用的选项，因为如果保持加密，用户将无法搜索和排序他们的电子邮件。

在法庭上，公司应该代表用户提起诉讼。他们应该要求法院下达所有访问权限的命令，并对任何看起来过于宽泛的法院命令进行反击。其中一些已经在进行中。2008年，雅虎在法庭上与NSA进行了长时间的秘密斗争，最后被迫加入了“棱镜”项目。2012年，推特在政府要求交出与“占领华尔街”抗议者有关的信息时未果。截至2014年，Facebook正在与一项法院命令抗争，该命令要求将400名用户的私人信息、照片等交给纽约地区检察官，以寻找社会保险欺诈的证据。

公司可以采取更多措施来支持诉讼工作。他们应该在任何判例对他们有影响的案件中提交法庭之友简报。2013年，当联邦调查局(FBI)要求所有Lavabit用户提供主密钥，试图获取一个人的电子邮件时，没有一家大型电子邮件提供商——谷歌(google)、微软(Microsoft)、雅虎(Yahoo)等任何人——提交了本案的简报。为什么不呢?他们需要认识到我们都是一条船上的人。

互联网的国际性再次在这方面制造了一个复杂的问题。这是一个

对于一家公司来说，遵守从自己国家获得数据的合法要求是件好事，但其他国家呢?21世纪初，雅虎曾四次按照中国政府的要求提供个人用户的数据，导致这些人以“颠覆”和“泄露国家机密”的罪名被逮捕和监禁。雅虎应该这么做吗?如果这个专制政权像沙特阿拉伯那样与美国保持友好关系，会有什么不同吗?许多美国互联网公司辩称，它们不受没有设立办事处的国家的管辖。一家美国公司可能无法抗拒中国的法律，但它可能可以抗拒那些更小、更弱的国家的法律。在很多方面，这些公司可以选择他们想要遵守或不遵守哪些外国法律。他们应该选择最大限度地保护用户隐私。

在政治舞台上，企业应该运用自己的政治影响力。谷歌、Facebook、微软和其他公司正在积极游说立法限制美国政府如何进行监控。这是好事，但我们需要做得更多。在华盛顿，最有说服力的论点往往来自那些关心自己底线的公司。

重要的是不要把这一切看得太重。公司的利益可能会暂时与用户的隐私利益重叠，但它们不会永远保持一致。多年来，企业一直在与任何限制其收集和使用数据能力的法律作斗争。欧盟一直试图通过一项更新的、更严格的数据保护法规，但面临着美国互联网公司的激烈游说，这些公司不想停止数据收集。这一新发现的对抗美国国家安全局的中坚力量，更多的是为了管理用户的看法，而不是为了解决隐私问题。这就是为什么我们也需要对企业进行强有力的监管。

一部新的大宪章

万维网的发明者蒂姆·伯纳斯-李呼吁制定新的《大宪章》，限制政府和企业的行为，将责任而不仅仅是权利强加给信息时代的企业。历史上的类比实际上并不是那么好，但其总体思路值得探索。这基本上就是我在这本书中所呼吁的。

还记得第4章，我把公司和用户的关系描述为封建关系吗?那是因为它是临时的、片面的:基于用令人麻木的法律术语写成的最终用户许可协议，公司可以随心所欲地改变。历史上的封建主义就很像这样;领主有权力强迫农民建立关系，在这种关系中，领主拥有所有的权利，几乎不承担可执行的责任。在中世纪的欧洲，中央集权国家和法治的兴起提供了封建制度所缺乏的灵活性。1215年，《大宪章》(Magna Carta)成为第一份现代文件，将统治者的合法性来自其臣民的理念奉为神圣，并将国王置于法治之下。这份文件首先规定了国王相对于下级领主的责任，随着时间的推移，社会走上了民有、民治、民享的漫长道路。

在18世纪，当各国开始认识到他们的统治权

当时流行的政治哲学是托马斯·霍布斯(Thomas Hobbes)的，他认为人民向仁慈的君主牺牲权力和自由，而君主则为他们提供包括安全在内的各种服务。约翰·洛克认为，这种关系是不公平和不平衡的，政府的权威来自于“被统治者的同意”。这种观念推动了英国、法国和美国的革命，并导致了法国的《人权宣言》和美国的《人权》。

记者兼数字权利倡导者丽贝卡·麦金农在她的著作《*网络的同意*》中指出:“没有一家公司是完美的——就像没有一个君主是完美的一样，无论国王、王后或仁慈的独裁者是多么善良和善良。但这就是问题的关键:目前我们与数字君主的社会契约处于原始的、霍布斯式的、保皇派的水平。如果我们幸运的话，我们会得到一个好的君主，我们祈祷他的儿子或选择的继承人不是邪恶的。大多数人不再接受这样的君主是有原因的。现在是时候将社会契约提升到洛克式的水平，以治理我们的数字生活，这样对我们身份的管理和对信息的获取才能更真实、更真诚地反映网络化的同意。”

《马德里隐私宣言》(2009)

民间社会借第31届国际隐私和数据保护专员年会之机:

1. Reaffirm support for a global framework of Fair Information Practices that places obligations on those who collect and process personal information and gives rights to those whose personal information is collected;
2. Reaffirm support for independent data protection authorities that make determinations, in the context of a legal framework, transparently and without commercial advantage or political influence;
3. Reaffirm support for genuine Privacy Enhancing Techniques that minimize or eliminate the collection of personally identifiable information and for meaningful Privacy Impact Assessments that require compliance with privacy standards;
4. Urge countries that have not ratified Council of Europe Convention 108 together with the Protocol of 2001 to do so as expeditiously as possible;
5. Urge countries that have not yet established a comprehensive framework for privacy protection and an independent data protection authority to do so as expeditiously as possible;
6. Urge those countries that have established legal frameworks for privacy protection to ensure effective implementation and enforcement, and to cooperate at the international and regional level;
7. Urge countries to ensure that individuals are promptly notified when their personal information is improperly disclosed or used in a manner inconsistent with its collection;
8. Recommend comprehensive research into the adequacy of techniques that deidentify; data to determine whether in practice such methods safeguard privacy and anonymity;
9. Call for a moratorium on the development or implementation of new systems of mass surveillance, including facial recognition, whole body imaging, biometric identifiers, and embedded RFID tags, subject to a full and transparent evaluation by independent authorities and democratic debate; and
10. Call for the establishment of a new international framework for privacy protection, with the full participation of civil society, that is based on the rule of law, respect for fundamental human rights, and support for democratic institutions.

这个想法是，一个新的大宪章，一个更专注于滥用权力的机构

在21世纪，权力也会做类似的事情。有几份文件与之接近。2009年由大约100个组织签署的《马德里隐私宣言》(Madrid Privacy Declaration)，仍然是现代社会对隐私权最有力的表述。

15

给我们其他人的解决方案

软监控对用户双方都有效。我们可以使用的技术和各种法律隐私问题。和匿名技术解决方案是为了保护我们的数据和身份。这些技术解决方案是有效的，但可能会受到政府秘密命令的阻挠。我们还需要打一场政治斗争。

政治解决方案需要集体努力，但通常仅限于特定国家。技术解决方案有可能是全球性的。如果微软在设计Windows操作系统时采用了无处不在的文件加密，或者如果互联网工程任务组(Internet Engineering Task Force)决定将所有互联网流量默认加密，那么这些变化将影响到世界上使用这些产品和协议的每个人。

问题的关键在于，政治可以破坏技术，同样，技术也可以破坏政治。两者都不占优势。如果我们要解决问题，我们需要在技术和政治战线上同时战斗。这不仅仅取决于政府和企业。我们人民在这方面有很多工作要做。

防范监视

法学教授埃本·莫格伦写道:“如果我们没有做错任何事情，那么我们就有权尽一切努力保持我们和倾听力量之间的传统平衡。我们有权保持低调。我们有权含糊不清。我们有权说他们不懂的语言。我们有权在我们喜欢的时间、地点和方式会面。”如果一个警察坐在你能听到的地方，你有权把你的谈话转移到别的地方。如果联邦调查局在你家门外停了一辆布满摄像头的货车，你完全有理由关上百叶窗。

同样，我们个人也有很多方法可以保护我们的数据，保护自己不受监控。我将把它们分成几类。

避免监视。你可以改变你的行为来避免监视。你可以用现金支付而不用信用卡，或者故意改变你的驾驶路线以避开交通摄像头。你可以克制自己不为孩子创建Facebook页面，也不给他们的照片贴上标签。你可以不使用谷歌日历、网络邮件或云备份。你可以使用DuckDuckGo进行互联网搜索。你可以把手机留在家里:这是一种避免被跟踪的简单方法，虽然不方便。更有针对性的是，当你去中国和俄罗斯这样的国家旅行时，你可以把电脑和手机留在家里，只使用借来的设备。

你可以通过故意不触发自动监视系统的检测算法来避免激活它们。例如，你可以把你的现金交易保持在金融机构必须向联邦政府报告交易的阈值以下。你可以

拒绝在邮件中讨论某些话题。在自动监控很普遍的中国，人们有时会把信息写在纸上，然后把这些信息的照片发到互联网上。这对打击有针对性的监控毫无帮助，但自动系统的监控难度要大得多。隐写术——将信息隐藏在无害的图像文件中——也是一种类似的技术。

阻断监视。这是我们可以做的最重要的事情来保护自己。美国国家安全局的预算可能比世界上其他国家情报机构的预算加起来还要多，但它并不是魔法造出来的。世界上其他国家情报机构也都不是。有效的国防利用了经济学、物理学和数学。虽然大国的国家安全机构如果想把你个人作为目标，他们将能够挫败你所能做的任何事情，但大规模监控依赖于轻松获取我们的数据。良好的防御会迫使那些想要监视我们的人选择他们的目标，他们根本没有资源来瞄准每个人。

隐私增强技术(宠物)可以帮助你阻止大规模监控。有很多技术可以保护你的数据。例如，有一些易于使用的浏览器插件，可以监控和阻止那些在你上网时跟踪你的网站:Lightbeam、Privacy Badger、Disconnect、Ghostery、FlashBlock等。请记住，你浏览器上的隐私浏览选项只会删除本地数据。因此，虽然它有助于向你的配偶隐藏你看色情片的习惯，但它并不能阻止互联网跟踪。

最重要的PET是加密。用微软的BitLocker或苹果的FileVault加密你的硬盘非常简单，而且完全透明。(去年，我推荐了TrueCrypt，但开发者在2014年神秘的情况下停止了对该程序的维护，没有人知道该怎么看待它。)你可以使用像Off the Record这样的聊天加密程序，用户友好且安全。Cryptocat也值得一看。如果使用云存储，选择提供加密的公司。我喜欢Spideroak，但也有其他公司。有针对网络语音的加密程序:Silent Circle, TORFone, RedPhone, Blackphone。

尝试使用电子邮件加密插件，如PGP。谷歌现在为其用户提供加密电子邮件。你会失去一些搜索和组织功能，但增加的隐私可能是值得的。

tls(以前的ssl)是一种对你的一些网页浏览进行加密的协议。当你在后台看到URL开头是“https”而不是“http”时，它就会自动发生。很多网站都提供这个选项，但不是默认设置。你可以通过运行一个名为HTTPS Everywhere的浏览器插件来确保它在任何可能的地方都是打开的。

这并不是一个全面的列表。那要单独写一本书，而且几个月之内就会过时。技术总是在变化;上网看看有什么被推荐。

我不会引导你;许多宠物将超出这本书的普通读者的能力。尤其是PGP电子邮件加密，使用起来非常麻烦。

最有效的加密工具是那些在后台运行的工具，即使你没有意识到它们，比如HTTPS Everywhere和硬盘加密程序。在第14章中，我讨论了一些公司正在做的事情来保护他们用户的数据。更多的事情正在幕后进行。管理互联网的标准机构对政府的监控非常愤怒，他们正在努力使加密在网上更加普遍。希望在这本书出版的时候会有更多的选择。

还要记住，有很多东西是加密无法保护的。谷歌默认情况下加密您与Gmail的连接，并在您的邮件位于其服务器上并在其网络中流动时对其进行加密。但是谷歌处理您的邮件，因此它有密钥的副本。这同样适用于你发送到任何社交网站的任何东西。

大多数元数据都无法加密。因此，虽然你可以加密电子邮件的内容，但收件人和发件人行需要不加密，这样电子邮件系统才能发送信息。同样，你的手机可以加密你的语音对话，但你拨打的电话号码，你的手机的位置，你的手机的ID号码都需要不加密。当你通过互联网将信用卡数据发送给在线零售商时，你可以加密信用卡数据，但该公司需要你的姓名和地址，以便将你购买的商品邮寄给你。

最后，加密不能保护你的电脑在使用中。你仍然可能被黑客攻击，要么是犯罪分子，要么是政府。但是，同样，这很可能是有针对性的监视，而不是大规模的。所有这些都意味着，虽然加密是解决方案的重要组成部分，但它并不是解决方案的全部。

在浏览网页时，当前保护你匿名性的最佳工具是Tor。它非常容易使用，而且据我们所知，它是安全的。同样，可以使用各种代理来逃避监视和审查。洋葱共享程序使用Tor在互联网上匿名发送文件。针对某些对手，网络代理是足够的匿名工具。

你可以做更多低技术含量的事情来阻止监视。你可以在不需要的时候关闭智能手机上的定位服务，并尝试做出明智的决定，决定哪些应用程序可以访问你的位置和其他数据。你可以避免在公共网站上发布身份信息。当斯诺登第一次在香港会见记者时，他让所有记者都把手机放在冰箱里，屏蔽所有进出这些设备的信号，这样就不能被远程变成监听设备。

有时候，监听屏蔽非常简单。在电脑摄像头上贴一张贴纸，可以防止远程控制摄像头的人给你拍照。你可以在信封上留下回信地址，以限制邮局可以收集的数据。你可以雇人跟在你车后面，让你的车牌不被自动扫描仪扫描到，就像德黑兰的人们做的那样。有时，这就像说“不”一样简单:拒绝在被要求的表格上透露个人信息，不把你的电话号码给商店的售货员，等等。

有些屏蔽行为是非法的:你实际上不允许覆盖你的

汽车的车牌。还有一些是不受社会鼓励的，比如戴着口罩在镇上走来走去。还有一些会让你看起来很滑稽，比如在脸上涂上颜料来骗过面部识别摄像头，或者穿特殊的衣服来迷惑无人机。

扭曲监视。我把浏览器设置为每次关闭时删除cookie，我每天都会这么做好几次。我仍然在被监视，但现在要把所有这些小的监视绑在我身上要困难得多，广告也不会一直跟着我。我在西夫韦购物的时候，会用朋友的常客号码。这最终扭曲了商店对她的监控。

有时这被称为混淆，一旦你开始思考，就会发现有很多技巧。你可以和朋友、邻居交换零售商亲和卡。你可以变装。在科里·多克托罗(Cory Doctorow) 2008年出版的《*小弟弟*》(Little Brother)一书中，主人公把石头放进鞋子里，改变自己走路的方式，骗过步态识别系统。

人多势众也有安全保障。只要世界上还有宠物让人活下去的地方，我们用得越多，它们就越安全。就像信封一样。如果每个人都默认使用明信片，那么少数使用信封的人就会受到怀疑。由于几乎所有人都使用信封，那些真正需要信封隐私的人并不会脱颖而出。对于像Tor这样的匿名服务来说尤其如此，它依赖于许多人使用它来掩盖每个人的身份。

你也可以——我知道有人就是这么做的——在Facebook上随机搜索一些名字，让它混淆你真正认识的人。充其量，这是部分解决方案;数据分析是一个信噪问题，加上随机噪声会让分析变得更加困难。

你可以在网页表单上或者在被要求的时候给出错误的信息。(你的孩子经常这么做。)多年来，早在消费者追踪成为常态之前，Radio Shack商店就会例行公事地询问顾客的地址和电话号码。有一段时间，我只是拒绝了，但这在社交上很尴尬。相反，我养成了回复“9800 Savage Road, Columbia, MD, 20755”的习惯:这是NSA的地址。几年前，当我把这个故事告诉一位同事时，他说他总是给出“1600 Pennsylvania Avenue, Washington, DC”这个地址。他坚持说没人认出这个地址。

也可以换一个名字办信用卡。这没什么可疑的，只要让你的信用卡公司用另一个名字再办一张卡，和你的账户绑定就行了。只要商家不要求提供ID，你就可以使用。

如果使用得当，骗术的威力会非常大。我记得一个关于摩洛哥一群激进分子的故事。那些没有携带手机的人会被秘密警察跟踪，偶尔还会被殴打。那些没有携带手机的人，因此当他们真正需要隐藏自己的行动时，可以把手机留在家里。更一般地说，如果你关闭了敌人的所有情报渠道，你就关闭了你欺骗他的能力。

打破监视。根据技术的不同，你可以破坏一些监控系统。你可以切断道路上自动测速装置的供电线路。你可以给监控摄像头的镜头喷漆。如果你是一个足够优秀的黑客，你可以禁用

互联网监控系统，删除或毒化监控数据库，或者其他扳手。这一类的东西几乎都是非法的，所以要小心。

其中一些方法比其他方法更难。我们中的一些人会比其他人做得更多。许多人在网络表单中输入随机信息。更少的人——我只遇到过一个这样做的人——在b谷歌上随机搜索一些东西来混淆他们的个人资料。许多这样的行为都需要付出社交、时间或金钱的代价，更不用说持续偏执的心理负担了。我很少注册零售亲和卡，这意味着我错过了折扣。我不用Gmail，也从不通过网络访问我的电子邮件。我没有个人Facebook账户，这意味着我和朋友们的联系不像平时那样紧密。但无论我走到哪里，我都随身带着手机，只要有可能，我就会收集飞行里程，这意味着我让这些公司跟踪我。你会找到自己的最佳位置。

我们都应该尽我们所能，因为我们相信我们的隐私是重要的，我们需要行使我们的权利，以免失去它们。但看在老天的份上，除非你知道你的数据最终会在哪里，否则不要参加那些愚蠢的在线调查。

援助政府监控

在这本书中呼吁帮助政府进行监控似乎不太合适，但请听我把话说完。

政府监控有其合理的需求，包括执法和情报方面的需求，我们应该认识到这一点。更重要的是，我们需要支持合法的监控，并努力让这些团体在不侵犯隐私、不颠覆安全、不侵犯公民不受不合理怀疑和观察的权利的情况下，做他们需要做的事情。如果我们能为执法人员提供调查犯罪的新方法，他们就不会再要求为了自己的利益而破坏安全。

地缘政治冲突不会消失，外国情报是应对这些事件的唯一工具。当我在2014年夏末写这篇文章的时候，俄罗斯正在集结军队对抗乌克兰，中国在南海欺负日本和韩国，维吾尔族恐怖分子正在杀害汉人，以色列正在攻击加沙，卡塔尔和土耳其正在帮助加沙自卫，阿富汗混乱不堪，利比亚正在衰落，埃及又回到了独裁统治。伊朗的核计划可能正在恢复，埃博拉病毒正在席卷西非，朝鲜正在测试新型导弹，叙利亚正在杀害自己的人民，伊拉克的大部分地区被一个名义上的伊斯兰极端组织ISIS控制。而这些都只是新闻的素材。当你读到这本书的时候，这个清单会有所不同，但同样严肃。我向你保证，白宫里没有人要求NSA尽量减少对这些和类似威胁的数据收集。他们也不应该这么做。

此外，世界各国政府普遍担心网络攻击。这在很大程度上是反应过度，但确实存在风险。而且网络防御陷入了一个典型的集体行动问题。网络空间的大部分基础设施掌握在私人手中，但重大网络攻击的大部分危害将由整个人口感受到。这

这意味着信任控制我们基础设施的公司来充分保护基础设施是行不通的。某种程度的政府介入是必要的。2013年，NSA局长基思·亚历山大(Keith Alexander)表示，“除非我进入所有的网络，否则我无法保卫国家。”这是华盛顿的主流观点。

是的，我们需要弄清楚我们有多希望NSA进入我们所有的网络。但我们也需要帮助NSA不要进入我们所有的网络。如果我们能给政府提供新的方法来收集敌对国家、恐怖组织和全球犯罪分子的数据，他们就不需要采取我在本书中详细介绍的极端措施了。这是对新思想、新工具和新技术的真正呼唤。老实说，我不知道解决方案会是什么样子。有一条中庸之道，要靠我们自己去寻找。

这不是每个人都能完成的任务。这是工业界、学术界以及我们这些理解和使用这些技术的人的任务。但这是一项重要的任务，情报部门或执法部门都不会为我们做这件事。如果我们想让NSA这样的机构保护我们的隐私，我们就必须给他们提供执行情报工作的新方法。

选择你的盟友和敌人

我们的法律是基于地理位置的。在人类历史的大部分时间里，这是有道理的。但在互联网上就没那么有意义了;互联网太国际化了。

你显然要遵守你所居住国家的法律规定，但当你上网时，事情就变得更复杂了。你会受到你的硬件制造商所在国的法律法规，你的软件供应商所在国的法律法规，你的在线云应用提供商所在国的法律法规的影响。你会受到你的数据所在国家的规则的影响，以及你的数据在互联网上移动时所经过的任何国家的规则的影响。

例如，《爱国者法案》要求美国公司在被要求时将数据移交给美国政府，无论数据存储在哪里。你可能是一个居住在法国的法国公民，而微软可能只把你的电子邮件存储在爱尔兰的服务器上。但由于微软是一家美国公司，美国坚称它有义务按需提供你的数据。英国也希望获得类似的访问权限。

这意味着你必须决定:你信任哪些国家的数据，你信任哪些公司的数据?

企业并不是都一样糟糕。你可以从谷歌或Apple获得电子邮件、日历和地址簿。它们都能保护你的数据不被政府大量收集，但在法律强制下，它们会把你的数据提供给世界上许多政府。b谷歌正在着手一项重大项目，以提高其用户的安全性，防止政府监控。但b谷歌的业务是收集你的数据并将其用于广告，而苹果的商业模式是保护客户的隐私。

你信任一家不受限制地处理你的数据、还受制于美国国家安全局(NSA)和联邦调查局(FBI)法律要求的美国公司吗?还是你相信一家欧洲公司，它在企业监控方面受到政府的严格监管，但同时也受到本国政府和美国政府的不受约束的监控，对它的使用意味着你的数据跨越了国际边界?如果你因为担心NSA后门而不从思科购买网络设备，你会从谁那里购买呢?华为?还记得我在第四章做的封建类比吗;哪个领主你更信任?

很难知道从哪里开始。在今天的云计算世界里，我们往往不知道哪些公司实际托管着我们的数据。像Orbitz这样的互联网公司可能会把它的基础设施托管在像Atlassian这样的提供商上，而Atlassian又把它的基础设施托管在像Rackspace这样的提供商上。你知道你的Orbitz数据到底在哪里吗?

我们需要能够知道我们的数据存储在哪里，并指定我们希望我们的数据存储在哪些国家，以及我们希望我们的数据永远不要靠近哪些国家。同时，我们必须尽我们所能做到最好。并认识到，在大多数情况下，我们根本不知道。

但说到政府，尽管我很不高兴，但我宁愿被美国政府窃听，也不愿被其他许多政权窃听。

鼓动政治变革

2014年，欧洲法院(European Court of Justice)推翻了欧盟的数据保留规定，该规定要求服务提供商将电子邮件和电话信息保存两年。作为回应，英国政府匆忙通过了一项新法律，恢复了数据保留要求，并赋予警方对公民的新监控权力。这是一个丑陋的政治铁路工作，但有趣的是，英国首相戴维·卡梅伦(David Cameron)是如何在一个广播节目中为这项法律辩护的:“我根本不准备成为一个在恐怖事件发生后必须向民众发表讲话的首相，并解释我本可以做得更多来防止恐怖事件发生。”

这是在用恐惧说话，但并不是对恐怖分子的恐惧。这是害怕在发生恐怖袭击时受到指责的政治恐惧。职业政治家想要尽一切可能，不顾代价，不顾是否真的让任何人更安全，不顾副作用，以避免因做得不够而受到指责。这种恐惧解释了大多数911后的反恐政策，以及大部分NSA的大规模监控项目。我们的政客害怕我们会指责他们，因为他们没有做到情报机构说他们本可以做的一切，以防止进一步的恐怖主义。

我们必须说服他们——以及我们的选民——无论如何他们都应该做正确的事。

前两章提供的大多数解决方案都要求政府要么执行现行法律，要么修改法律。总的来说，除非我们提出要求，否则这两件事都不会发生。政客们不愿意参与这些辩论，更不愿意对政府的监控实施有意义的限制。

立法机构自然会顺从执法部门的要求，而庞大的监控产业联合体则雇佣了强大的游说力量来支持他们。没有人愿意被描绘成对犯罪或恐怖主义软弱。如今，当美国情报机构被发现违法时，面临牢狱之灾的只有举报人。

在企业方面，成群结队的游说者正在尽最大努力确保对企业监控进行没有意义的改革。自由市场被当作继续无所作为的正当化。警方和国家安全机构也在努力确保我们所有的数据仍然可供他们自己使用。

如果我们想让我们的立法者投票反对军队、执法部门和游说者众多的公司(包括为政府提供服务的公司和直接监视我们的公司)的强大利益，我们就必须让自己变得更加强大。这意味着我们必须参与到政治进程中来。在此，我有三点具体建议。

通知监控。这是第一步。很多监控是隐藏的，但并非完全看不见。这些摄像头可能很小，但如果你仔细观察，你仍然可以看到其中的大部分。当你进入酒吧时，你会注意到有人扫描你的身份证。你可以安装一个浏览器插件，看看是谁在网上跟踪你。你可以关注有关监控的新闻报道。网上有识别监控摄像头的网站。你知道的越多，你就越能理解发生了什么。

说说Surveillance吧。这是下一步。我们谈论得越多，人们就越能意识到发生了什么。而他们越是意识到正在发生的事情，他们就越会关心它。我们在公开场合谈论得越多，我们选出的代表就越会意识到我们对它的关心。

我的意思是非常笼统的。和你的家人、朋友和同事谈论监控。不要成为那种从不发其他事情，但在社交媒体上分享有趣新闻故事的烦人人。参加集会，签署请愿书。给你选出的代表写信。把这本书作为礼物送给你所有的朋友。让别人知道你的观点。这很重要。

谈谈你们国家的法律。在你的国家，什么样的政府监视是合法的?你们国家的企业是如何参与其中的，他们进行什么样的监视是合法的?人们有哪些权利使用增强隐私的技术?一起来看看。

基于斯诺登文件的NSA故事中最超现实的一个方面是，它们如何让最偏执的阴谋论者看起来像理性和常识的典范。人们很容易忘记细节，重新陷入自满;只有继续讨论细节，才能防止这种情况的发生。

从政治上组织。这是我们最有效的策略。最近有很多人们组织起来反对监控的好例子:韩国教师反对新的学生数据库，德国消费者反对支持rfid的购物车，Facebook用户反对新的服务条款，美国航空公司旅客反对

机场全身扫描仪。这些活动并不总是成功的，结果也不完美，但集体行动的重要性怎么强调都不为过。我们需要看到，这些问题对我们所有人来说都是共同的，解决方案也是通用的。

这不是一本关于政治组织的书，在建议如何鼓动政治变革方面，有比我优秀得多的人。我确实知道，政治不仅仅是在选举期间发生的事情。这是一个持续的过程，包括与立法者接触，在公共场合抗议，以及支持相关的非营利组织。看看电子前沿基金会、电子隐私信息中心、民主与技术中心、隐私国际、开放技术研究所等。他们都在争取更多的隐私和更少的监控。帮助他们吧。

当然，我们对世界上的许多地方都无能为力，但我们可以在力所能及的地方推动变革。然后我们可以慢慢地向外发展。世界范围的变化就是这样发生的。

不要放弃

宿命论是改变的敌人。宿命论的意思是:政府和大公司都是无所不能的，而大多数政客都无意约束它们中的任何一个，所以我们对改变现状无能为力。宿命论的意思是:大规模监控无处不在，我们无法抵制，而抵制只会让他们对我们更感兴趣。

断言本身有一定道理，但结论是错误的。良好的计算机安全性和普遍的加密技术使大规模监控变得困难。根据公司的隐私政策来选择做生意的公司，会让公司更有可能拥有良好的隐私政策。政治组织是有效的。我们对大数据的迷恋和对恐怖主义的非理性恐惧都会随着时间的推移而减弱。法律最终会限制政府和企业在互联网上的权力。

我建议的政策转变是重大的，它们将会发挥作用。历史上每一次重大的政策转变在一开始看起来都是徒劳的。事情就是这样。我们需要为政治变革而战，我们需要继续战斗，直到胜利。在此之前，我们还可以赢得许多小小的战斗。

人多力量大，如果公众的呼声越来越高，政府和企业将被迫做出回应。我们正在努力防止出现奥威尔《一九八四》中描绘的那种威权政府，以及无数反乌托邦赛博朋克科幻小说中描绘的那种公司化国家。我们离这两个终点都很远，但火车正朝两个方向行驶，我们需要踩刹车。

16
社会规范与大数据权衡

在前面的企业、三章和个人中，我概述了行为。他们中的一些变化需要技术上的改变，但其中大部分的变化需要新的法律或至少新的政策。在这一点上，其中许多是不现实的，至少在美国是这样。我还没有生活在一个大多数人都希望这些改变的国家，更不用说一个人民的意愿很容易转化为立法行动的国家了。

大多数人似乎并不关心他们的私密信息是否被企业收集和利用;他们认为，自己信任的政府进行监控，是保证自己安全的必要前提。大多数人仍然过于害怕恐怖主义。他们不了解政府和私人团体可获得的监控能力的程度。他们低估了正在进行的监控的数量，也没有意识到大规模的政府监控对保护我们的安全没有多大作用。大多数人都乐于用敏感的个人信息换取免费的电子邮件、网络搜索或与朋友聊天的平台。

欧洲有些不同——它对企业监控的监管更严格，而对政府监控的监管则少得多——但就大多数目的而言，公众的情绪是一样的。

在我们进行有意义的政治变革之前，我们的一些社会规范将不得不改变。我们需要让人们理解监控的范围之广，以及由此产生的巨大的权力集中。一旦他们明白了，大多数人可能会说，“这是不行的。”我们需要拿出政治意愿，既要打击政府方面的执法部门和国家情报界，也要打击企业方面的政府承包商和监控行业。在这一切发生之前，社会看待和重视隐私、安全、自由、信任以及其他一些定义这场辩论的抽象概念的方式必须发生一些重大变化。

这是困难的。舆论倾向于走向实际。我们善于接受现状——不管现状是什么，不管它是最近才出现的。(老实说，大多数监控都是在不到20年的时间里出现的，这让我很震惊。)我们越来越习惯了“圆形监狱”。当人们耸耸肩说:“你要做什么?”每次Facebook降低用户隐私选项的时候，你都能看到它的缩影;人们一开始会抱怨，但很快就习惯了。

这一章接下来的，都是态度的改变。如果我们想要超越监控社会，我们就必须通过这些方式来改变我们的感受和思想。

重新调整我们的恐惧

《爱国者法案》于2001年10月26日签署成为法律，就在恐怖分子袭击世贸中心和五角大楼的45天后。这是一份警察和情报权力和当局的愿望清单，在参众两院以最小的辩论以压倒性多数通过。国会没有人在投票前读过这份清单。几乎全国所有人都希望这项法律通过，尽管他们不理解其中的条款。

2014年，我参加了一场演讲，广告公司M&C Saatchi的董事长兼首席执行官蒂姆·达菲(Tim Duffy)试图改善隐私的信息传递。他建议“你的底线在哪里?”作为可能的框架。但如果听众害怕恐怖分子，他们就会以允许大量监控的方式划清界限。哈佛法学院教授杰克·戈德史密斯(Jack Goldsmith)指出，当我们感到害怕时，更多的国会监督会产生更多的国家安全局权力。

恐惧胜过隐私。对恐怖主义的恐惧胜过对暴政的恐惧。如果足够强大，它会压倒本书中堆积在一起的所有担忧。在民众中，是对下一次恐怖袭击的恐惧。对于政治家来说，这是恐惧，同时也害怕被*指责*为下一次恐怖袭击的罪魁祸首。但无论如何，这是一种恐惧。回想一下前一章中的卡梅伦首相。当我问到针对恐怖主义威胁的大规模监控明显无效时，这是我一次又一次从政府官员那里听到的。是的，他们承认，大规模监控没有取得任何成功;但这是一种保险。他们知道，他们的目标监视工作在某一时刻会失败，他们希望大规模监视能够作为后备。的确，这样的可能性很低，但他们相信，他们必须尽一切可能——既为了国家的安全，也为了他们工作的安全。

无论威胁有多严重，大规模监控都不是有效的对策;传统的警察和情报工作才是。我们需要抵制*做某件事的冲动*，不管所提议的行动是否有效。

保持恐慌情绪是一件大事。情报界的人知道这是他们影响力和权力的基础。政府承包商也知道这是他们合同的资金来源。作家和互联网活动家克莱·舍基(Clay Shirky)指出，“机构将试图保护他们解决的问题。”恐惧就是那个问题。

这是一种被每天的新闻所激起的恐惧。一旦发生可怕的犯罪或恐怖袭击，只要联邦调查局或国土安全部能够访问Facebook上存储的或iPhone上加密的数据，人们就会要求知道为什么联邦调查局或国土安全部不能访问这些数据——为什么他们不能“把这些点联系起来”。然后，法律将会改变，赋予他们更多的权力。杰克·戈德史密斯又说:“政府将增加权力，以充分应对国家安全威胁(因为人民要求这样做)。”

我们需要一种更好的方式来处理我们对恐怖主义的情绪反应，而不是让我们的政府全权侵犯我们的自由，以某种绝望的方式再次感到安全。如果我们找不到一个，那么，正如他们所说，恐怖分子就真的赢了。一

政府的目标是为人民提供安全，但在民主国家，我们需要承担风险。一个拒绝犯罪、恐怖主义或其他风险的社会，从定义上讲就是一个警察国家。而警察国家也会带来自身的危险。

这不仅仅是政客们的责任。媒体也难辞其咎。通过关注罕见和壮观的事件，它们使我们表现得好像恐怖主义比实际情况普遍得多，并使我们对恐怖主义的恐惧远远超过其实际发生的比例。如果我们听信了媒体兜售的宣传，我们也有错。

我们还需要反对那种认为现代技术使一切都不同的观念。在9/11恐怖袭击发生后的几天和几周内，当我们讨论新的法律和新的警察权力时，我们听到了这句话:“宪法不是自杀协议。”它表达了一种基于恐惧的情绪，其含义值得解读。它是这样说的:“制定法律的人不可能预料到我们现在面临的情况。因此，他们对警察权力的限制和对监视的禁令不应该适用于我们。我们的情况是独特的，我们必须忽略所有这些。”我们屈服于这些观念的主要原因是，我们相信恐怖分子可能造成的破坏是如此巨大，以至于我们无法依靠传统的执法手段和事后起诉。

但事实并非如此。这是一种常见的心理谬误，认为我们生活在一个独特的时代，我们面临的挑战与以前的任何挑战都完全不同，因此有必要忽略我们之前为检查政府当局的权力而实施的任何社会控制。林肯总统在南北战争期间暂停人身保护令时就屈服于这种谬论。威尔逊总统在第一次世界大战结束后逮捕并驱逐社会主义者和劳工领袖时就是这样做的。罗斯福总统在第一次世界大战期间拘留日本、德国和意大利血统的美国人时也是这样做的。我们在冷战时期的麦卡锡时代也这么做过。9/11之后，我们又在这样做。

恐惧并不是我们应对这些威胁的唯一方式，历史上有很多例子表明，社会并没有为了保持安全而放弃自己的权利。在2011年安德斯·布雷维克(Anders Breivik)在挪威犯下可怕的大屠杀之后，这个国家在很大程度上保留了自由和开放的核心价值观。当然，还有罗斯福的名言“我们唯一需要恐惧的就是恐惧本身”。百折不挠才是对恐怖主义的正确回应。

美国还有希望。我们并不总是用恐惧来应对恐怖主义。回顾最近的历史，那些勇敢地对抗恐怖主义的总统——杜鲁门、艾森豪威尔、尼克松、里根(有时还有老布什)——比那些利用恐怖主义作为政治哗众取众的机会的总统——卡特、里根(有时还有小布什)——取得了更好的行动和政治成果。我们需要认识到那些在风险面前保护我们自由的政治家的力量，以及那些无法解决问题而选择牺牲我们自由的人的弱点。9/11事件发生十多年后，我们早就应该超越恐惧，回归自由、自由和正义的美国核心价值观。有迹象表明，我们正在这样做。2013年，我们开始看到美国人的观念发生了重大转变

关于公民自由和国家安全之间的权衡。

重新校准隐私

我们个人对隐私的定义既有文化上的，也有情境上的。100年前的定义和今天不一样，100年后的定义也会不一样。美国的情况与欧洲、日本和其他地方的情况不同。几代人之间也不同。

现在，互联网正在迫使我们对隐私的态度发生前所未有的转变。这是因为我们使用互联网的主要方式之一是相互了解。律师寻找潜在的陪审员。求职者查找公司高管;公司的人力资源部门寻找潜在的员工。在第一次约会之前，人们会互相了解对方。这种事情甚至有一个名字:谷歌跟踪。

在网上，我们不断地窥探，偶尔还会侵犯彼此的隐私。这可能会让人很不舒服。网络交流的半永久性为别人让你难堪提供了各种机会。你私下发给某人的电子邮件很容易被转发给其他人。孩子们总是这样对待彼此:转发私人聊天、照片和信息，或者在社交网站上给对方看私人帖子。几秒钟后就删除信息和照片的应用程序在青少年中如此受欢迎的原因之一是，它们有助于防止这类事情的发生。旧网页总有办法留存下来。2010年，维基解密创始人朱利安·阿桑奇(Julian Assange)的OKCupid约会资料被挖出来供公众讨论。

更糟糕的是那些利用互联网进行羞辱和骚扰的人。报复性色情——大部分是前男友发布前女友的艳照——就是一个极端的例子。面部照片勒索网站把这类事情变成了一门生意。嫌疑犯照片是公开记录，但并不容易获得。嫌疑犯照片网站的所有者大量获取照片并将其发布到网上，每个人都可以找到它们，然后向个人收取从网站上删除照片的费用。虽然从技术上讲是合法的，但这是敲诈勒索。这一切都不会消失，即使某些情况在某些司法管辖区是非法的。

我们需要弄清楚这个问题。每个人都有能力购买精密的监控设备，所以我们需要社会规范来告诉我们什么时候不要使用它。我们对彼此的了解超过了我们每个人都能接受的程度，所以我们需要围绕承认我们知道的或假装我们不知道的制定社会规范。这本质上是大卫·布林1998年出版的《*透明社会》一书的观点*;无所不在的监控即将到来，我们必须适应。

互联网造成了自摇滚时代以来最大的代沟。正如Clay Shirky所指出的，并不是老一辈对摇滚乐会带来的所有变化的预测都错了;而是他们错估计了摇滚乐的危害有多大。人们会适应。当每个人都留下了自出生以来的个人想法的公共数字痕迹时，没有人会对它的存在三思而后行。如果科技意味着我们所说的一切——令人遗憾的指责、陈词滥调，所有的一切——都将被永久记录和保存，

我们要学会接受这个事实。

问题是，我们太善于适应了，至少在短期内是这样。在监控更多的环境下长大的人，会更适应这种环境。我们有些人上学的时候，有身份检查和金属探测器。我们中的一些人在需要每天检查徽章的大楼里工作。我们大多数在美国乘坐飞机的人现在都接受运输安全管理局的检查。我们所有购物的人都不再对大量信用卡号码被盗感到惊讶。这些都是我们习惯于失去隐私的方式。像许多基本权利一样，隐私是只有当它消失时才会被注意到的东西之一。这是很不幸的，因为一旦它消失了，就很难重新获得了。

我们必须阻止这种下滑。从根本上说，对隐私的争论是一个道德问题。这是我们应该拥有的东西——不是因为它有利可图或效率高，而是因为它是道德的。大规模监控应该被扔进历史的垃圾箱，就像其他许多人类曾经认为正常、但现在被普遍认为令人憎恶的做法一样。隐私是一项人权。这并不是一个新想法。《世界人权宣言》(1948年)和《欧洲人权公约》(1970年)确认隐私权是一项基本权利。

美国宪法中也有——虽然没有明确规定，但在第四、第五和第九修正案中有所暗示。这是2000年《欧洲联盟基本权利宪章》的一部分。2013年，联合国大会通过了一项题为“数字时代的隐私权”的决议，肯定了我们的基本隐私权线上线下都适用，大规模监控的风险破坏了这一权利。

这些原则在国内法和国际法中都有明文规定。我们需要开始遵循这些原则。隐私不是只有在安全的时候我们才能负担得起的奢侈品。相反，它是一种需要保护的价值。它对自由、自主性和人类尊严至关重要。我们必须明白，隐私不是为了某种可怕的保证安全的企图而可以出卖的东西，而是为了获得真正的安全而需要维护和保护的东西。

欧洲联盟基本权利宪章(2000年)

ARTICLE:尊重私人和家庭生活。人人有权尊重他或她的私人和家庭生活、家庭和通讯。

ARTICLE:个人资料的保护。1. 每个人都有权保护有关他或她的个人资料。2. 此类数据必须出于特定目的，在当事人同意或法律规定的其他合法依据的基础上进行公平处理。每个人都有权查阅收集到的与他或她有关的数据，并有权要求纠正这些数据。3. 本规则的遵守应受一个独立机构的监督。

如果不改变态度，这一切都不会发生。最终，我们将得到我们作为一个社会所需要的隐私，而不是更多。

不要再等了

我们等待改变的时间越长，改变就会变得越困难。在企业方面，无处不在的跟踪和个性化广告已经成为常态，企业有强大的游说力量来阻止任何改变这一现状的尝试。加州的Do Not

赛道法就是一个例子:它一开始是个好主意，但随着时间的推移，它被彻底摧毁了。监控技术的自然发展轨迹(还记得第2章中提到的成本下降吗?)和新现状的确立，将使变革在未来更难实现，尤其是在美国。

反对变革的不只是企业。政客们喜欢的数据和商业广告商一样:人口统计数据、个人消费者偏好信息、政治和宗教信仰。他们在竞选活动中使用这些数据，并且不想放弃这些数据。说服他们放弃访问数据，以帮助他们进行有针对性的信息传递和动员投票活动，将是困难的。一旦有人弄清楚如何利用这些数据使选举永远不公平，就像不公正地划分选区一样，改变将更加困难。

在去年的一次会议上，我无意中听到有人说，“谷歌Analytics是互联网监控领域的可卡因。一旦你看到它，你就永远不想放弃它。”更普遍的是，数据成为它自己的正当化。我们等待的时间越长，就会有越多的人和组织习惯于广泛访问我们的数据，他们就会越努力地维护这种访问权。

我们正处于一个独特的时期，可以做出我在本书中推荐的各种改变。

收集和转售我们数据的行业很强大，但它们仍然相对较新。随着它们的成熟和更加根深蒂固，要在它们的经营方式上做出重大改变将会困难得多。

斯诺登揭露了美国NSA和政府通信总部的行为，迫使政府监控成为人们关注的焦点。这在世界各国之间，尤其是德国和美国之间，造成了一些特殊的紧张关系。在美国，这种政治紧张关系跨越了传统的党派分歧。这是一个实现真正变革的机会。正如芝加哥市长、奥巴马前幕僚长拉姆·伊曼纽尔所说，“你永远不希望浪费一场严重的危机。”这句话在这里是千真万确的，即使大多数人没有意识到这是一场危机。

我们正处于美国和欧盟关系的一个独特时刻。双方都希望协调这类事情的规则，使跨境贸易更容易。事情可能以两种方式发展:欧洲可能变得更加宽松，以赶上美国;或者美国可能变得更加严格，以赶上欧洲。一旦这些规则变得平等，它们将更难改变。

我们也正处于信息时代发展的独特时期。互联网正在融入一切事物。我们暂时可以看到这些系统。我们现在可以做出的改变将持续几十年。

即便如此，我们也需要做好重新来过的准备。

技术在不断变化，使新事物成为可能，旧的法律被淘汰。我们没有理由认为，那些保护我们免受今天威胁的安全、隐私和匿名技术，也能抵御明天的威胁。

政治现实也会改变，法律也会随之改变。相信任何

我们今天建立的一套解决方案将永远有效，甚至可以维持半个世纪。回顾美国近代史就会发现，行政权力的严重滥用——以及由此引发的重大公共丑闻和缓和改革——每隔25至30年就会发生一次。想想20世纪20年代的帕尔默突袭(Palmer Raids)、50年代的麦卡锡主义(mccarthy)、70年代国家安全局(NSA)和联邦调查局(FBI)的滥用职权，以及21世纪头十年911事件后持续不断的滥用职权。

仔细想想，30年大概是一个专业公务员的职业生涯长度。我猜，这并不是巧合。似乎发生的事情是，我们进行改革，我们暂时记得我们实施这些改革的原因，然后最终有足够多的人在政府中更换，我们开始忘记。然后我们撤销改革，不得不在新的技术背景下重新做所有的事情。

然而，下一组滥用是下一代人要考虑的。这是我们的问题。

我担心我们无法胜任:这是一代人的问题，需要下一代来推动必要的社会变革，制定保护我们基本隐私的政策变化。我担心，目前掌权的这一代人太害怕恐怖分子，太急于满足企业的任何要求。我希望我是错的。

大数据的取舍

这本书的大部分内容都是关于我们个人数据的误用和滥用，但事实是，这些数据也为社会提供了难以置信的价值。

当我们把所有的数据放在一起的时候，我们的数据具有巨大的价值。我们的运动记录有助于城市规划。我们的财务记录使警方能够发现和防止欺诈和洗钱。我们的帖子和推文帮助研究人员了解我们作为一个社会是如何运作的。个人数据有各种各样的创造性和有趣的用途，这些用途产生了新知识，使我们的生活变得更美好。

我们的数据对我们每个人个人来说也是有价值的，可以按照自己的意愿隐藏或披露。这就是问题所在。使用数据使群体利益与自身利益对立，这是人类自诞生以来一直在努力解决的核心紧张关系。

还记得我在引言中谈到的讨价还价吗?政府向我们提供了这样的交易:如果你让我们拥有你所有的数据，我们可以保护你免受犯罪和恐怖主义的侵害。这是敲竹杠。行不通。而且它以牺牲个人安全为代价，过分强调群体安全。

谷歌提供给我们的交易也是类似的，而且同样是不平衡的:如果你让我们拥有你所有的数据并放弃你的隐私，我们会向你展示你想看的广告——我们还会提供免费的网络搜索、电子邮件和各种其他服务。只有当足够多的人放弃自己的隐私时，b谷歌和Facebook这样的公司才能达成这种交易。只有在足够多的人默许的情况下，这个群体才能受益。

并非所有集体利益对抗个人利益的交易都是如此不公平的交易。医学界即将与我们达成类似的交易:让我们拥有你所有的健康数据，我们将用它来彻底改变医疗保健，改善人们的生活

每个人。在这种情况下，我认为他们是对的。我认为没有人能理解，把我们所有的健康数据放在一个单一的数据库中，让研究人员访问它，会给人类带来多少好处。当然，这些数据是非常私人的，必然会落入意想不到的人手中，被用于意想不到的目的。但在这个特殊的例子中，在我看来很明显，数据的公共使用应该优先考虑。其他人不同意。

这是另一个在群体和个人利益之间取得平衡的案例。社交媒体研究员雷诺·Junco分析了他的学生的学习习惯。许多教科书都在网上，教科书网站收集了大量关于学生如何以及多久与课程材料互动的数据。Junco通过监视学生的其他电脑活动来增强这些信息。这是一项令人难以置信的侵入性研究，但持续时间有限，他对好学生和坏学生的学习方式有了新的认识，并开发了旨在改善学生学习方式的干预措施。这项研究的群体利益是否超过了参与研究的受试者的个人隐私利益?

Junco的实验对象同意接受监控，他的研究也得到了大学伦理委员会的批准——但是由公司进行的实验呢?约会网站OKCupid多年来一直在其用户身上进行实验，有选择地显示或隐藏照片，放大或缩小兼容性指标，以观察这些变化如何影响人们在网站上的行为。你可以说，我们已经从这个实验中吸取了教训，但在不知情或未经允许的情况下，以这种方式操纵人们很难站得住脚。

一次又一次，都是同样的张力:群体价值vs个人价值。我们的集体数据对于评估社会项目的有效性是有价值的。我们的集体数据对市场研究也有价值。这对改善政府服务也有价值。研究社会趋势并预测未来趋势也是有价值的。我们必须权衡这些好处与监控带来的风险。

最大的问题是:我们如何设计系统，利用我们的数据集体造福整个社会，同时保护每个人?或者，用博弈论的术语来说，我们如何找到数据收集的“纳什均衡”:即使放弃任何一个方面的优化，也能创造出最优的整体结果的平衡?

就是这样:这是信息时代的根本问题。我们可以解决它，但这需要仔细思考具体问题，并对不同的解决方案如何影响我们的核心价值观进行道德分析。

我遇到过一些坚定的隐私倡导者，尽管如此，他们仍然认为，不把你的医疗数据放入一个全社会范围的数据库中，应该是一种犯罪。我也遇到过一些人，他们对允许企业进行最私密的监控完全没有意见，但希望政府永远不能接触到这些数据。我也遇到过一些人，他们对政府的监控没有意见，但反对任何带有利润动机的行为。我也遇到过很多人，他们对上述任何一种都没有意见。

作为个人和社会，我们一直在努力平衡我们不同的价值观。我们从来没有完全做到正确。重要的是我们有意识地参与这个过程。这种平衡往往是由政府和企业按照自己的议程为我们完成的。

无论我们的政治立场如何，我们都需要参与其中。我们不希望联邦调查局(FBI)和国家安全局(NSA)秘密决定我们手机的默认政府监控级别;我们希望国会在公开和公开的辩论中决定这些问题。我们不希望中国和俄罗斯政府决定在互联网上建立什么样的审查能力;我们希望有一个国际标准机构来做这些决定。我们不希望Facebook来决定我们在朋友之间享有的隐私程度;我们要自己决定。所有这些决定都比任何一个组织更大、更重要。它们需要由一个更大、更具代表性和包容性的机构来做出。我们希望公众能够就这些事情进行公开辩论，“我们人民”能够让决策者承担责任。

我经常引用小马丁·路德·金牧师(Rev. Martin Luther King Jr .)的一句话:“历史的弧线很长，但它会向正义倾斜。”尽管我在短期内仍然悲观，但我长期乐观。我认为我们会克服恐惧，学会如何重视自己的隐私，并制定规则，在获得大数据好处的同时，保护自己免受一些风险的影响。现在，我们正在看到一场非常强大的全球运动的开始，它将隐私视为一项基本人权，而不仅仅是我们在许多公开声明中看到的抽象意义上的隐私，而是以一种有意义和可执行的方式。欧盟正在引领这一潮流，但其他国家也将紧随其后。这个过程可能需要数年，甚至数十年，但我相信，在半个世纪后，人们看待今天的数据实践的方式将与我们现在看待租户农业、童工和公司商店等古老商业行为的方式相同。它们会被认为是不道德的。这场运动的开端，最重要的将是爱德华·斯诺登(Edward Snowden)的遗产。

在这本书的开头，我谈到了数据就像废气:我们在信息时代的商业活动中都会产生的东西。我想我可以把这个类比更进一步。数据是信息时代的污染问题，保护隐私是环境的挑战。几乎所有的电脑都会产生个人信息。它留在周围，溃烂。我们如何处理它——如何控制它以及如何处理它——是我们信息经济健康的核心。正如我们今天回顾工业时代最初的几十年，想知道我们的祖先如何在匆忙建立一个工业世界的过程中忽视污染一样，我们的孙子们将回顾信息时代最初的几十年，并根据我们如何应对数据收集和滥用的挑战来评判我们。

我们应该努力让他们引以为豪。

致谢

对我来说，写书就是对一个话题的探索。在写完之前，我不知道自己会在哪里结束。这让我的书很难卖出去。我无法提供大纲。我甚至不能确定这本书是关于什么的。出版商一般不太喜欢这个。

首先，我要感谢我的经纪人，Susan Rabiner文学代理公司的Eric Nelson，在我的书还没出书之前，他就代理了我的书。他相信他可以把“下一本施奈尔的书”卖给主流出版商，并且如此相信，以至于他在开始之前没有要求任何正式的协议。

其次，我要感谢我的编辑，诺顿出版社的杰夫·施里夫。他愿意买“下一本施奈尔的书”，但只含糊地保证书的内容。而且他也愿意接受我的写作过程。

我不从头到尾写书。我是从下往上写的。我的意思是，我每时每刻都在同时写整本书。这有两个奇怪的效果。第一，在我开始写作后，这本书很快就完成了。它不是很好，随着我继续写，它会越来越好。只要我继续写，它就会不断提高。第二，如果允许的话，我会一直写下去，不断改进这本书。我所做的就是武断地将“完成”定义为书到期的那一刻。

这个过程可以让我在整个过程中得到关于这本书的详细反馈。很多人会阅读全部或部分手稿:罗斯·安德森、史蒂夫·巴斯、卡斯帕·鲍登、科迪·查雷特、大卫·坎贝尔、凯伦·库珀、多萝西·丹宁、科里·多克托罗、瑞安·埃利斯、艾迪森·菲舍尔、卡米尔·弗朗索瓦、娜奥米·吉伦斯、约翰·吉尔摩、杰克·戈德史密斯、鲍勃·古尔利、比尔·赫德尔、黛博拉·赫尔利、克里斯玛·杰克逊、雷诺·琼科、约翰·凯尔西、亚历山大·克林伯格、大卫·莱瓦里、斯蒂芬·利、哈里·刘易斯、李君、刘肯、亚历克斯·卢米斯、萨沙·迈因拉斯、阿莱西亚·m·麦克唐纳、巴勃罗·莫利纳、拉米兹·纳姆、彼得·诺伊曼、约瑟夫·奈、克里斯滕·潘恩、大卫·佩里、利亚·普伦基特、大卫·普伦蒂斯、巴拉特·拉加万、马克·罗滕伯格、马丁·施奈尔、塞斯·大卫·舍恩、亚当·肖斯塔克、彼得·斯威尔、基特·沃尔什、萨拉·m·沃森、大卫·温伯格、达斯汀·温泽尔、玛西·惠勒、理查德·威利、本·维茨纳、约瑟芬·沃尔夫、乔纳森·齐特兰和肖莎娜·祖伯夫。他们每个人都给了我建议，我把这些建议都写进了书里。

有几个人在写这本书的过程中发挥了不可估量的作用。Kathleen Seidel是我找到的最好的研究者，我再也无法想象没有她的帮助我能写一本书。Rebecca Kessler也是如此，她在我的写作过程中两次编辑了这本书，每次都给了我批评性的建议。贝丝·弗里德曼(Beth Friedman)，十多年来为我编辑了所有的作品，仍然是不可替代的。

我还要感谢爱德华·斯诺登(Edward Snowden)，他的勇敢行动引发了我们现在对监控的全球讨论。可以毫不夸张地说，如果没有他的所作所为，我就不会写这本书。另外，作为一名长期的NSA监视人员，阅读那些绝密文件也挺酷的。

关于标题的说明。我的编辑和我都立刻喜欢上了*《数据》和《歌利亚》*，但是

有一个问题。马尔科姆·格拉德威尔最近出版了一本名为《*大卫与歌利亚*》*的书*。这还不算太糟，但我上一本书的名字是《*说谎者和异类*》;它紧随格拉德威尔的上一本书《*异类*》*出版*。模仿他两次似乎太过分了。今年4月，我在博客上解释了我的困境，然后突然收到了格拉德威尔的一封电子邮件，他说:“我喜欢数据和巨人!:-)”所以在他的祝福和宣传下，我的标题保留了下来。

我在哈佛法学院伯克曼互联网与社会研究所(Berkman Institute for Internet and Society)工作时写了这本书，我对那里的每一个人都感激不尽。和我一起度过时光的其他研究员和各种哈佛教授帮助我思考了这些问题，我在2014年春季带领的阅读小组的学生也是如此。此外，自2014年1月以来，我一直是Resilient Systems的首席技术官，我也必须感谢他们。尽管这本书与我们在公司所做的事情没有直接关系，但我被赋予了写作的自由。

最后，我要感谢我的朋友们，尤其是我的妻子凯伦·库珀，感谢她对我“写书”模式的容忍。我知道，这一次比上一次容易，但仍然很辛苦。

谢谢大家。

笔记

引言

大卫J.克兰德尔等人(2010年12月8日), “从地理巧合推断社会关系”,《*美国国家科学院院刊*》107,http://www.pnas.org/content/107/52/22436.short。

累积的数据:德国政治家马尔特·施皮茨(Malte Spitz)通过向记者提供六个月的每日行踪记录，展示了地理定位数据的力量。时代在线(2011年3月), “泄密电话”，*时代在线*，http://www.zeit.de/datenschutz/malte-spitz-data-retention。

Manlio De Domenico, Antonio Lima和Mirco Musolesi(2012年6月18-19日),
“人类移动性和社会互动的相互依赖和可预测性”，诺基亚移动数据挑战研讨会，英国纽卡斯尔，http://www.cs.bham.ac.uk/research/projects/nsl/mobility-prediction。

手机位置分析:将手机信号塔数据与实际记录的窃听音频相协调，在法庭上是非常有力的证据，证明被告不可信，因为可以通过他自己的话证明他在撒谎。在2002年斯科特·彼得森的情妇安珀·弗雷与警方合作后，这类证据帮助斯科特·彼得森被判谋杀他的妻子。美联社(2004年8月27日), “彼得森案的证词转向电脑证据”，《*今日美国*》，http://usatoday30.usatoday.com/news/nation/2004-08-27-peterson_x.htm。

警察可以“ping”: Evan Perez和Siobhan Gorman(2013年6月15日), “手机留下的线索”，*华尔街日报*，http://online.wsj.com/news/articles/SB10001424127887324049504578545352803220058。Trevor Hughes(2013年12月7日), “手机数据帮助解决拉里默县的两起谋杀案”，*Coloradoan*, http://archive.coloradoan.com/article/20131207/NEWS01/312070068/Cellphone-data-aided-solving-two-Larimer-County-murders。

警方正在使用这些数据:但他们夸大了数据的准确性，并根据这些数据给无辜的人定罪。*经济学人*(2014年9月6日), “双塔”，*经济学人*，http://www.economist.com/news/unitedstates/21615622-junk-science-putting-innocent-people-jail-two-towers。Mike Masnick(2014年9月6日), “事实证明手机位置数据甚至不接近准确，但每个人都相信它，”*Tech Dirt*, https://www.techdirt.com/articles/20140908/04435128452/turns-out-cell-phone-location-data-is-not-even-close-to-accurate-everyone-falls-it.shtml。

乌克兰政府:Heather Murphy(2014年1月22日), “发给基辅抗议者的不祥短信让互联网发冷”,《*纽约*时报》，*the Lede*, http://thelede.blogs.nytimes.com/2014/01/22/ominous-text-message-sent-to-protesters-in-kiev-sends-chills-around-the-internet。

密歇根警方寻求信息: Michael Isikoff(2010年2月18日), “FBI在没有搜查令的情况下追踪嫌疑人的手机”，*新闻周刊*，http://www.newsweek.com/fbi-tracks-suspects-cell-phones-without-warrant-75099。

公司使用你的手机: Steve Olenski(2013年1月17日), “基于位置的广告是移动营销和移动广告的未来吗?”《*福布斯*》，http://www.forbes.com/sites/marketshare/2013/01/17/is-locationbased-advertising-the-future-of-mobile-marketing-and-mobile-advertising。John McDermott(2014年2月20日), “为什么网络上最大的玩家正在吞噬基于位置的应用程序，”*Digiday*, http://digiday.com/platforms/applegoogle-microsoft-yahoo-are-betting-on-mobile。

位置数据非常有价值: Anton Troianovski(2013年5月21日), “电话公司出售客户数据”,《*华尔街*日报》，http://online.wsj.com/news/articles/SB10001424127887323463704578497153556847658。Rachel King(2013 年 7 月 13 日), “ACLU: AT&T客户隐私面临风险”，*CIO* Journal，*华尔街日报博客*，http://blogs.wsj.com/cio/2013/07/13/aclu-att-customer-privacy-at-risk。

sennetworks等公司:hiwatha Bray(2013年7月13日), 《挖掘手机数据创建个人档案》，《*波士顿环球报*》，http://www.bostonglobe.com/business/2013/07/07/your-cellphoneyourself/eSvTK1UCqNOE7D4qbAcWPL/story.html。

Verint销售手机跟踪系统: Craig Timberg(2014年8月24日), “出售:可以秘密追踪全球手机用户行踪的系统,《*华盛顿*邮报》，http://www.washingtonpost.com/business/technology/for-sale-systems-that-can-secretly-track-where-cellphone-users-go-around-the-globe/2014/08/24/f0700e8a-f003-11e3-bf76-447a5df6411f_story.html。

公司网站: Verint(2014), “关于Verint”，http://www.verint.com/about。

“盲目”打电话:Privacy International(2012), “Cobham销售监控中心，电话监控,

技术监控和位置监控技术。英国出口法并没有具体规范这些技术，所以它们很容易落入坏人之手，”https://www.privacyinternational.org/sii/cobham。

该**公司自豪地说:**截至2011年，完整的名单是阿尔及利亚、澳大利亚、奥地利、比利时、文莱、捷克共和国、格鲁吉亚、加纳、爱尔兰、科威特、利比亚、挪威、巴基斯坦、沙特阿拉伯、新加坡、斯洛伐克共和国、西班牙、瑞典、台湾、土耳其、英国和美国。Cobham(2011)，“战术C4I系统:鹰-近距离战斗无线电(CCR)”，https://s3.amazonaws.com/s3.documentcloud.org/documents/409237/115-cobham-tactical-c4i.pdf。

Craig Timberg(2014年8月24日)，“出售:可以秘密追踪全球手机用户行踪的系统”，*华盛顿邮报*，http://www.washingtonpost.com/business/technology/forsale-systems-that-can-secretly-track-where-cellphone-users-go-around-the-globe/2014/08/24/f0700e8a-f003-11e3-bf76-447a5df6411f_story.html。

Tobias Engel演示: Tobias Engel(2009年1月9日)，“使用7号信号系统定位移动电话”，Chaos Computer Club, http://berlin.ccc.de/~tobias/25c3-locating-mobile-phones.pdf。

收集并出售: Kevin J. O 'Brien(2012年10月28日)，“通过应用程序收集数据呈现灰色法律区域”，*纽约*时报，http://www.nytimes.com/2012/10/29/technology/mobile-apps-have-a-ravenous-ability-to-collect-personaldata.html。

HelloSpy是一个应用程序:有相当多这样的跟踪应用程序在那里。HelloSpy尤其明显。虽然主页上的免责声明说它是为“父母的道德间谍”而设计的，或者是在“你拥有或获得适当同意进行监控的移动设备上”使用，但文献中也大肆宣扬它能够以“隐身模式”运行，并有一个专门的页面专门讨论婚姻不忠。详见http://hellospy.com。

偷窥妻子或女友: StealthGenie是另一款间谍软件。2014年，该公司首席执行官因在美国销售该软件而被起诉并被捕。Craig Timberg和马特·萨帕托斯利(2014年9月29日)，《用于间谍活动的应用程序StealthGenie的开发者在弗吉尼亚州被起诉》,*华盛顿*邮报，http://www.washingtonpost.com/business/technology/make-ofapp-used-for-spying-indicted-in-virginia/2014/09/29/816b45b8-4805-11e4-a046-120a8a855cca_story.html。

监视员工:Spencer E. Ange和Lauren Weber(2013年10月22日)，《给员工的备忘录:老板在监视》，《*华尔街*日报》http://online.wsj.com/news/articles/SB10001424052702303672404579151440488919138。

手机定位数据: Barton Gellman和Ashkan Soltani(2013年12月4日)，“NSA追踪全球手机位置，斯诺登文件显示”，*华盛顿*邮报，http://www.washingtonpost.com/world/nationalsecurity/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html。Ashkan Soltani和Barton Gellman(2013年12月10日)，“新文件显示NSA如何根据移动位置数据推断关系，”*华盛顿邮报*，http://www.washingtonpost.com/blogs/the-switch/wp/2013/12/10/new-documents-show-how-the-nsa-infers-relationships-based-on-mobile-location-data。James Glanz, Jeff Larson和Andrew W. Lehren(1月27日)，“间谍机构从手机应用程序中获取数据流”，*纽约时报*，http://www.nytimes.com/2014/01/28/world/spyagencies-scour-phone-apps-for-personal-data.html。

即使它们被关闭:我们不能确切地知道这是否属实。Dana Priest(2013年7月22日)，《*华盛顿邮报*》，http://www.washingtonpost.com/world/national-security/nsa-growth-fueled-by-need-to-target-terrorists/2013/07/21/24c93cf4-f0b1-11e2-bed3-b9b6fe264871_story.html，“NSA的增长受到打击恐怖分子需求的推动”。Ryan Gallagher(2013年7月22日)，“据报道，NSA即使在关机的情况下也能追踪手机，”*Slate*, http://www.slate.com/blogs/future_tense/2013/07/22/nsa_can_reportedly_track_cellphones_even_when_they_re_tur

监控的黄金时代:据我所知，这是Peter Swire的说法。Peter Swire和Kenesa Ahmad(2011年11月28日)，“走向黑暗”与“监控的黄金时代”，民主与技术中心，http://www.futureofprivacy.org/wp-content/uploads/Going-Dark-Versus-a-Golden-Age-for-Surveillance-Peter-Swire-and-Kenesa-A.pdf。

“反正你的**隐私为零**。: Polly Sprenger(1999年1月26日)，“隐私的太阳:‘克服它’，”*Wired*, http://archive.wired.com/politics/law/news/1999/01/17538。

美国军方定义监视:美国参谋长联席会议(2011年8月11日)，“联合作战”，联合出版物3-0,http://fas.org/irp/doddir/dod/jp3_0.pdf。

如果你让我们拥有你所有的数据:埃里克·施密特和贾里德·科恩(2013),《*新数字时代:重塑人民、国家和商业的未来*》,克诺夫,http://www.newdigitalage.com。

这就是NSA的**正当化:**从来没有人明确提到过这笔交易，但每个人都认为监控

是保证我们安全的必要手段。Patricia Zengerle和Tabassum Zakaria(2013年6月18日), “NSA局长，立法者为监控项目辩护”，路透社，http://www.reuters.com/article/2013/06/18/us-usa-securityidUSBRE95H15O20130618。半岛电视台(2013年10月22日), “面对盟友的抗议，NSA局长为间谍项目辩护”，半岛电视台，http://america.aljazeera.com/articles/2013/10/29/nsa-chiefdefendsspyprogramamidusriftwitheurope.html。

我们需要思考:技术评论家叶夫根尼·莫罗佐夫指出了这一点。叶夫根尼·莫罗佐夫(2013年10月22日), “真正的隐私问题”，*麻省理工科技评论*，http://www.technologyreview.com/featuredstory/520426/the-realprivacy-problem。

1:数据作为计算的副产品

唯一标识你的电脑: Peter Eckersley(2010年7月), “你的网络浏览器有多独特?”*第十届隐私增强技术国际会议论文集*，柏林，https://panopticlick.eff.org/browseruniqueness.pdf。

Paul A. Zandbergen(2009年6月26日), “iPhone定位的准确性:辅助GPS、WiFi和蜂窝定位的比较”，《*地理信息系统事务*》第13期，http://onlinelibrary.wiley.com/doi/10.1111/j.1467-9671.2009.01152.x/abstract。Paul A. Zandbergen和Sean J. Barbeau(2011年7月), “来自高灵敏度GPS手机的辅助GPS数据的定位精度”，《*导航杂志*》64期，http://www.paulzandbergen.com/files/Zandbergen_Barbeau_JON_2011.pdf。

现代汽车装载了电脑: Ben Wojdyla(2012年2月21日), “它是如何工作的:你车里的电脑”，*Popular* Mechanics, http://www.popularmechanics.com/cars/how-to/repair/how-it-works-the-computer-insideyour-car。

其中大部分都是自动记录的: Nate Cardozo(2013年2月11日), “汽车中的强制黑匣子引发隐私问题”，电子前沿基金会，https://www.eff.org/press/releases/mandatory-black-boxes-carsraise-privacy-questions。

自动驾驶汽车: Lucas Mearian(2013年7月23日), “自动驾驶汽车每秒可以产生1GB的数据”，*Computer World*, http://www.computerworld.com/s/article/9240992/Self_driving_cars_could_create_1GB_of_data_a_second。

嵌入到数码照片中:Benjamin Henne, Maximilian Koch和Matthew Smith(2014年3月3-7日), “关于共享照片元数据的意识、控制和隐私”，莱布尼茨大学分布式计算与安全小组，在巴巴多斯举行的第十八届金融密码学和数据安全国际会议上发表，http://ifca.ai/fc14/papers/fc14_submission_117.pdf。

15如果你上传照片:这是一个关于相机元数据的特别令人毛骨悚然的故事。马修·霍南(2009年1月19日), “我在这里:一个人对位置感知生活方式的实验”，《*连线*》，http://www.wired.com/gadgets/wireless/magazine/17-02/lp_guineapig。

自动支付系统，如EZPass:越来越多的政府正在取消匿名现金的选择。Adrianne Jeffries(2013年3月27日), “金门大桥新的无现金收费公路承诺以隐私换取便利，”*Verge*, http://www.theverge.com/2013/3/27/4150702/golden-gate-bridges-new-cashlesstollway-promises-convenience-for-privacy。Anh Do(2014年3月20日), “奥兰治县的收费公路走向无现金化”，《*洛杉矶*时报》，http://www.latimes.com/local/lanow/la-me-ln-cashless-toll-roads-20140320-story.html。Trevor Pettiford(2014年6月13日), “退伍军人高速公路收费站将开始无现金化”，*Bay News* 9, http://www.baynews9.com/content/news/baynews9/news/article.html/content/news/articles/bn9/2014/6/13/veterans_Martine Powers(2014年7月17日), “从周一开始，托宾收费站将不再收现金。”《*波士顿环球报*》，http://www.bostonglobe.com/metro/2014/07/16/starting-monday-more-cash-tobin/WZKMDilsfLULQtYiGZCrEK/story.html。

智能恒温器: Nest(2012), “Nest学习型恒温器”http://certified.nest.com/resources/NEST_POS_brochure_r7_300.pdf。

智能冰箱:伊丽莎·巴克莱(Eliza Barclay, 2012年5月4日), “‘智能冰箱’找到了丢失的生菜，*这是有代价的*”，《*盐:你盘子里有什么*》，NPR, http://www.npr.org/blogs/thesalt/2012/05/03/151968878/the-smart-fridge-finds-thelost-lettuce-for-a-price。

智能空调:Ry Crist(2014年1月8日), “海尔的新空调是第一款获得苹果认证的家电”，*CNET*, http://ces.cnet.com/8301-35306_1-57616915/haiers-new-air-conditioner-is-the-first-applecertified-home-appliance。

智能烟雾和一氧化碳探测器:希瑟·凯利(2014年1月15日), “谷歌想用Nest管理你的家，”CNN, http://www.cnn.com/2014/01/15/tech/innovation/google-connect-home-nest。

智能电网:美国能源部(2008), “智能电网:介绍”，

http://energy. gov/sites/prod/files/oeprod/DocumentsandMedia/DOE_SG_Book_Single_Pages(1). pdf. US Department of Energy (2014), "What is the smart grid?" https://www.smartgrid.gov/the_smart_grid.

when you're having sex: Gregory Ferenstein, "How health trackers could reduce sexual infidelity," *Tech Crunch*, http://techcrunch.com/2013/07/05/how-health-trackers-could-reduce-sexual-infidelity.

Give the device more information: Fitabase (3 Dec 2013), "Privacy policy," http://www.fitabase.com/Privacy.
Many medical devices: Sarah E. Needleman (14 Aug 2012), "New medical devices get smart," *Wall Street Journal*, http://online.wsj.com/news/articles/SB10000872396390444318104577587141033340190.

It's not just specialized devices: Sara M. Watson (10 Oct 2013), "The latest smartphones could turn us all into activity trackers," *Wired*, http://www. wired. com/2013/10/the-trojan-horse-of-the-latest-iphone-with-the-m7-coprocessor-we-all-become-qs-activity-trackers.

Companies like 23andMe: Thomas Goetz (17 Nov 2007), "23AndMe will decode your DNA for $1,000. Welcome to the age of genomics," *Wired*, http://www.wired.com/medtech/genetics/magazine/15-12/ff_genomics. Elizabeth Murphy (14 Oct 2013), "Inside 23andMe founder Anne Wojcicki's $99 DNA revolution," *Fast Company*, http://www.fastcompany.com/3018598/for-99-this-ceo-can-tell-you-what-might-kill-you-inside-23andme-founder-anne-wojcickis-dna-r.

personalized marketing: Charles Seife (27 Nov 2013), "23andMe is terrifying, but not for the reasons the FDA thinks," *Scientific American*, http://www.scientificamerican.com/article/23andme-is-terrifying-but-not-for-reasons-fda.

insurance companies may someday buy: Rebecca Greenfield (25 Nov 2013), "Why 23andMe terrifies health insurance companies," *Fast Company*, http://www. fastcompany. com/3022224/innovation-agents/why-23andme-terrifies-health-insurance-companies.

lifelogging apps: Leo Kelion (6 Jan 2014), "CES 2014: Sony shows off life logging app and kit," *BBC News*, http://www.bbc.com/news/technology-25633647.

it will include a video record: Alec Wilkinson (28 May 2007), "Remember this? A project to record everything we do in life," *New Yorker*, http://www.newyorker.com/reporting/2007/05/28/070528fa_fact_wilkinson.

Google Glass is the first wearable device: Jenna Wortham (8 Mar 2013), "Meet Memoto, the lifelogging camera," *New York Times Blogs*, http://bits.blogs.nytimes.com/2013/03/08/meet-memoto-the-lifelogging-camera.

Internet of Things: Ken Hess (10 Jan 2014), "The Internet of Things outlook for 2014: Everything connected and communicating," *ZDNet*, http://www.zdnet.com/the-internet-of-things-outlook-for-2014-everything-connected-and-communicating-7000024930.

smart cities: Georgina Stylianou (29 Apr 2013), "Idea to have sensors track everything in city," *Press* (Christchurch), http://www. stuff. co. nz/the-press/business/the-rebuild/8606956/Idea-to-have-sensors-track-everything-in-city. Victoria Turk (Jul 2013), "City sensors: the Internet of Things is taking over our cities," *Wired*, http://www.wired.co.uk/magazine/archive/2013/07/everything-is-connected/city-sensors.

smart toothbrushes: Sam Byford (5 Jan 2014), "Kolibree's smart toothbrush claims to track and improve your dental hygiene," *Verge*, http://www.theverge.com/2014/1/5/5277426/kolibree-smart-toothbrush.

smart light bulbs: Margaret Rhodes (23 Sep 2014), "Ex-Tesla and NASA engineers make a light bulb that's smarter than you," *Wired*, http://www. wired. com/2014/09/ex-tesla-nasa-engineers-make-light-bulb-thats-smarter.

smart sidewalk squares: Charles Stross has discussed the implications of these. Charles Stross (25 Jun 2014), "YAPC::NA 2014 keynote: Programming Perl in 2034," *Charlie's Diary*, http://www.antipope.org/charlie/blog-static/2014/06/yapcna-2014-keynote-programmin.html.

smart pill bottles: Valentina Palladino (8 Jan 2014), "AdhereTech's smart pill bottle knows when you take, and miss, your medication," *Verge*, http://www.theverge.com/2014/1/8/5289022/adheretech-smart-pill-bottle.

smart clothing: Econocom (19 Sep 2013), "When fashion meets the Internet of Things," *emedia*, http://blog.econocom.com/en/blog/when-fashion-meets-the-internet-of-things. Michael Knigge (28 Aug 2014), "Tagging along: Is Adidas tracking soccer fans?" *Deutsche Welle*, http://www.dw.de/tagging-along-is-adidas-tracking-soccer-fans/a-1788463.

because why not?: We've seen this trend before. Digital clocks first became popular in the 1970s. Initially they were largely stand-alone devices—alarm clocks and watches—but as their price declined, they became embedded into other things: first your microwave, then your coffeepot, oven, thermostat, VCR, and television. Internet-enabled sensors are heading in that direction.

Natasha Lomas(2013年5月9日), “ABI Research表示，今天的无线连接设备超过100亿，2020年的‘万物互联’将超过300亿”, *Tech Crunch*, http://techcrunch.com/2013/05/09/internet-of-everything。

The hype level is pretty high: Valentina Palladino (10 Jan 2014), “Invisible intelligence: How tiny sensors could connect everything we own,” *Verge*, http://www.theverge.com/2014/1/10/5293778/invisible-intelligence-tiny-sensors-that-connect-everything.

eyes and ears of the Internet: Ben Hammersley (Jul 2013), “When the world becomes the Web,” *Wired*,

http://www. wired. co. uk/magazine/archive/2013/07/everything-is-connected/when-the-world-becomes-the-web. **Smart streetlights will gather data:** Newark Airport has installed these. Diane Cardwell (17 Feb 2014), “At Newark Airport, the lights are on, and they’re watching you,” *New York Times*,

http://www. nytimes. com/2014/02/18/business/at-newark-airport-the-lights-are-on-and-theyre-watching-you. html. **Cameras will only get better:** Olga Kharif (31 Oct 2013), “As drones evolve from military to civilian uses, venture capitalists move in,” *Washington Post*, http://www.washingtonpost.com/business/as-drones-evolve-from-military-to-civilian-uses-venture-capitalists-move-in/2013/10/31/592ca862-419e-11e3-8b74-

d89d714ca4dd_story.html.

Raytheon is planning to fly a blimp: Paul McLeary (29 Jun 2014), “Powerful radar blimp to surveil Washington, Baltimore, out to sea,” *Defense News*,

http://www.defensenews.com/article/20140629/DEFREG02/306290012/Powerful-Radar-Blimp-Surveil-

Washington-Baltimore-Out-Sea.

An e-mail system is similar: Some of that argument is here. Electronic Frontier Foundation (2014), “The government’s word games when talking about NSA domestic spying,” https://www. eff. org/nsa-spying/wordgames. **an exabyte of data:** This is based on the reasonable assumption that a page is 2 kilobytes. It’s not really fair, though, because so much of this data is voice, images, and video.

creating more data per day: M. G. Siegler (4 Aug 2010), “Eric Schmidt: Every 2 days we create as much information as we did up to 2003,” *Tech Crunch*, http://techcrunch.com/2010/08/04/schmidt-data.

76 exabytes of data will travel: Cisco (10 Jun 2014), “Cisco visual networking index: Forecast and methodology, 2013–2018,” http://www.cisco.com/c/en/us/solutions/collateral/service-provider/ip-ngn-ip-next-generation-network/white_paper_c11-481360.html.

a petabyte of cloud storage will cost: Chris M. Evans (18 Apr 2014), “IAAS Series: Cloud storage pricing: How low can they go?” *Architecting IT*, http://blog.architecting.it/2014/04/18/iaas-series-cloud-storage-pricing-how-low-can-they-go.

store every tweet ever sent: K. Young (6 Sep 2012), “How much would it cost to store the entire Twitter

Firehose?” *Mortar: Data Science at Scale*, http://blog.mortardata.com/post/31027073689/how-much-would-it-cost-to-store-the-entire-twitter.

every phone call ever made: Brewster Kahle (2013), “Cost to store all US phonecalls made in a year so it could be datamined,” https://docs.google.com/spreadsheet/ccc?

key=0AuqlWHQKlooOdGJrSzhBVnh0WGlzWHpCZFNVcURkX0E#gid=0.

In 2013, the NSA completed: James Bamford (15 Mar 2012), “The NSA is building the country’s biggest spy center (watch what you say),” *Wired*, http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/all.

third largest in the world: Forbes (19 Oct 2012), “The 5 largest data centers in the world,” *Forbes*,

http://www.forbes.com/pictures/fhgl45ijg/range-international-information-hub.

The details are classified: Kashmir Hill (24 Jul 2013), “Blueprints of NSA’s ridiculously expensive data center in Utah suggest it holds less info than thought,” *Forbes*,

http://www. forbes. com/sites/kashmirhill/2013/07/24/blueprints-of-nsa-data-center-in-utah-suggest-its-storage-capacity-is-less-impressive-than-thought.

cost $1.4 billion so far: Siobhan Gorman (21 Oct 2013), “Contractors fight over delays to NSA data center,” *Wall Street Journal*, http://online.wsj.com/news/articles/SB10001424052702303672404579149902978119902.

Google has the capacity: Randall Munro (2013), “Google’s datacenters on punch cards,” *What If? XKCD*, https://what-if.xkcd.com/63.

In 2011, Schrems demanded: Cyrus Farivar (15 Nov 2012), “How one law student is making Facebook get serious about privacy,” *Ars Technica*, http://arstechnica.com/tech-policy/2012/11/how-one-law-student-is-making-facebook-get-serious-about-privacy. Olivia Solon (28 Dec 2012), “How much data did Facebook have on one man?

57个类别的1200页数据，”*BBC新闻*，http://www.wired.co.uk/magazine/archive/2012/12/start/privacyversus-facebook。

Facebook寄给他一张CD: Schrems的发现让他对Facebook提起了集体诉讼。Liat Clark(2014年8月1日)，“Facebook遭遇国际集体诉讼”，*《连线英国》*，http://www.wired.co.uk/news/archive/2014-08/01/facebook-class-action-lawsuit。

2:数据即监控

我们对NSA监控的了解:之前的泄密者包括托马斯·德雷克、马克·克莱因和比尔·宾尼。其他泄密者的身份尚未确定。Bruce Schneier(2014年8月7日)，“美国情报界有第三个泄密者”，*Schneier on Security*, https://www.schneier.com/blog/archives/2014/08/the_us_intellig.html。

NSA收集手机通话记录:格伦·格林沃尔德(2013年6月5日)，“NSA每天收集数百万Verizon客户的电话记录”，*卫报*，http://www.theguardian.com/world/2013/jun/06/nsa-phonerecords-verizon-court-order。

一个政府辩护:巴拉克·奥巴马(2013年6月7日)，“总统声明”，美国总统行政办公室，http://www.whitehouse.gov/the-press-office/2013/06/07/statement-president。James R. Clapper(2013年6月7日)，“DNI关于最近未经授权披露机密信息的声明”，国家情报总监办公室，http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/868-dnistatement-on-recent-unauthorized-disclosures-of-classified-information。Ed O 'Keefe(2013年6月7日)，“文字记录:Dianne Feinstein, Saxby Chambliss解释，为NSA的电话记录项目辩护，”*华盛顿*，http://www.washingtonpost.com/blogs/post-politics/wp/2013/06/06/transcript-dianne-feinstein-saxby-chambliss-explain-defend-nsa-phone-records-program。

其**本意是:**我是唯一一个怀疑奥巴马总统总是使用非常具体的词语的人吗?他会说，“没人在听你的电话。”这就留下了NSA正在记录、转录和分析你的电话的可能性，偶尔还会阅读它们。这更有可能是真的，一个迂腐的总统可能会说他没有撒谎。

收集人的元数据:这是一篇很好的关于元数据亲密关系的一般性文章。Dahlia Lithwick和Steve Vladeck(2013年11月22日)，“从元数据中剔除‘meh’”，*Slate*, http://www.slate.com/articles/news_and_politics/jurisprudence/2013/11/nsa_and_metadata_how_the_government_c

电话元数据显示: Edward W. Felten(2013年8月23日)，“Edward W. Felten教授的声明”，*美国公民自由联盟等人诉James R. Clapper*等人，纽约南区联邦地方法院(案件1:13-cv-03994-WHP),

https://www. aclu. org/files/pdfs/natsec/clapper/2013. 08. 26%20ACLU%20PI%20Brief%20-%20Declaration%20-%20Felten.pdf.。

它提供了一个窗口: Yves-Alexandre deMontjoye等人(2013年4月2-5日)，“使用新颖的基于手机的指标预测人们的个性”，第六届社会计算国际会议，行为文化建模和预测，华盛顿特区，http://realitycommons.media.mit.edu/download.php?file=deMontjoye2013predicting-citation.pdf。

它产生了一个详细的摘要:IBM提供了一个分析电话元数据的类。IBM公司(2014)，“9T225G:使用i2分析师笔记本进行电话分析”，http://www-03.ibm.com/services/learning/content/ites.wss/zz/en?pageType=course_description&courseCode=9T225G&cc=。

研究者的个人性质:Jonathan Mayer和Patrick Mutchler(2014年3月12日)，“MetaPhone:电话元数据的敏感性”，*Web Policy*, http://webpolicy.org/2014/03/12/metaphone-the-sensitivity-oftelephone-metadata。

网络搜索数据是另一个来源:虽然很明显这是数据而不是元数据，但NSA似乎将其视为元数据。我认为它的正当化是搜索词被编码在url中。NSA的XKEYSCORE幻灯片谈到了收集“基于网络的搜索”，这进一步表明NSA考虑这些元数据。格伦·格林沃尔德(2013年7月31日)，《XKeyscore:NSA工具几乎收集了用户在互联网上的所有行为》,*《卫报》*，http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-onlinedata。

NSA声称这是元数据:这表明这种差异更像是法律上的吹毛求疵。

当我输入“我应该告诉我的w吗”:它和“我应该告诉我的女朋友吗”是一样的。

谷歌知道是谁点击的: Arwa Mahdawi(2013年10月22日)，“谷歌的自动补全功能说出了我们最黑暗的想法，”*卫报*，http://www.theguardian.com/commentisfree/2013/oct/22/google-autocomplete-un-women-ad-

discrimination-algorithms.

Google's CEO Eric Schmidt admitted: Derek Thompson (1 Oct 2010), "Google's CEO: 'The laws are written by lobbyists,'" *Atlantic*, http://www.theatlantic.com/technology/archive/2010/10/googles-ceo-the-laws-are-written-by-lobbyists/63908.

Your tweets tell the world: You can search for the sleep patterns of any Twitter user. Amit Agarwal (2013), "Sleeping Time," *Digital Inspiration*, http://sleepingtime.org.

Your buddy lists and address books: Two studies of Facebook social graphs show how easy it is to predict these and other personal traits. Carter Jernigan and Behram R. T. Mistree (5 Oct 2009), "Gaydar: Facebook friendships expose sexual orientation," *First Monday* 14, http://firstmonday. org/article/view/2611/2302. Michal Kosinski, David Stillwell, and Thore Graepel (11 Mar 2013), "Private traits and attributes are predictable from digital records of human behavior," *Proceedings of the National Academy of Sciences of the United States of America (Early Edition)*, http://www.pnas.org/content/early/2013/03/06/1218772110.abstract.

Your e-mail headers reveal: The MIT Media Lab tool Immersion builds a social graph from your e-mail metadata. MIT Media Lab (2013), "Immersion: A people-centric view of your email life," https://immersion.media.mit.edu.

Metadata can be much more revealing: Brian Lam (19 Jun 2013), "Phew, NSA is just collecting metadata. (You should still worry)," *Wired*, http://www.wired.com/2013/06/phew-it-was-just-metadata-not-think-again.**metadata is far more meaningful:** Edward W. Felten (23 Aug 2013), "Declaration of Professor Edward W. Felten," *American Civil Liberties Union et al. v. James R. Clapper et al.*, United States District Court, Southern District of New York (Case 1:13-cv-03994-WHP),

https://www. aclu. org/files/pdfs/natsec/clapper/2013. 08. 26%20ACLU%20PI%20Brief%20-%20Declaration%20-%20Felten.pdf.

"If you have enough metadata": Alan Rusbridger (21 Nov 2013), "The Snowden leaks and the public," *New York Review of Books*, http://www.nybooks.com/articles/archives/2013/nov/21/snowden-leaks-and-public.

"We kill people based on metadata": David Cole (10 May 2014), "'We kill people based on metadata,'" *New York Review of Books*, http://www.nybooks.com/blogs/nyrblog/2014/may/10/we-kill-people-based-metadata.**one spy for every 166 citizens:** John O. Koehler (1999), *Stasi: The Untold Story of the East German Secret Police*, Westview Press, http://books.google.com/books?id=waxWwxY1tt8C.

Roving wiretaps meant: Mary DeRosa (2005), "Section 206: Roving surveillance authority under FISA: A summary," *Patriot Debates*, http://apps.americanbar.org/natsecurity/patriotdebates/section-206.

The motivations are different: David Lyon makes this point. David Lyon (2003), *Surveillance after September 11*, Polity, http://www.polity.co.uk/book.asp?ref=0745631819.

Another device allows me to see all the data: BrickHouse Security (2014), "iPhone / Android Spy Stick," *Skymall*, https://www.skymall.com/iphone-%2F-android-spy-stick/28033GRP.html.

I can buy a keyboard logger: Keyloggers. com (2014), "Top keyloggers of 2014 comparison and reviews," http://www.keyloggers.com.

I can buy call intercept software: Stealth Genie (2014), "Live call intercept," http://www.stealthgenie.com/features/live-call-intercept.html.

I can buy a remote-controlled drone helicopter: Amazon. com (2014), "DJI Phantom 2 Ready to Fly Quadcopter - With Zenmuse H3-2D Camera Gimbal: $959.00 (list $999)," Amazon.com, http://www.amazon.com/Dji-Phantom-Ready-Fly-Quadcopter/dp/B00H7HPU54.

Professional surveillance devices: There are prototypes for flying sensors that resemble birds and insects, and even smaller sensors—no larger than dust particles—that will float around in the wind. Elisabeth Bumiller and Thom Shanker (19 Jun 2011), "War evolves with drones, some tiny as bugs," *New York Times*, http://www.nytimes.com/2011/06/20/world/20drones.html. John W. Whitehead (15 Apr 2013), "Roaches, mosquitoes, and birds: The coming micro-drone revolution," Rutherford Institute, https://www.rutherford.org/publications_resources/john_whiteheads_commentary/roaches_mosquitoes_and_birds_t

Sprint charges law enforcement: Ashkan Soltani (9 Jan 2014), "The cost of surveillance," http://ashkansoltani.org/2014/01/09/the-cost-of-surveillance. Kevin S. Bankston and Ashkan Soltani (9 Jan 2014), "Tiny constables and the cost of surveillance: Making cents out of *United States v. Jones*," *Yale Law Journal* 123, http://yalelawjournal.org/forum/tiny-constables-and-the-cost-of-surveillance-making-cents-out-of-united-states-v-jones.

FBI was required to: Carrie Johnson (21 Mar 2012), "FBI still struggling with Supreme Court's GPS ruling," *NPR*