1 曾几何时，东德是西方人心中最完备的监听国家，拥有十多万公民间谍和数以万计的专业间谍。但如今的美国比东德已经大大地向前迈进了一步，他们用大数据这种资本密集型和技术密集型的运作方式，代替了原始的劳动密集型监听网络。

2 斯诺登事件暴露了一种越来越尖锐的矛盾，以国家安全为借口对公民隐私的侵犯是否已经到了失控的边缘，或者已经失控？而参与“棱镜”项目的谷歌、微软、Facebook等9家互联网企业，正是大量个人信息数据的占有者，在谋取商业利益的同时，它们掌握的大数据对我们未来的生活产生的冲击难以估量。大数据时代的法律和道德底线应当划在哪里？这直接涉及未来社会的公平和正义。

3 斯诺登事件告诉我们，大数据时代的博弈刚刚开始……

“棱镜”折射出的隐忧

大数据时代 你我都是透明人

□本报记者　赵恩霆　整理

网络海量数据 让监控轻而易举

早期互联网本身，就是在美国国防先进研究计划内研发出来的，在上世纪90年代互联网大规模商业化应用之前，美国政府一直掌控着网络的控制权。作为信息时代的幕后推手，美国政府从未将全球信息网络当做单纯的商业空间，而是特别重视其在国家政治和安全领域的利用价值。“棱镜”计划不过是延续了冷战以来美国国安局全面监听国内外通讯的传统，将其进一步延伸到数据空间而已。

十年前出国，你也许会听到这样的建议：在给国内亲友打电话时，电话中最好插一些涉及弹道导弹、核潜艇之类的军事敏感词。作为对个人隐私权遭受侵犯的抗议，如果所有普通人都在电话中夹杂一些容易被注意到的关键词，会增加那些情报监听机构的工作量，增加其成本，最终获得干扰对方监听的效果。

如今，随着计算机运算和存储能力的提升，以及相应成本的下降，网络化计算能力得到指数倍的提升。时下，随便哪个网站都可能需要处理数量巨大的在线数据，例如，当你使用谷歌在线翻译，寻找英语单词“light”是该翻译成中文的“光”还是“轻”时，一瞬间谷歌就会检索数十亿页的翻译资料。

这个世界每年所创造的数据量正在以指数形式增长，去年，这一数字则达到了2.8ZB(1ZB=1024^4GB)，听起来很可怕吧？据知名信息行业咨询服务商IDC称，这一数字将在2015年翻一番。此外，这些数据中的3/4是由个人在创造或移动数字文件时贡献的。

举例来说，一个标准的美国“上班族”每年可以贡献180万MB的数据量，平均每天有约5000MB，其中包括下载的电影、文档、电邮以及这些数据通过移动或非移动互联网传播时所产生的附加数据量。

在这种庞大的运算能力面前，此前似乎像散沙一样不具备任何关联性的海量数据得到了有效处理。面对一个个体生活不断被互联网信息化高度整合，甚至裹挟和绑架的时代，暂且不去讨论大数据技术是否会沦为一个专制的恶政府的可怕工具，即便一个民主政体出于一个好的目的，但是，你永远无法判断结果的好坏，因为魔鬼永远用一个好的理由将人们带向地狱。“棱镜”事件折射出的对个人隐私权的漠视，似乎正成为一个可怕结果的开始。

大数据可预测80周后 你可能到达的位置

斯诺登揭露的“棱镜”项目的重要特征是美国的“政商协作”。这种协作既包括政府购买服务(政府订单和服务外包)，也包括企业自愿或服从政府要求提供服务，以获取政府信任和政商互动(如人员流转)。“棱镜”项目暴露出的战略与技术咨询提供商博思艾伦和与政府合作的九大互联网公司，也是在此政商协作模式下工作的。

很明显，美国政府与企业的数据情报合作是互惠性的。一方面，美国的互联网大企业本身具有巨大的技术和资本优势，可以弥补政府开支的局限性，并增强国家情报的储存和分析能力；另一方面，国家安全局为快速发现潜在可用情报而研发的最新算法和培养的新人才，可以反过来被高科技资本迅速利用，从而保持美国公司在全球信息技术领域的领先性。

Facebook已经可以实现对个人信息收集的自动化与实时化，其首次公开募股时的财务档案显示，Facebook上每位用户的图片和视频资料数据量约为111MB，而Facebook的用户数如今已经超过了10亿，这可是整整100PB(1PB=1024^2GB)的个人信息数据。这意味着，可以获得的个人数据量越多，其中的信息量就越大。只要拥有了足够多的数据，我们甚至可能发现关于一个人的未来信息。去年，来自美国罗彻斯特大学的亚当·萨迪克和来自微软实验室的工程师约翰·克拉姆发现他们可以大致预测一个人未来可能到达的位置，最多可以预测到80周后，其准确度高达80%。为此，他们收集了32000天里307个人和396辆车的GPS数据并建造了一个“大规模数据集”。

根据斯诺登提供的信息，美国国安局拥有的正是一套基于大数据的新型情报收集系统，这套名为“无界爆料”的系统，以30天为周期，可以从全球网络系统中接收到970亿条讯息，再通过比对信用卡或者通讯记录等方式，能几近真实地还原个人的实时状况。

随着数据越来越详尽，数据挖掘和解读的技术不断提高，哪怕是个人生活最隐秘的部分也越来越趋于透明化。事实上，我们可以直接说数字化生存在很大程度上就是透明化生存，而且是透明化的程度在不断地提高。随着数据采集取样越来越趋于详实，对个人和群体行为趋势的预判越来越准确。

潜在危险 需要监督制约

相比网络之前的时代，时下的数据分析能力得到了空前的提升，但谁能保障大数据分析的准确性呢？我们可以回过头去，看看电脑是如何得出这个结果的，或许可以查阅一下硬盘上的数据，或许可以检查一下一两个程序代码，来判断其逻辑是否有误。但在大数据时代，因为大数据算法和结构太过复杂，从外部没有人能够追溯错误的源头。

维克多·梅耶·松博格与肯尼迪·古奇尔在他们合著的《大数据：改变我们生活、工作、思考的革命》一书中，记录了这样一件事：在2004年美国国家安全局依赖大数据系统，自动分析生成了一张禁止飞行的危险人物名单，但这一名单错误百出，甚至美国参议员也赫然在列。幸亏国家安全局一名算法师从内部阻止了这张名单生效。

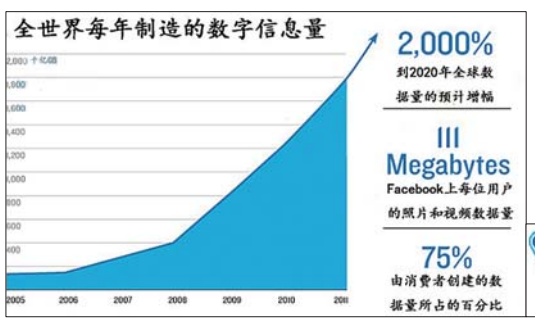
在这个故事中，我们可以看到大数据出错的风险。在没有有效的保障下，大数据分析系统可能变成一个不可说明、不可追踪，甚至不可信的黑匣子。在这种情况下，大数据和政府治理一旦密切联姻，可能将产生无数的受害者。试想一下，谁能真正保证“棱镜”计划制止的恐怖分子不会有错误呢？

在西方，消费者信息监控已经发展为一项规模达几十亿美元的产业，其中的企业基本不受什么监管，即使是有影响力的人物的个人信息，其卖价通常都不会超过一美元。在这种力量不平衡之下，手中掌握着更强大的数据分析能力的大公司以及更强大的政府，就拥有了自由利用这些信息而不受监督的能力。

显然，“棱镜”折射出了这一潜在的危险。大数据时代的到来，要求我们必须建立一套新的监督制衡机制来规范政府行为，建立一个更加开放的社会治理环境来减少大数据错误的危害。

在大数据时代之前，民众可以以保密的方式来保护隐私，但今天人们在不知不觉间就透露了隐私。这就要求那些保存和管理信息的企业承担更大的责任，这应该成为一种新的隐私保护模式：政府不应假定消费者在使用企业的通讯工具等产品时主动透露了自己的隐私，就意味着他们授权企业使用这些隐私。力量越大责任也越大，现在是那些掌控大数据的大企业和政府负起责任，构建一张更完善的安全网的时候了。

(据《中国青年报》、《经济观察报》、果壳网、《21世纪经济报道》、新加坡《联合早报》等)



来源：果壳网

巴拉迪：埃及的“国际公务员” B03　　黑船来航 B04

统筹：赵恩霆　美编：马晓迪　组版：陈华