# 第26话

# 监视还是隐私？

经验应该告诉我们，当政府的目的是有益的时候，我们要最警惕地保护自由……

对自由的最大威胁潜伏在充满热情、善意但缺乏理解力的人的阴险侵犯中。

最高法院大法官路易斯·布兰代斯

一切秘密都会堕落，甚至司法行政也是如此；没有什么是安全的，不表明它如何经得起讨论和宣传。

阿克顿勋爵

律师和工程师的争论像愤怒的幽灵一样相互交织。

– 尼克·博姆、伊恩·布朗和布赖恩·格拉德曼

## 26.1 简介

政府在网上有越来越多的利益，从监视到审查，从隐私到安全，从市场竞争到公平选举。

他们的目标往往与全球化网络世界的现实存在紧张关系，彼此之间也存在紧张关系。它们具体围绕着一些具体的政策问题，从恐怖主义和反叛乱，通过国家战略和经济优势，到压制有害或不受欢迎的内容和维护人权。在本章中，我们将探讨监视、审查、取证和隐私之间的联系。

互联网以许多复杂的方式改变了世界，就像它之前的其他重大技术一样 电力、蒸汽机、写作、农业和火。公民与国家之间的关系到处都在发生变化，国家通常会获得更多的权力和控制。早年，随着 PC 取代大型机，互联网向所有人开放，许多先驱者

是乌托邦主义者:我们相信自由获取信息会在个人层面上带来解放,也会破坏专制政府的稳定。然而,政府和大公司及时学会了使用新工具。 2001 年 9 月 11 日发生在纽约和华盛顿的恐怖袭击产生了真正的影响,它激发了大规模监视的动机并削弱了对它的政治反对。在线业务的发展创造了工具,以及为个人信息付费的商业市场。虽然钟摆在 2010 年代重新转向监视资本主义,但 COVID-19 大流行似乎将再次增加国家监视,权衡不是隐私与安全,而是隐私与健康。

这是监视的繁荣时期。这不仅仅是 Ed Snowden 在 2013 年披露的 NSA 能力;俄罗斯和中国等民族国家的竞争对手也有强大的能力;虽然在叙利亚等欠发达国家有更原始但仍然有效的系统。

2010 年代还见证了越来越多的网络冲突和破坏,各国暗中干涉其他国家的事务。美国和以色列利用 Stuxnet 恶意软件破坏和延缓伊朗获取核武器的努力,这导致其他国家争先恐后地获取各种网络武器。自从俄罗斯干预 2016 年美国大选以来,许多国家的立法者都希望对社交媒体进行监管:许多政客一旦意识到自己的工作受到威胁,就不再忽视技术。

有很多棘手的问题。首先,拥有民主和新闻自由的开放社会是否更容易受到攻击,因为我们更容易被剥削?如果是这样,我们能做些什么呢?我们的核心价值观面临着真正的挑战 在美国表现为宪法,在欧洲表现为人权公约。

自 9/11 以来,我们看到了一项又一项的专制措施,从大规模的通讯监控到未经审判的拘留甚至酷刑。许多这些措施不仅是非法和不道德的,而且是无效的,甚至适得其反:在阿布格莱布监狱中与基地组织恐怖分子一起折磨伊拉克秘密警察是使他们成为伊斯兰国核心的原因。我们不能找到更好的方法来捍卫自由吗?我们如何重申和捍卫我们的核心价值观?

其次,是安全的政治经济学。艾森豪威尔总统在他的告别演说中警告说,“我们必须警惕军事工业综合体获得不必要的影响,无论是寻求还是未寻求。”错位权力灾难性崛起的可能性存在并将持续存在。自 9/11 以来,我们已经看到了一种安全工业复合体捕获策略,其方式与冷战开始时国防工业所采用的方式相同。在安全机构和新闻界的怂恿下,左翼和右翼政客们煽动了一种恐惧文化。自 2008 年金融危机以来,民族主义的抬头加剧了这种情况。

安全技术争论经常被用来迷惑或恐吓立法者。例如,从 20 世纪 70 年代到 90 年代的爱尔兰共和恐怖主义运动,英国警方不得不在四天内对被捕的恐怖嫌疑人提出指控。但在 9/11 之后,这一天数很快提高到 28 天;然后政府说需要 90 天,声称他们可能难以解密从嫌疑人手中没收的个人电脑上的数据。真正的问题是警察

取证管理效率低下。现在,如果警察只是说“我们需要将嫌疑人关押 90 天,因为我们没有足够的索马里语翻译”,那么常识就可以发挥作用;议会很可能会告诉他们使用商业翻译机构的员工 。但是谈论解密似乎是让立法者的大脑变得糊涂的好方法。懂密码学的人有发言权。

对恐怖主义的关注使其他执法部门挨饿。现在大约一半的犯罪活动都发生在网上,但用于打击犯罪活动的资源却很少。许多诈骗者逍遥法外。

围绕审查制度还有更多问题。对在线滥用的担忧是真实的,但这是一个困难的领域。虐待的严重程度从顶端的谋杀和强奸儿童视频,到仇恨言论、强奸威胁和网络欺凌,再到大规模可能有害的新闻操纵。各国开始通过法律,要求像 Facebook 这样的公司为他们进行审查,这导致了许多紧张局势。这些公司不喜欢额外的费用,有思想的公民不喜欢审查制度掌握在私人垄断手中的想法 或者我们上传的所有东西,从图片和视频到私人信息,都被过滤的想法。因此,公司有动力重新设计他们的系统,这样他们就更难被滥用;例如,Facebook 声称正在重建其系统,以更多地关注极端分子更难玩弄的群体,并更多地使用端到端加密,因此它可以声称无知。

这样的论点在重大事件中丝毫没有破绽,例如 2019 年 3 月,一名枪手在新西兰克赖斯特彻奇的两座清真寺杀人,并使用 Facebook 分享了犯罪现场视频。这迫使该公司开始审查白人至上主义团体,这是该公司之前避免的一项政治敏感任务 [1913 年]。 COVID-19 大流行导致该公司迅速采取了许多此前被业界谴责为不可能、不可取或不切实际的事情:消除错误信息、禁止剥削性广告和推广社会建议 [984]。隐私和审查制度之间的紧张关系可能会继续以不可预测的方式解决。

隐私监管已经很复杂。美国法律支离破碎,联邦法律针对健康数据和视频租赁等特定主题,FTC 惩罚违反其公布的隐私政策的公司,而州法律推动安全漏洞披露。欧洲非常不同 :通用数据保护条例提供了一个全面的框架,并得到人权法的支持,该法已被用来废除有关监视的法律。从 IT 行业的角度来看,总体效果是欧洲正在成为世界隐私监管机构;华盛顿不在乎,没有其他人足够重要。 (有强烈的迹象表明,这种监管权力也将稳步扩展到安全领域,尽管我们将把它留给关于保证的章节。)

在本章中,我将讨论监视的演变,然后在讨论审查制度和隐私监管之前先看看恐怖主义,最后尝试将整个事情放在背景中。

## 26.2 监视

2010 年代技术监控大幅增加,不仅是政府,还有商业公司监控我们的点击流和位置历史,以便更好地定位广告 Shoshana Zubo 将其描述为“监控资本主义”[2075]。两者以各种方式相互作用。在一些国家,如美国,执法和情报机构不仅从他们自己的收集系统获取信息,而且还使用搜查令从谷歌和 Facebook 等公司获取信息。在其他国家,比如中国,这些公司被禁止,因为它们拒绝向当局提供完全的访问权限;在其他国家,比如伊朗和叙利亚,警察机构只是破解人们的密码,或者钓鱼他们的朋友,或者黑掉他们的手机。

这是一个巨大的主题,我所能合理提供的只是一次直升机之旅:将监视置于其历史背景中,勾勒出正在发生的事情,并提供指向主要来源的指针。

### 26.2.1 政府窃听的历史

统治者一直试图控制通信。在古典时期,信使在海关接受检查,而从中世纪开始,许多国王要么垄断邮政,要么将其授予亲信。 David Kahn 的历史“The Codebreakers”[1001] 中描述了早期现代国家的信件打开和密码破译设施,即所谓的黑室。

当电子通信出现时,政府试图保持控制。在欧洲大部分地区,电报服务是作为邮局的一部分设立的,归政府所有;在英国,Gladstone 于 1869 年将电报业国有化。大量的国家规则造成了如此多的麻烦,以至于国际电报联盟 (ITU) 于 1865 年成立,以实现标准化 [1818]。在美国,西联汇款是第一个全国性的工业垄断企业,并在 19 世纪主导了市场。联盟和邦联士兵互相窃听对方的电报线,纽约警察局于 1895 年开始窃听行动。

电话的发明引发了关于隐私的争论。在美国,最高法院于 1928 年在 Olmstead vs United States 案中裁定,窃听并未违反第四修正案关于搜查和扣押的规定,因为没有实际破坏住所;著名的布兰戴斯大法官持异议。 1967 年,法院在 Katz 诉合众国案中推翻了判决,裁定该修正案保护的是人,而不是地方。次年,国会根据有组织犯罪规模的证词,将联邦窃听合法化(在综合犯罪控制和安全街道法案的“第三章”中)。 1978 年,在对尼克松政府的滥用职权进行调查后,国会通过了《联邦情报监视法》(FISA),该法控制窃听以保障国家安全。 1986 年,电子通信保护法 (ECPA) 放宽了 Title III 授权条款。到 1990 年代初,解除管制的服务从移动电话扩展到呼叫转移已经开始削弱当局窃听的能力,调制解调器中的自适应回声消除等技术发展也是如此。

因此,1994 年的执法通信援助法案 (CALEA) 要求所有通信公司以 FBI 批准的方式使其网络可窃听。到 1999 年,根据 1,350 项法院命令 [634, 1257],超过 2,450,000 次电话交谈被合法窃听;到 2017 年,窃听订单的数量几乎增加了两倍,达到 3,813 件,但其中 94% 是针对手机等便携式设备的 [1927]1。外国情报监视法院 (FISC) 全部或部分批准了另外 1,598 项命令,而拒绝了 26 项。

甚至在 9/11 之前,一些分析人士就认为,未经授权的窃听至少与经授权的窃听一样多 [558]。首先是电话公司勾结:如果电话公司出示搜查令,他们必须允许警察进入,但在许多国家,他们也被允许提供帮助 多年来,有许多电话公司与政府关系融洽的报道。

其次,存在情报机构套利:如果国家安全局想在没有授权的情况下窃听美国公民,他们可以找一个盟友来做,然后再回报。例如,据说玛格丽特·撒切尔 (Margaret Thatcher) 使用加拿大情报部门窃听涉嫌不忠的部长 [728]。这些机构多年来一直否认这种做法,但斯诺登泄密事件表明它们是真实的;例如,如我在 2.1 中所述,NSA 让 GCHQ 窃听 Google 数据中心之间的链接。第三,在一些国家,如果其中一位用户同意,窃听是不受控制的 因此来自电话亭的电话可以自由窃听(电话亭的所有者是合法用户)。公司可能会窃听他们的员工以检测欺诈行为,并自愿将产品交给警方或安全机构;当安全部门参与一项非法的、秘密的计划,将试图组织工会的建筑行业员工列入黑名单时,英国发生了一起丑闻 [658]。最后,在许多国家/地区,警方通过传票而不是搜查令获取电子邮件和其他存储的通信信息。在 2007 年法院停止这种做法之前,他们在美国也这样做了 [1161] – 但判决并没有阻止赏金猎人和保释代理人等私人行为者从数据聚合商那里购买电话位置历史记录 [489]。

但是,即使官方数字必须增加一倍或三倍,民主政体使用窃听的次数也比威权政体少得多。现在的监控领导者是中国,它在新疆和西藏等少数民族地区使用无处不在的技术监控,在街角、清真寺和学校安装监控摄像头,通过人脸识别软件连接到数据库,记录谁在什么地方见过谁,什么时候。还有侵入性的物理措施,从频繁的街道检查站,通过在少数民族家庭家中安置党员,到在劳改营中进行大规模监禁 [1110]。

窃听的发生率在民主国家内部和民主国家之间也存在很大差异。例如,在美国,只有大约一半的州使用它,在 20 世纪的大部分时间里,大多数水龙头都在纽约、新泽西和佛罗里达等“黑手党”州(尽管内华达州和加利福尼亚州现在已经赶上了)[ 1927]。欧洲也有类似的变化。窃听在荷兰非常普遍:他们在旅途中一次窃听多达 1,000 次,其中十分之一

1 相关法律为 18 USC(美国法典)2510–2521,而 FISA 对外国情报收集的规定现编入美国法律为 50 USC 1801–1811。

美国人口[356]。在荷兰的凶杀案调查中,通常会在一周内窃听受害者通讯录中的每个人,以监控他们对死亡的反应。窃听最多的发达国家是意大利,这要归功于其有组织犯罪的历史 [1160]。在英国,国内窃听应该需要部长令,不能作为证据;所以警方改用房间窃听器和计算机漏洞。如果你能 root 歹徒的电话或笔记本电脑,你就可以记录附近所说的一切,并寄回家,无论是对同一房间的人说的,还是在电话中说的。国际电话几十年来一直被例行记录并存储几天到几周,以备不时之需,许多其他国家也效仿这种模式;例如,在 2008 年孟买大屠杀之后,印度可以挖掘出恐怖分子与其在巴基斯坦的控制者通话的录音。

自动化正在将窃听成本从每次通话的人工成本转变为一次性资本成本。在引入 CALEA 之前,1993 年,美国警察机构在窃听上的花费仅为 5170 万美元 这也许是对问题变得政治化之前的价值的一个很好的估计 [862]。 CALEA 的实施成本超过 5 亿美元,这是在 2007 年扩展到 VOIP 之前。VOIP 更难:从波士顿的咖啡馆打电话到巴黎的旅馆房间,一个小时后从剑桥的办公室打电话到卢浮宫的礼品店"[220]。在 2010 年代,随着人们从手机等物理平台转向 Facebook、Skype 和 Signal 等虚拟平台,事情变得更加困难。因此,决策者的趋势是进行资本投资以降低接入的边际成本。例如,十年前,如果英国警方正在调查三起类似的强奸案,他们可能不得不向电话公司支付数千英镑以收集手机基站转储点,以便他们可以查找所有三个地点都存在的手机。现在,在花费数亿美元并通过多项法律后,他们可以访问手机位置数据库,只需数据库查询即可。这改变了警察和情报工作的性质。

美国还修改了法律以促进批量监控。 9/11 袭击发生 43 天后,国会通过了《爱国者法案》,该法案允许执法部门更多地访问存储的记录(包括财务、医疗和政府记录),在没有所有者身份的情况下对住宅和企业进行"偷偷摸摸"搜索知识,以及 FBI 使用国家安全信件来获取财务、电子邮件和电话记录。

但这对机构来说还不够。 2005 年 12 月,《纽约时报》披露,布什总统于 2002 年签署了一项秘密命令,要求对涉嫌恐怖主义的美国居民进行未经授权的窃听,这违反了法律 [1606]。 2006 年,《今日美国》披露,美国国家安全局秘密获取了美国三大电话公司 AT&T、Verizon 和 BellSouth 的 2 亿客户的完整通话数据记录 (CDR)。 CDR 计划于 1992 年在老布什总统领导下由 DEA 启动,目标是美国人往来于某些国家的电话;它在 9/11 之后有所增加,当时他的儿子也授权收集所有美国内部电话的 CDR [877]。 Qwest 没有合作,因为当时的首席执行官 Joe Nac chio 坚持认为 NSA 需要法院命令。美国国家安全局施压

Qwest 威胁要扣留机密合同,因此 Qwest 的律师要求 NSA 将其提议提交给 FISA 法庭。他们拒绝了,称法院可能不会同意他们的意见。从那以后,他们已经向 Qwest 施加压力,要求他们甚至在 9/11 之前就交出数据 [768]。 2007 年 10 月,Verizon 向参议员们承认,自 2005 年以来,它已经向 FBI 提供了 720 次关于其客户的针对国家安全信函的第二代通话数据 [1376]。

2007 年 11 月,《华盛顿邮报》披露 NSA 窃听了大量纯国内电话和流量数据,还窃听了 AT&T 在旧金山的对等中心以获取互联网流量 [1377]。经过两年的辩论,国会修正了 FISA 以授予与非法窃听合作的电话公司的追溯豁免权,并修改法律以便 NSA 甚至不再需要 FISA 授权来窃听一方被认为不在其范围内的电话。美国或非美国人。 （这导致两党分裂,参议员奥巴马和范斯坦支持修正案,而参议员麦凯恩、拜登、里德、莱希和克林顿则反对。）

## 26.2.2 呼叫数据记录（CDR）

从历史上看,更多的警方通信情报来自电话数据记录和其他元数据的分析,而不是窃听。我们在关于电信安全的章节中讨论了警方如何使用此类数据来追踪犯罪联系网络,以及犯罪分子如何通过使用预付费移动电话和 PBX 黑客攻击等技术将信号隐藏在无害的网络中来做出回应。

同样,这并不是什么新鲜事。长期以来,统治者一直利用对邮政服务的控制来追踪嫌疑人的通讯员,即使信件没有被打开。 1840 年邮票的引入是隐私方面的进步,因为它使匿名发送信件变得更加容易。一些国家非常担心煽动叛乱的威胁,以至于他们通过了法律,要求在信封背面写上回信地址。另一方面,电报的发展是监视的进步。由于消息是按发送者、接收者和字数记录的,因此可以编译总流量,并发现它是经济活动的有效指标 [1818]。第一次世界大战教会了战斗人员通过测量敌方无线电通信量可以收集到多少情报,即使无法方便地对其进行破译 [1001, 1380]。二十世纪后期的冲突强化了这一点。

当我写这本书的第一版时,我注意到美国在 1998 年批准了 1,329 份窃听申请,同时有 4886 份笔式登记传票（加上 4621 份延期）（记录从目标电话线路拨出的所有号码的设备)和 2437 份用于陷阱和跟踪设备的传票（加上 2770 份分机）（记录来电的主叫线路 ID,即使来电者试图阻止它）。执法机构在 1990 年代也开始转向使用传票获取电话公司数据库中的通话详细记录。例如,Bell Atlantic 在 1989-92 年间回应了 25,453 份传票或法院命令,要求其 213,821 名客户的通行费记录,而 NYNEX 仅在 1992 年就处理了 25,510 份传票,涵盖了未记录的客户数量 [402]。扩大到七个 Baby Bells,这表明可能有 50 万客户拥有他们的记录

1990 年代每年都有人查获,收集到的 trac 数据可能是被窃听人数的一百倍。

在 9/11 之后,在非法收集期间,统计数据变得暗淡无光,尽管美国国家安全局确实在 2006 年透露它希望“创建一个数据库,记录在该国境内拨打过的每一个电话”,以便它可以绘制整个美国社交网络的地图反恐战争 [395]。斯诺登在 2013 年透露它已经为全球所有通信建立了相当不错的所有跟踪数据数据库后,国会于 2015 年通过了《自由法案》,我们开始从国家情报总监那里获得年度统计透明度报告。 2018 年 4 月的报告给出了 2017 年的一些数据;这些仅与国家安全问题有关,但对内容和 trac 数据之间的平衡给出了一些感觉。窃听令在美国每年稳定在 1,500 起左右(针对约 300 名美国人和 1000 名其他人),海外的目标数量也在不断增加 2016 年为 106,469 起,2017 年为 129,080 起。此外,有 7,512 名美国居民的检索了通信内容(例如电子邮件的传票),同时检索了 16,924 名居民的非内容(例如 trac 数据)以及 56,064 名非居民。还有 87,834 条收集的业务记录,其中可能包括哪个用户使用哪个 IP 地址的记录 [1464]。

现在,美国情报界只有在人类分析师查看时才认为通信被“拦截”;软件分析不算在内(英国法律两者都算在内)。正如我在第 23.3.1 节中所述,寻找嫌疑人的通常过程是联系链,也称为“滚雪球搜索”。如果有人在恐怖袭击中引爆了自己,分析人员将使用软件查看所有与他们交流过的人,然后是这些直接接触者与之交流过的每个人,甚至达到三度分离。标准的二次深度搜索通常会提供数万个间接联系人。然后将这些联系人与各种嫌疑人名单上的数百万个名字 宗教极端分子、右翼仇恨团体、有组织犯罪 进行比较,然后分析人员会找出与任何已知嫌疑人的联系。 (这个比喻是将雪球滚下坡,然后将其融化,然后看看你在桶底发现了什么泥土。)所以分析员可能只看六个与死去的恐怖分子有过接触的人以及一些宗教团体,但数以万计的无辜者的通话数据记录被该软件查看。 DNI 报告估计,2017 年,以这种方式自动检查了 534,396,285 条呼叫数据记录 (CDR),比 2016 年的 151,230,968 条大幅增加。

然而,国会就允许《爱国者法案》(经 FISA 修订)第 215 条失效进行了长时间的辩论。这是允许批量收集 CDR 的部分 [416];美国国家安全局已经表示它不想要它。大量收集通信数据是埃德·斯诺登强调的引发最多争议的问题之一。 2013 年 6 月 8 日,媒体披露了 Boundless Informant,这是一种 NSA 可视化工具,显示了语音和计算机通信元数据收集位置的热图;在截至 2013 年 3 月的 30 天内,从 504 个来源(或 SIGAD)收集了 30 亿条记录。虽然最密集的收集是在中东,但斯诺登说,在美国收集到的美国人的记录多于在俄罗斯收集到的俄罗斯人的记录 [756]。在另一次阅读材料时,

Boundless Informant 通过美国电信提供商收集了 30 亿条电话记录,另外还有 970 亿封电子邮件和 1240 亿通全球电话记录 [816,p. 92];总体而言,每天收集 200 亿个事件 [816,p. 98]。
然而,一份解密报告显示,虽然美国国家安全局的通话数据记录计划耗资超过 1 亿美元,但它只产生了两条线索和一项重大调查 [1656]。 2020 年,该条款在 3 月被允许失效,但在 5 月重新声明;政治很混乱。
Susan Landau 和 Asaf Lubin 解释说,在 4g 移动网络中,传统的 CDR 不再可靠地识别主叫方和被叫方 [1126]。无论如何,行动正在从普通的旧电话系统转移到消息系统。

至于特定刑事调查中的有针对性的收集,根据 18 USC 3123 [1925],调查人员只需向地方法官证明“通过此类安装和使用可能获得的信息与正在进行的刑事调查有关”。这可以是任何犯罪 重罪或轻罪 并且根据联邦或州法律。自CALEA以来,用户发送电子邮件的地址等通信数据仍然需要保证,但可以通过传票获得基本的通行费记录 无需通知用户,一旦没有法院监督订单已下达。法律要求美国司法部公布其非国家安全执法活动的统计数据,但似乎不愿意这样做;美国公民自由联盟 (ACLU) 仅在信息自由 (FOI) 诉讼后提取了 2011-12 年的数据,该诉讼显示笔式登记器和用于监视手机的陷阱和追踪设备的原始订单总数增加了 60%,从 2009 年的 23,535 人增加到 2011 年的 37,616 人 [765]。我一直无法找到更多最近的东西。

大量访问 trac 数据也导致了欧洲严重的政治斗争。英国于 2006 年在欧盟推行了一项数据保留指令,根据该指令,成员国必须将电信数据(包括 IP 地址和每封电子邮件、电话和短信发送或接收的时间)存储 6 个月至 24 个月,并将所有这些提供给执法和情报机构。 2014 年,在爱尔兰数字权利提起诉讼后,该指令被欧洲法院否决,该诉讼称一揽子数据收集违反了欧盟基本权利宪章。

在英国,有针对性地访问通信数据只需要高级警官向电话公司或 ISP 发出通知,而不需要搜查令;和美国一样,数据可以提供给范围广泛的公共部门机构。根据数据保留指令,布莱尔政府希望将事情集中起来;它争辩说警方需要一个“通讯数据库”,并推动通过一项法律来建立它。当一些邪恶的人偷走了议会成员提交的所有费用报销单的副本并将其卖给《每日电讯报》时,命运介入了。原来,无数大臣等人一直在出言不逊。几位尊贵的议员入狱,英国大部分知名政治家都不得不偿还。 (我在上文第 8.6.5 节中讲述了内政大臣雅克·史密斯的悲惨故事 他一直在推广通讯数据库。)直到埃德·斯诺登在 2013 年告诉我们他们只是无论如何建造它,即使没有议会批准。

在欧洲法院废除数据保留并且斯诺登揭露了 GCHQ 的一些非常令人反感的活动之后,英国通过了 2014 年的 DRIP 法案,以断言 GCHQ 一直在做的事情毕竟是合法的。很明显,欧洲法院最终会反对,但需要一些喘息的空间,而该法案给出了这一点(它有一个为期两年的日落条款;首相卡梅伦的自由联盟伙伴不会再给他)。最终,在英国脱欧公投之后,议会通过了《调查权力法案》,该法案很好地使 GCHQ 可以为所欲为,并迫使辖区内的任何公司为其提供协助。未来有趣的行动首先是美国大公司将在多大程度上提供帮助,其次是欧洲人权法院将采取的路线2。我稍后会回到这些问题。

### 26.2.3 搜索词和位置数据

在过去的 20 年里,越来越清楚的是,电话公司时代发展起来的监控监管并不真正适合互联网时代的目的。那时,您要么获得完整的窃听并记录内容,要么使用通话数据记录中的跟踪数据。但随着事物在线化,通信数据和内容都混在一起了,因为一个抽象级别的内容通常是下一个抽象级别的通信数据。有些人可能认为 URL 只是要获取的页面的地址,但诸如 http://www.google.com/search?q=marijuana+cultivation+UK 之类的 URL 包含输入搜索引擎的术语以及搜索引擎的名称。显然,一些警察想要一份提交此类调查的所有人的名单。这在 1999 年成为一个现实问题,当时英国政府对其监控法进行了现代化改造;学术界、非政府组织和行业设法将“大浏览器修正案”纳入 2000 年调查权力条例法案,将 trac 数据定义为识别通信机器所必需的信息;对于 URL,这意味着直到第一个斜杠的所有内容。

在美国,司法部向一些搜索引擎发出传票,要求其交出整整两个月的搜索查询以及其索引中的所有 URL,声称它需要这些数据来支持其声称儿童在线保护法没有违反宪法,过滤可以有效打击儿童色情内容。 (回想一下我们在 11.2.3 节中讨论过的,当 AOL 发布一些搜索历史时,其中的一些很容易被个人识别。)AOL、微软和雅虎悄悄地答应了,但谷歌拒绝了。一名法官最终在 2006 年裁定,该部门将不会收到任何搜索查询,而只会从它最初寻求的 URL 中随机抽取 50,000 个样本 [2035]。

下一个问题是手机位置数据,它最终在不同的司法管辖区受到不同的对待。在英国,所有关于手机位置的信息都算作trac数据,公务员很容易得到;但在美国,上诉法院在 2000 年裁定,当警方获得手机定位令时,手机所在的小区就足够了,并且需要对设备进行三角测量(警方的解释是通缉)

2英国脱离欧盟将让它逃脱欧洲法院,这是一个欧盟机构,但不是人权法院,因为这是欧洲委员会的一个机构

会侵犯隐私 [1926]。此外,在适用于笔式登记传票的较低标准下,即使是单元粒度的位置信息也将不可用。然而,尽管有这些规定,还是有大量信息泄露。 2019 年出现的情况表明,AT&T 和 Sprint 多年来一直在向数据经纪人出售客户的位置信息,其中不仅包括基站数据,还包括 GPS;这通常被赏金猎人和保释代理人购买以追踪违约者 [489]。许多政府现在正在收集位置数据,以更广泛地追踪 COVID-19 患者的接触者和流行病学。它也被许多应用程序收集:Untappd 啤酒评级应用程序由数百万啤酒饮用者运行,他们记录了数百个带时间戳的位置,这使记者能够追踪世界各地的美国军事和情报人员 [1538]。

## 26.2.4 算法处理

呼叫数据的分析只是一个更广泛问题的一个方面:批量数据集的执法匹配。最早认真使用多源数据似乎是在 70 年代后期的德国,目的是追踪 Baader-Meinhof 恐怖组织使用的安全屋。调查人员寻找公用事业使用高峰期不规律的出租公寓,这些公寓的租金和电费是通过一系列不同地点的远程信用转帐支付的。这很奏效:它产生了一份包含数百套公寓的清单,其中包括几处安全屋。进行此类分析的工具现在随许多用于 trac 分析和管理主要警方调查的产品一起提供。它们的使用范围取决于当地的监管环境;在英国,警方对药剂师填写的处方数据库的访问权存在争议,而在美国,医生对调查人员从保险公司传唤个人健康信息的频率感到震惊。理解商业和政府数据处理器使用的许多专有数据格式的成本也存在实际限制。但警方通常至少可以访问公用事业数据,例如通过拖网找到大麻种植者的电费单,并且几乎没有什么可以阻止他们使用商业上可用的数据,例如来自信用咨询机构的提要。

自从 2016 年 AlphaGo 击败李世石以来,出现了许多机器学习初创公司,其中不少旨在以某种方式使执法更容易。但这并不像看起来那么容易。恐怖分子在人口中所占的百分比如此之少,以至于如果你不想淹没在误报中,你用来“检测”他们的任何测试都需要非常特殊。组合多个传感器很困难,如果您要大海捞针,建造更大的大海捞针并不总是明智的。正如曾任 IBM 数据挖掘部门首席科学家的 Je Jonas 所说,“通过观察人们的行为来预测恐怖主义意图的技术远未达到我认为它们仅是必要的准确度水平侵犯公民自由的引擎”[757]。

### 26.2.5 ISP 和 CSP

2000 年代,互联网服务提供商 (ISP) 和通信服务提供商 (CSP – 像谷歌和雅虎这样的公司) 的侵入式监控迅速增长。在 ISP 处窃听数据流量比过去的语音更难;存在许多障碍,例如为大多数客户提供的临时 IP 地址以及 trac 日益分散的特性。在过去（比如 2002 年）,ISP 可能拥有调制解调器机架和可以放置窃听设备的 LAN;如今,许多客户通过 DSL 进入,而提供商使用的交换网络通常没有任何明显的地方可以放置水龙头。 ISP 简单地成为了自然的控制点。

许多国家/地区现在都有法律要求 ISP 提供帮助,而在大型 ISP 处执行此操作的通常方法是安装已安装的设备,将感兴趣的数据包副本（或 NetFlow 记录)发送到单独的机密网络。 FBI 的系统 DCSNet 非常灵活 允许特工点击访问来自参与电话公司的跟踪和内容 [1761]。 （有关哪些公司已被带入的信息被严密掌握,但聪明的坏人使用小型 ISP。)而且事情经常出错,因为警察不了解 ISP;他们传唤错误的事情,或提供不准确的时间戳,以便将错误的用户与 IP 地址相关联。有关故障模式的分析,请参见 Clayton [442]。

智能手机革命将自然控制点从 ISP 转变为 CSP。现代罪犯可能会起床,使用家里的 wifi 在 Gmail 或 WhatsApp 上查看他的消息,然后乘公共汽车进城并使用他的 3G 或 4G 数据连接做同样的事情,然后可能在星巴克或公共图书馆使用 wifi。 .. 在这些情况下,ISP 的窃听都不会提供任何信息,而不仅仅是使用了特定服务这一事实。由于该通信服务的踪迹是加密的,警方必须提供有关该服务的文书工作才能到达任何地方。这就是 FBI 建立 Prism 系统的原因,据此,情报机构只需按一下按钮,就可以从谷歌、雅虎、苹果、微软、Facebook 和其他公司获取客户数据。

这也是导致英国在其 2016 年调查权力法案中授予自己权力,命令任何公司做任何它实际可以做的事情,以协助情报调查的执法。越来越多的国家正在通过此类法律,这使服务提供商与其他国家的法律发生冲突。

一个重要的引爆点是欧盟隐私和数据保护法之间的紧张关系,前者要求对侵犯隐私行为采取正当程序,而后者要求美国公司按要求交出外国人数据。但还有更多。谷歌宁愿离开中国也不愿让警方不受限制地访问所有用户数据。正如一位谷歌高管告诉我的那样， ‘如果印度的家庭法庭命令你交出居住在加拿大的某人的 Gmail 并强制执行终身保密令,你如何同时雇用印度人,并提供可信的保证?加拿大人的隐私?

最后,围绕 Facebook 等 CSP 提供的更丰富的数据存在很多问题,这些数据不仅大规模收集高度敏感的数据,而且能够以以前不可能的方式从 trac 数据中推断出敏感事实。正如我在第 11.2.5 节中讨论的那样,Michal Kosinski 及其同事

发现他可以从四个 Facebook 点赞中判断某人是异性恋还是同性恋 [1086],此后他的一些同事以工业规模收集 Facebook 数据并将其用于政治竞选,导致剑桥分析丑闻被发现社交网络数据曾在 2016 年被用于大规模非法干预英国脱欧公投和美国总统大选。对于执法机构和情报机构或公共卫生机构对社会分析方法的使用,应该有什么样的控制? （稍后我们将回到这些技术引发的更广泛的问题。）

## 26.2.6 五眼联盟体系

我们在 2.2.1 中讨论了斯诺登泄密事件的技术要点。这些并非完全来自蓝色;之前有很多关于信号情报收集的披露。大卫·卡恩 (David Kahn) 颇具影响力的密码学历史通过描述直到第二次世界大战 [1001] 开始之前发生的事情来设定场景。一位匿名的前 NSA 分析师,后来被确认为 Perry Fellwock,随后在 1972 年透露了 NSA 的运作规模 [674]。 “国家安全局的信息收集工作已经完成，”他写道。 “它涵盖了外国政府正在做什么,计划做什么,过去做过什么:什么军队正在向哪里移动以及针对谁;什么空军正在向哪里移动，他们的能力是什么。 NSA 确实没有任何限制。它的任务从在越南召集 B-52 一直到监视苏联太空计划的各个方面。”

虽然 Fellwock 的动机是反对越南,但下一个主要的告密者是英国战时密码破译者 Frederick Winterbotham,他想写一部关于他在战时成就的回忆录,并且在他快要死的时候，并没有为起诉而烦恼。 1974 年,他透露了盟军在那场战争 [2031] 期间成功破解了德国和日本的密码系统,这导致了更多关于第二次世界大战信号情报 (Sigint) 的书籍的出版 [438, 1002, 2007]。

此后,调查记者慢慢揭露了一些消息,其中有不少消息来源担心官方监控他们不应该监控的目标（例如国内政治团体)的腐败或滥用设施。举报人 Peg Newsham 透露,NSA 非法窃听了参议员 Strom Thurmond 打来的电话 [373, 374]。詹姆斯·班福德 (James Bamford) 通过公开来源和与前雇员的交谈 [160] 拼凑了大量有关 NSA 的信息,而新西兰记者尼基·海格 [849] 在新西兰情报界未能遵守命令后挖掘出了大量信息从他们的总理那里降级与美国的情报合作。

美国经济间谍活动的首次高调曝光是在 1999 年提交给欧洲议会的一份报告中 [644],该报告担心在苏联解体后,欧盟成员国正成为美国国家安全局的主要目标 [377 ].到那时,关注的人已经意识到数据、传真和电话会在大量节点上被收集,这些节点包括国际通信电缆在友好国家的着陆点（或在水下秘密窃听），通过观察往返商业的流量通信卫星和特殊的 Sigint 卫星收集

跟踪敌对国家,到成员国大使馆的监听站[644]。

冷战期间,大部分努力都是军事方面的,目的是了解苏联的雷达和通信,并在位置、干扰和欺骗方面获得决定性优势。没有进行电子战的能力,现代国家在空战、海战甚至坦克战中都没有竞争力。美国国家安全局的大部分人员都是军人,其负责人一直是现役将军或海军上将。在了解潜在对手的信号方面仍需付出大量努力。

有人可能会质疑这个庞大的全球体系是否仍然物有所值。自 9/11 以来,政客们就恐怖主义问题为其预算辩护,并且在打击恐怖分子方面确实取得了一些成功 特别是逮捕了一名涉嫌 9/11 恐怖主义的策划者,因为他使用了已知恐怖分子购买的一批手机 SIM 卡在瑞士。但是,正如我在第 19 章中所讨论的那样,针对伊拉克叛乱分子的电子战被证明效率较低。而且很明显,人类的智能应该付出更多的努力。在 9/11 之前发表的一篇文章中,一位分析人士写道:“中央情报局可能没有一个真正合格的中东背景的说阿拉伯语的官员可以扮演一个可信的穆斯林原教旨主义者,他自愿与他共度一生。阿富汗山区的食物很糟糕,没有女人。看在上帝的份上,大多数病例都住在弗吉尼亚州的郊区。我们不做那种事。”另一个人甚至更直截了当地说:“将腹泻作为一种生活方式的手术不会发生”[758]。

在阿富汗、伊拉克、叙利亚和北非战争爆发近二十年后,我们还没有训练足够多的士兵用阿拉伯语、达里语或普什图语进行基本对话。

尽管其他国家可能会抱怨美国的 Sigint 收集,但他们对此进行道德说教是虚伪的。其他国家也开展情报行动,而且在进行经济和其他非军事间谍活动时往往更加积极。五眼联盟国家与其他国家之间的真正区别在于,没有其他人建立过“体系之体系”。事实上,Sigint 和其他地方一样存在网络效应:虽然像印度这样的不结盟国家很乐意从前苏联购买战机,但如今它们倾向于与美国共享情报,因为它拥有更大的网络比俄罗斯人或中国人 [84]。斯诺登文件揭示了 NSA 与其他 60 多个国家共享信息。

我自己的观点是,就像他们经常参与的武装部队一样,信号情报机构既是必要的,又是潜在危险的。一支军队可以是一个好仆人,但很可能是一个令人无法忍受的主人。问题不在于这些资源是否应该存在,而在于如何追究它们的责任。在美国,丘奇参议员在 1975 年举行的听证会详细描述了一些侵权行为,例如对美国公民的非法监控 [423];这导致了 FISA。斯诺登的揭露反过来导致美国政府的所有三个部门都采取了行动,尽管效果有限3。

不过,结构性问题依然存在。国家安全局对两者负责

3 奥巴马总统成立了 NSA 审查小组并接受了其大部分建议,但他的积极工作被特朗普总统毁掉了。国会通过了美国自由法案,该法案对美国机构大量收集美国居民的通信数据施加了一些限制。首席大法官罗伯茨对 FISA 法庭做出了一些改变。

攻守兼备,而防守往往处于次要地位。想象一下,您是美国国家安全局局长,您的一位工程师带着一个很酷的新 Windows 零日攻击来找您。你是告诉微软,从而保护 3 亿美国人,还是保密,这样你就可以攻击 12 亿中国人?用这些术语来说,答案是显而易见的。这个股票问题是奥巴马总统拒绝听从美国国家安全局审查小组建议的一个问题。该小组建议,在几乎所有情况下,应将引起美国国家安全局注意的漏洞报告给供应商以进行修复； NSA 更愿意储存它们。事实上,它为 Bullrun 制定了 100 美元的年度预算,这是一个通过公平和犯规的方式将它们插入商业产品的程序,如第 2.2.1.5 节所述。当错误自然发生时,美国国家安全局会尽可能地使用它们;例如,2014 年有报道称,SSL 中具有巨大破坏性的 Heartbleed 漏洞在被独立发现并修复之前已被美国国家安全局利用了两年 [2065]。

在一些国家,情况更清洁:在法国和德国,都有独立的攻击和防御机构。但在大多数国家,甚至都没有讨论对情报的监督。在英国,只有欧洲法院才迫使政府承认监视的规模,并通过立法对其进行一些控制。新的案例不断突出了电子和人工方法的过度收集。 2019 年,欧洲人权法院命令英国警方从其“极端主义”数据库中删除约翰·卡特 (John Catt) 参加的大约 60 次示威的记录,约翰·卡特是一名 94 岁的抗议者,没有犯罪记录 这一判决即使在保守派出版社 [2024]。

这是监控在过去几十年中如何演变的高层次图景。另一个方面是规模。跨境带宽从 2007 年的 11Tbit/sec 增加到 2017 年的 704Tbit/sec,当时正在构建 Ed Snowden 描述的系统;这种消防水管给机构带来了更大的压力,要求他们从 CSP 或其他边缘系统而不是从 ISP 或骨干网收集流量,因为他们可以更好地定位收集。由此产生的政府访问数据的压力与 1990 年代政府访问加密密钥的压力非常相似,这是许多政府（以及行业和民间社会)在监视和技术政策问题上的形成性经验。

## 26.2.7 加密战争

1990 年代的技术政策主要是关于密钥托管的激烈辩论 克林顿政府的信条是,任何加密数据的人都应该向政府提供密钥副本,这样民用密码学就不会干扰情报收集。

我作为研究和教学受到拟议控制措施威胁的学者之一参与其中,1998 年,我是建立信息政策研究基金会的人之一,这是一家英国互联网政策智囊团,它与加密政策、出口政策、版权和相关问题。 2003 年,我们与其他欧洲非政府组织一起成立了欧洲数字版权 (EDRi),以在布鲁塞尔就这些问题开展活动。在接下来的几节中,我将简要介绍加密战争的背景,然后讨论政府为何未能控制住互联网。

#### 26.2.7.1 加密政策的背景故事

许多国家在 19 世纪中叶制定了法律,禁止在电报中使用密码技术,有些国家甚至禁止使用批准列表以外的语言。普鲁士甚至要求电报运营商保留所有消息明文的副本 [1818]。有时借口是执法 阻止人们在“官方”传输之前获得赛马结果或股票价格 但真正的担忧是国家安全。这种模式在 20 世纪再次重演。

在第二次世界大战期间盟军在信号情报方面取得巨大成功后,英国和美国政府于 1946 年同意继续开展情报合作。加拿大于 1948 年加入,澳大利亚和新西兰于 1956 年加入这项“BRUSA 协议”,在信号情报方面建立了“五眼联盟”伙伴关系。他们决定阻止密码设备和技术诀窍的扩散。直到 1980 年代,几乎唯一的供应商是向政府市场销售产品的公司,他们大多可以相信不会在海外做任何会令国内主要客户不高兴的事情。出口管制加强了这一点,出口管制“以尽可能隐蔽的方式进行,对任何想要出口许可证的人提供最少的公开指导。大多数事情都是在官方与潜在出口商的可信赖代表之间进行的幕后谈判中完成的。” [206]

在这些谈判中,当局会尝试引导申请人尽可能使用弱密码,并且在遇到更复杂的用户时会尝试确保系统有“后门”(在行业中称为红线)这将允许访问 trac。任何试图在国内销售体面的加密货币的人都可以通过各种方式被劝阻。如果他们是一家大公司,他们将面临失去政府合同的威胁;如果规模很小,他们可能会在试图获得许可证和产品批准时被繁文缛节扼杀。结果是大多数政府都使用弱密码,而 NSA 可以轻松破解它。但这还不是全部,正如我们在 Buhler 案例中了解到的那样。

..

..

Hans Buhler 曾在瑞士公司 Crypto AG 担任推销员,该公司是一家领先的加密设备供应商,向政府提供加密设备,但没有技术能力自行构建。他于 1992 年在伊朗被捕,当时当局发现伊拉克人在两伊战争期间一直在阅读他们的踪迹;他们指责他向他们出售被篡改过的密码机,以便国家安全局可以获取明文。 Crypto AG 支付了 14.4 亿里亚尔(约合 100 万美元)保释他,但在他回到瑞士后解雇了他。布勒随后在瑞士广播电台和电视台声称,该公司由德国情报部门秘密控制,多年来一直从事情报工作 [335]。一个故事是,当 Crypto AG 的创始人 Boris Hagelin 决定退休时,他联系了 NSA 的首席科学家 William Friedman; Friedman 是一位朋友,美国政府是一位大客户,在第二次世界大战期间购买了 Hagelin 机器。

哈格林将他的公司秘密卖给了美国国家安全局,后者由德国提名人秘密控制。它出售的设备通常是红色螺纹 [1205]。
Crypto AG 的说法是,这些指控是由美国国家安全局炮制的,目的是

破坏公司,因为它是第三世界为数不多的加密设备来源之一。 Res Strehle [1837] 在一本书中讲述了布勒的故事。
现在已知 Crypto AG 由德国 Bundesnachrichten dienst 与丹麦、瑞典、荷兰和法国的机构以及中央情报局合作运营。例如,英国在 1982 年福克兰群岛战争期间使用他们设备中的后门来破译阿根廷的通信 其结果“即使没有决定,也受到了重大影响”[970]。

### 26.2.7.2 DES 和密码研究

尽管早期的银行密码系统质量很差,但美国国家安全局在 70 年代仍然担心银行业可能会进化出好的算法,而这些算法会逃到野外。许多国家仍在使用转子机器或其他设备,这些设备可以使用第二次世界大战中开发的技术来破解。银行业如何能够满足银行业对受人尊敬的密码的渴望,不仅在美国而且在海外,如果这种密码不被美国采用外国政府并推高情报收集成本?

解决方案是数据加密标准 (DES)。当时,正如我在 5.4.3.2 节中提到的,关于 56 位是否足够存在争议。我们现在知道这是故意的。 NSA 当时没有进行 DES 密钥搜索的机制;那是后来的。但通过给人的印象,他们成功地阻止了大多数外国政府采用它。转子机器继续使用,在许多情况下使用微控制器重新实现; Crypto AG 和其他可出价供应商继续蓬勃发展; trac 继续收获。使用此类密码加密其重要数据的外国人只是将该流量标记为值得收集。

第二项举措是破坏密码学的学术研究。在 1970 年代,这是通过骚扰相关人员直接完成的;到 1980 年代,它已经演变成一种更微妙的策略。虽然五角大楼资助了计算机安全研究,但它试图将密码研究转移到理论渠道,并声称更实用的已发表研究工作都是老生常谈:“我们三十年前就做了所有这些研究;现在我们已经做了所有这些研究”。纳税人为什么要付两次钱?暗示 DES 可能插入了一个“活板门”,这与该剧本非常吻合。我们仍然存在的一个副作用是,加密货币和计算机安全社区在 1980 年代初期彼此分离,因为美国国家安全局致力于让一个靠边站并建立另一个。

到 20 世纪 90 年代中期,这条线路已经耗尽。机构在密钥托管系统设计中的失误揭穿了他们在密码学方面远远领先于我们其他人的故事,无论如何,战斗转移到了不同的战场。

### 26.2.7.3 加密战争 1 – Clipper 芯片

随着 Clipper 芯片的推出,加密政策在 1993 年成为主流。在 AT&T 提议向美国国内市场引入一种加密技术之后

电话会使用 Die-Hellman 密钥交换和三重 DES 来保护流量,NSA 说服克林顿政府推广不同的标准。这将使用分类块密码 Skipjack,在防篡改芯片中实施,并使用一个协议使机构可以使用备用（“托管”）密钥来解密 trac。这个“托管加密标准”引起了公众的强烈抗议； AT&T 计算机科学家 Matt Blaze 在 Clipper 中发现了一个协议漏洞,该漏洞破坏了托管机制 [258],该提案被撤回。

在 1990 年代,人们又进行了几次尝试,以促进密码学的使用以及政府对密钥的访问。密钥托管获得了各种新名称,例如密钥恢复;保留其客户的私人解密密钥副本的证书颁发机构被称为受信任的第三方 (TTP) – 在某种程度上强调了 NSA 将受信任组件定义为可以破坏安全性的组件。在英国,为公共部门引入了一个密钥托管协议 [980],这被用来试图让私营部门也采用它;但我们也发现了其中的一些漏洞 [115]。

支持托管的人说,由于加密提供了保密性,而保密性可以帮助犯罪分子,因此需要有某种方法来击败它。反托管游说团体一开始就争辩说,既然加密是保护隐私所必需的,那么一定没有办法打败它。现实情况要复杂得多 [56]。大多数加密应用程序都是关于身份验证而不是机密性的,所以帮助警察而不是阻碍他们。至于罪犯,他们主要需要不引人注意的通信　而在 1990 年代,加密电话是引起人们注意的好方法。如果您想不引人注目,最好只购买预付费电话。至于隐私,大多数侵犯行为都是由内部人员滥用授权访问造成的。最后,对于警察来说,一个更为严峻的问题是找到可接受的证据,为此,体面的身份验证也会有所帮助。

辩论迅速与武器出口管制纠缠在一起,武器是传统上控制密码学的手段。美国软件公司不得出口包含难以破解的密码技术的产品,这也被用作国内控制密码技术的一种手段;将加密软件放在其网站上的美国人可能会因向外国人提供该软件而受到起诉。美国软件作者菲尔·齐默尔曼 (Phil Zimmermann) 在他编写的一个程序　PGP　“逃脱”到互联网后,因武器追踪而被带到大陪审团面前。随着他的产品占据市场领导地位,他成为了民间英雄并发了财。其他人,例如 Bruce Schneier,在书中印制了密码算法,作为行使宪法规定的言论自由权的一种方式 [1667]。冲突变成了国际性的:美国国务院努力说服其他国家也控制密码学（我将在下面关于出口控制的第 26.2.9 节中详细介绍）。在世界范围内实施美国政策成为副总统戈尔的使命之一（这也是许多技术人员在 2000 年为布什竞选活动做出贡献的原因）。

Crypto War 1 的明显解决分为两个阶段。 1999 年,欧盟单一市场专员 Martin Bangemann 推动通过了电子签名指令,该法律禁止认证机构的强制许可。这破坏了来自

NSA 和 GCHQ 认为所有私人签名密钥都应该被托管 不仅是解密密钥,还有签名验证密钥。德国人反对托管签名密钥不仅可以让这些机构读取消息,还可以伪造消息,从而破坏人们对电子商务和身份验证的普遍信任。当欧盟遵循德国路线而不是英国路线时,随之而来的是个人可以使用他们的签名密钥对进行加密,或者验证 Die-Hellman 密钥并使用它们进行加密。

欧洲官员安抚了美国政府,通过了一项出口管制条例,将欧盟的出口管制从有形商品扩展到软件等无形资产,因此欧洲公司面临与美国公司相同的加密软件出口管制 [651]。

其次,在 2000 年阿尔戈尔竞选总统并希望让硅谷站在一边时,政府决定叫停。这些机构和技术专业人士在匡蒂科的联邦调查局办公室举行了会议,达成了一项协议,即这些机构将不再推动将漏洞插入产品和系统。相反,这些机构会利用许多自然发生的漏洞,而美国国家安全局则诱使自己进入修补周期。当向 CERT 生态系统报告软件漏洞时,它会找到位于匹兹堡软件工程研究所的 CERT,该研究所由国防部赞助。这与 NSA 共享,并报告给供应商进行修复。补丁周期通常需要一两个月 如果很难协调漏洞披露和产品测试,有时会更长 给 NSA 一个利用漏洞的窗口。

我们这些在欧洲积极从事数字版权工作的人普遍对电子签名指令感到满意,但对无形的出口管制感到震惊;我们于 2003 年成立了欧洲数字版权 (EDRi),以在布鲁塞尔建立游说机构,得到欧洲国家数十个非政府组织的支持。我们认为监控问题已经基本解决,未来的斗争将围绕软件版权和数据保护等问题展开。2013 年,埃德·斯诺登 (Ed Snowden) 向我们展示了我们的错误。美国国家安全局和其他机构只是转入地下,一直在运行一个名为 Bullrun 的秘密计划,每年的预算为 100 美元,以破坏商业密码学,干扰标准、实施、供应链等。但那是后来的事。

Crypto War 1 的工程教训之一是,正确地进行密钥托管是很困难的。将两方安全协议变成三方协议会增加复杂性和出现严重设计错误的风险,并且集中托管数据库会产生巨大的目标;我在与其他 10 位密码学家合写的论文“密钥恢复、密钥托管和受信任的第三方加密的风险”中讨论了这一点,该论文成为该主题引用次数最多的参考文献 [4]。在需要托管的地方,通常最好使用简单的本地机制来完成。在一支军队中,每个军官都必须在一张纸上写下他的密码,把它放在一个信封里,在上面盖上“秘密”,然后交给他的指挥官,他把它放在他的办公室保险箱里。这样一来,密钥就与它们所保护的电子版本文件保存在同一个地方,而且没有中央数据库可供飞机轰炸或间谍窃取。但试图将其自动化并扩大规模会带来麻烦。英国政府的想法是,每个人的私钥都将使用他们的电子邮件地址生成

由 GCHQ 生成的超级机密主密钥保存在由其部门安全人员控制的设备中,以便部门和 GCHQ 都可以在必要时解密 trac。结果是一个笨拙的系统无法轻松应对政府部门重组和更名时频繁更名的问题。对定制中央控制的需求导致大量 IT 项目延期数年、超出预算数百万,或者根本无法运行。向社会提供有效电子邮件系统的问题导致他们转而使用私人帐户,最终卡梅伦政府或多或少地放弃了;内阁办公室(Top Secret 下的 stu )的日常电子邮件开始使用 G Suite 的品牌版本,即 Gmail 的付费版本。由于冠状病毒大流行,尽管已知存在不安全因素,但内阁仍在使用 Zoom 开会;事实上确实存在一个安全的视频会议系统,但由于它是机密的,部长们不能把它带回家。

加密战争 1 留下了重要的遗产,既有技术方面的,也有政治方面的。在技术方面,强制使用弱加密技术让 DVD 更容易被破解,让汽车更容易被盗,让蓝牙更容易被破解,并让数以百万计的建筑锁变得容易破解包括我工作的大楼 4。销售酒店门锁的公司的商业模式已被削弱,因为他们无法再锁定客户购买他们专有的卡片库存。至于政策,俄罗斯等专制政府通过了严厉的加密控制法;英国从 1990 年代中期约翰·梅杰 (John Major) 的自由放任政策转变为托尼·布莱尔 (Tony Blair) 的 2000 年调查权监管 (RIP) 法案,该法案使警察能够要求我交出我拥有的密钥或密码,以及出口管制2002 年法案规定,如果我将任何使用超过 56 位密钥的加密软件发送到欧洲以外的地方,就必须获得出口许可证5。我稍后会回到出口管制。

## 26.2.8 加密战争 2 – 参差不齐

爱德华·斯诺登 2013 年的披露导致加密战争在某种程度上重新开始。事实上,美国国家安全局及其合作伙伴从未停止过,只是将他们的“加密支持”活动转入地下。他们不仅从主干网收集每个人的 SMS 和电子邮件,还使用授权从主要服务提供商那里获取内容,其规模比我们想象的要大得多。他们是黑客盟友,就像 GCHQ 入侵 Belgacom [734] 一样 这是一个关于一个欧盟成员国如何攻击另一个成员国的关键基础设施,并继续窃听欧盟委员会的惊人故事。另一个例子是新西兰对五眼联盟的贡献,其中包括监视萨摩亚、汤加和法属波利尼西亚等小邻国 [850]。 NSA 曾向国会撒谎,例如收集美国公民的通话数据记录。他们绕过了法律控制:GCHQ 可以使用 Prism 从 Google 获取我的 gmail,因为我不是美国居民,我们一直怀疑这一点,但一直被拒绝。他们还通过秘密方式从主要服务中获取它 通过窃听谷歌数据中心之间的通信。

4 汽车盗窃见 4.3.1 节,蓝牙攻击见 5.7.2.2 节, [?]节见攻击门锁。

5谢天谢地,进行导出的人就是点击链接的人 所以如果你在伊朗,如果你点击我网站上的链接下载 Serpent 分组密码,那你就是一个非常糟糕的人。你被警告了!

2015年,英国一家法院裁定,英国通过美国获取英国居民的大规模监控数据是非法的,因为这违反了《欧洲人权公约》[304]。

所有这些都对行为产生了真正的影响。首先,服务提供商清理他们的行为;谷歌已经开始加密其内部网络,但加速了该计划,以确保获得用户数据的唯一途径是通过前门,并获得授权。微软和雅虎紧随其后。其次,大多数消息传递系统都提供端到端加密来让用户放心(同时也为系统运营商节省了遵守授权的成本)。第三,政策对话开始解决更现实的问题,例如管辖权;鉴于世界警察部队感兴趣的大部分材料都保存在属于美国公司的服务器上,谁可以访问它,以什么条件访问?英国等国家致力于更快地访问美国数据,而其他国家则致力于本地化。印度已经坚持要求所有私人黑莓用户将他们的消息保存在印度的服务器上;中国禁止Facebook 和谷歌,以确保其居民使用中国系统;许多国家/地区已通过数据本地化法律,以确保某些类型的个人数据保存在管辖范围内。例如,非洲的大多数国家都要求将财务数据保存在本地;稍后我将讨论欧盟的数据保护法规及其与美国公司的互动。

尽管这些机构不再要求获得所有密钥,但托管争论在斯诺登之后以新形式回归。 GCHQ 和 FBI 开始争辩说,应该强制 WhatsApp 和 FaceTime 等消息服务提供商建立一个设施,让执法部门可以作为一个沉默的电话会议方(所谓的“幽灵用户”)当他们获得逮捕令时。 FBI 局长 James Comey 与 GCHQ 局长 Robert Hannigan 一起领导了这项指控,后者在 2014 年指责 Facebook 帮助恐怖主义 [1566],要求他通过英国/美国司法互助条约的程序来获取信息。 Facebook 的回应是他们只是遵守美国和欧盟的隐私法;相关服务中心在爱尔兰,不在英国,所以汉尼根不能简单地用英国法律来强迫他们帮助他。他和科米得到了英国首相戴维·卡梅伦的支持。

我和我的密码学家同事再次聚在一起撰写我们分析的更新,“门垫下的钥匙”,它解释了 1990 年代的密钥托管提案中有多少问题只是以一种新的形式卷土重来,如果你要求政府访问数据而不是键 [5]。影响可能会更糟,因为我们现在比 1990 年代更加依赖互联网。如果政府强迫设计人员放弃安全机制,如前向保密、认证加密和严格的传输安全,这将是一件坏事;并且由于以不同方式保护的系统之间存在许多交互,因此强制性漏洞具有严重和未预料到的副作用的风险现在要大得多。内置特殊访问权限还会在窃听系统本身中创建巨大的目标,以及可能导致进一步安全故障的额外复杂性。事实上,2010 年中国对谷歌窃听系统的黑客攻击表明,即使是经营最好的公司也无法始终将国家行为者拒之门外 而这次黑客攻击的目标是系统

谷歌为窃听服务而生。中国人显然想知道他们在美国的哪些特工受到怀疑。围绕管辖权存在巨大问题。如果 Facebook 将来自法国用户的 WhatsApp 消息传送给阿根廷用户，是只有这两个政府可以访问，还是 NSA 也要求访问？自从斯诺登以来，每个人都知道他们会这样做，而且没有人相信他们能够控制住这种能力。对此类系统的任何需求都会引发许多法律和工程问题，我们在分析 [5] 中阐明了其中的一些问题。

下一步行动发生在 2016 年，当时 FBI 试图迫使苹果公司为 iPhone 生产一个操作系统“升级版”来解锁它，他们使用一部被锁定的 iPhone 作为他们的测试案例，该 iPhone 曾在圣贝纳迪诺的恐怖袭击中使用过。苹果公司的蒂姆库克此前曾顶住压力安装后门，认为此案对苹果用户隐私和苹果品牌构成严重威胁；他在法庭上与联邦调查局作斗争 [1006]。 Comey 作证说，如果没有 Apple 的帮助，该机构将无法获得如此重要的信息。

此案在美国产生了分歧，共和党人支持联邦调查局（当时的候选人特朗普呼吁抵制苹果公司），而大多数民主党人和科技行业则支持蒂姆库克。正如我在 3.4.8.3 中讨论的那样，我的同事 Sergei Skorobogatov 研究出了如何击败 iPhone PIN 重试计数器 [1777]。至于 FBI，他们从一家以色列公司 Cellebrite 购买了一个商业 iPhone 漏洞利用程序，并撤销了此案。

在英国脱欧公投后的混乱中，新任英国首相特蕾莎·梅（作为内政大臣一直是监视鹰派）推动英国议会通过了《调查权力法》。这项法律赋予部长们权力，命令任何公司采取任何实际可能的行动来促进信号情报收集，并永远保持沉默。 2018 年，GCHQ 的两位高级数学家 Ian Levy 和 Crispin Robinson 提出了政府访问消息服务的可能方式 [1153]；他们的想法是，当 GCHQ 向 Facebook 提供搜查令时，他们会悄悄地在目标的钥匙圈上添加一个 GCHQ 公钥，这样他们就可以成为他所有电话的无声会议方。我的同事 Bruce Schneier 详细回应 [1678]：事实上，这种方法适用于某些系统（它适用于 WhatsApp 但不适用于 Signal）实际上是一个错误，正在通过更好的透明机制修复，并且强制执行它会阻止错误修正。

无论如何，这样的访问权限是过大的；情报机构不应该拥有它，因为他们有滥用这种访问权限的历史，或者干脆失去它。在第 2.2.3 节中，我描述了 NSA 工具 EternalBlue 如何被俄罗斯人窃取并在 NotPetya 蠕虫中用于攻击乌克兰，在 2016 年对美国公司造成数十亿美元的附带损害；到 2019 年，它被用于关闭巴尔的摩市的电子邮件和其他服务的运行索软件，就在美国国家安全局 [1529] 的路上。

2019 年，马克·扎克伯格 (Mark Zuckerberg) 宣布，Facebook 将通过将 WhatsApp 与 Instagram 和 Messenger 统一起来，将其重点从公开帖子转移到临时的、端到端的加密消息 [1439]。一些愤世嫉俗者认为，这将更容易向媒体和法律隐藏假新闻和仇恨言论，并降低节制成本以及丑闻对公关的损害；其他人则认为这是为了防止欧盟或美国政府下令拆分公司 [1911 年，1931 年]。 10 月，美国

总检察长与英国内政大臣和澳大利亚内政部长一起要求扎克三思,强调“将无法访问的消息服务与公开配置文件结合在一起的单一平台的风险,为潜在罪犯提供独特的途径”识别和培养我们的孩子。时间会证明 Zuck 是否可以单独使用元数据进行滥用检测;我们将在下面考虑节制和其他形式的审查。

## 26.2.9 出口管制

加密战争的一个溢出效应是实施了比以前更统一的出口管制,尤其是在欧洲;这是一个快速总结。国际军备控制协议（COCOM 和 Wassenaar)约束大多数政府对加密设备实施出口管制,后者在欧盟通过一项欧盟法规实施,强制成员国控制和许可两用商品的出口 –兼具民用和军用的商品。密码分析产品属于军事制度,而仅使用加密技术进行保护的软件属于双重用途。

过去,国家政策差异更大,在 1990 年代,像我这样的欧洲研究人员可以编写加密软件并将其发布在我们的网页上,而我们的美国同事却被美国国际武器追踪条例 (ITAR) 禁止这样做。美国公司抱怨,1997 年,副总统戈尔说服即将上任的英国首相托尼布莱尔将出口管制扩大到无形资产。他最初试图将其出售给英国议会,但相关委员会并不热衷,因此布莱尔将其作为欧盟法规推动通过,然后他的部长们高兴地告诉我们“我们的手被束缚了 - 我们必须这样做,因为它是欧盟法”。 （这种所谓的政策洗钱在欧洲很普遍,也是推动英国退出欧盟的因素之一。）

数以万计的学者和小型软件公司现在在不知情的情况下通过出口包含密钥长度超过 56 位的加密产品（甚至赠送软件)来违反法律。您可以使用开放式通用出口许可证 (OGEL),但您必须了解其机制并提交文件。这不仅仅是密码学。例如,在我们的硬件防篡改研究中,我们使用离子束工作站,它就像电子显微镜,只是它向目标发射金属离子而不是电子,因此您可以通过切割轨道和添加新轨道来修改芯片。与密码学一样,这也在双重用途清单上。在过去,我们购买时必须获得出口许可证,七年后,当我们把它扔进料斗时,又要获得出口许可证。现在,理论上,每当我们与非欧盟公民或居民共享我们为机器编写的脚本时,我们都应该获得许可。实际结果是成千上万的科学家乐于违法 这可能使他们容易受到来自机构的压力。既然大流行导致许多人在家工作,通常是在海外工作,而且英国已经离开欧盟,那么这个数字肯定会飙升。我个人处理此类问题的方式是非常小心所有此类软件和脚本都在我的网站上,这使我能够使用公共域豁免,并依赖于点击的人这一事实

在执行导出的链接上。

2012年,叙利亚内战暴露了出口管制的阴暗面。数家数字版权非政府组织的人士游说英国政府,要求其利用出口管制法阻止一家英国公司向阿萨德政府出售大量监控设备。英国非政府组织认为,大规模监视设备不应仅列入两用清单,而应列入军事清单,情报界将批量收集纳入军事“密码分析”;将其出售给参与大规模侵权行为的政府是违反人权法的。 GCHQ 的女士竭尽全力抗争;销售是通过迪拜的一家军火商进行的,所以供应商如何确定目的地;他们来自一家德国子公司,所以这是德国人的问题; Wassennaar 是一个讨论军事问题而不是人权问题的论坛;甚至大规模监控也被用于营销。真正的问题是 GCHQ 担心英国军队最终会进入叙利亚,他们决定如果阿萨德总统要在他的网络上安装黑匣子,它们应该是英国的黑匣子而不是乌克兰的。最终,德国总理默克尔公开承认,她已决定允许向叙利亚出售监控设备,这是她做出的最艰难的决定之一。 2013 年 8 月,英国议会投票反对在叙利亚采取军事行动,奥巴马总统决定不再单干。

在适当的时候,出口管制问题被提交给欧洲机构并被悄悄遗忘。

这场斗争的一个令人不快的副作用仍然存在:英国大学的外国学生审查制度。 GCHQ 反对中国学生学习密码学,安全部门通报说,一名在英国获得博士学位的伊拉克妇女继续指导萨达姆侯赛因所谓的大规模杀伤性武器研究计划的一部分。通报者对来自苏丹等恐怖分子名单上国家的人获准学习医学表示恐慌。病毒学教授兼剑桥大学同事托尼·明森 (Tony Minson) 认为,大自然可以做比人类更恶劣的事情,如果埃博拉病毒从尼罗河下游而来时喀土穆没有称职的公共卫生人员,我们会后悔的。他当然被无视了。我们有一个“学术技术批准计划”,来英国的研究生必须获得“ATAS 许可”才能获得签证。

## 26.3 恐怖主义

谈论恐怖主义推动了很多关于监视和隐私的政策,尤其是自 9/11 以来。潮流开始退去,但这仍然是政客们想吓唬我们时打出的一张牌,媒体也经常配合。

人们一直在谈论网络恐怖主义;这基本上还没有发生,但人们确实担心加密聊天服务和社交媒体被用来培养和招募年轻人加入从右翼仇恨团体到伊斯兰国等犯罪组织。那么关于恐怖主义我们能说些什么呢?

政治暴力并不是什么新鲜事;人类学家发现,部落战争在早期人类中很流行,黑猩猩也确实如此 [1132]。

长期以来,恐怖一直被用来恐吓臣民 玛雅人,

印加,征服者威廉。 “现代”类型的恐怖主义也可以追溯到几个世纪以前。 1605 年,盖伊·福克斯 (Guy Fawkes) 试图炸毁英国议会大厦;他的继任者爱尔兰共和军发动了一系列反对英国的运动。最近,从 1969 年到 97 年,约有 3000 人死亡,爱尔兰共和军甚至炸毁了首相玛格丽特·撒切尔 (Margaret Thatcher) 下榻参加党内会议的一家旅馆,炸死了她的几名同事。在冷战期间,俄罗斯人不仅支持爱尔兰共和军,还支持德国的 Baader Meinhof Gang 和许多其他组织;西方武装并支持圣战分子在阿富汗与俄罗斯作战。一些恐怖分子,如巴德尔和迈因霍夫,最终入狱,而其他人 如爱尔兰共和军领导人格里·亚当斯和马丁·麦吉尼斯、伊尔贡领导人梅纳希姆·贝京、法国抵抗运动领导人戴高乐和非洲反殖民领导人乔莫·肯雅塔,罗伯特·穆加贝和纳尔逊·曼德拉 最终落入了办公室。

从这段历史中可以得出什么一般性教训?嗯,有好处
新闻和坏消息。

## 26.3.1 政治暴力的原因

最大的好消息是恐怖主义暴力的趋势一直在稳步下降 [1350]。 1960 年代和 70 年代有许多叛乱,有些是种族的,有些是反殖民的,有些是意识形态的。尽管有少数(特别是尼加拉瓜反政府武装和阿富汗反苏运动)是由西方资助的,但其中许多是由苏联或其盟友资助的,作为冷战中的代理人冲突。冷战的结束消除了动机和金钱。

第二点(也是相关的)是国内冲突的部分原因是经济原因。 Paul Collier 和 Anke Hoe er 为世界银行所做的一项有影响力的研究调查了 1960 年至 1999 年的战争,以了解它们是否主要是由不满情绪(例如高度不平等、缺乏政治权利或种族和宗教分歧)引起的,或贪婪(有些叛乱在经济上比其他叛乱更可行)[459]。世间怨声载道,但数据显示,叛乱的发生更多取决于能否持续。 (事实上 ,西塞罗在 2000 年前说过:“无尽的金钱构成了战争的力量。”)因此,爱尔兰共和军的运动得到了苏联集团和利比亚的大力支持;斯里兰卡的泰米尔人起义是由美国和印度的泰米尔人资助的;基地组织的资金来自海湾国家的富有捐助者。所以我们知道解决叛乱的一种方法:切断他们的货币供应。当然,这并不完全那么简单。苏联对非国大(以及安哥拉和莫桑比克)失去支持减轻了南非最后一届白人政府的压力,但给了他们与纳尔逊·曼德拉达成历史性和平协议的空间。

## 26.3.2 政治暴力的心理

不太令人鼓舞的发现来自心理学、政治学和媒体学者。心理学对潜在机制提供了很多见解。我在第 3.2.5 节中提到了影响启发式:人们依赖于影响,或者

情绪,概率的计算往往被忽视。幸福事件的前景,例如中彩票,会使大多数人对高赔率和低预期回报视而不见;同样,可怕的事件,例如恐怖袭击,会使大多数人忽视这样的事件极其罕见的事实 [1787]。大多数死于 9/11 的美国人可能是在决定开车而不是坐飞机后死于车祸的:在接下来的三个月里,从坐飞机到驾车的转变导致大约 1,000 人额外死亡,大约从那时起每年 500 [1677]。

在心理学和文化的边界上还有其他影响。 Tom Pyszczynski、Sheldon Solomon 和 Je Greenberg 对恐怖心理学的研究着眼于人们如何应对对死亡的恐惧 [1564]。他们在亚利桑那州图森市召集了 22 名市法院法官参加一项实验,要求他们为一名吸毒成瘾的妓女保释。他们首先接受了一份性格问卷,其中一半的人被问到诸如“请简要描述你想到自己的死亡时在你心中激起的情绪”之类的问题,以提醒他们我们终有一天都会死去。死亡率突出的法官设定平均保释金为 455 美元,而对照组设定的平均保释金为 50 美元 这对这样的实验产生了巨大的影响。进一步的实验表明,死亡率显着组不仅变得刻薄:他们还准备对做出某些公共行为的公民给予更大的奖励。

事实证明,当你提醒人们死亡时,他们会更加坚定地坚持自己的文化规范,更加有力地捍卫自己的世界观。

这有助于解释为什么网络恐怖主义还没有发生。黑掉几个变电站并关闭城镇的电力可能会带来极大的不便,但它不会像一个流血的孩子那样产生情感上的影响。媒体分析证实了这一点;覆盖率与死亡人数密切相关,每增加一具尸体,覆盖率就会增加 46% [1026]。

9/11 袭击使死亡成为人们关注的焦点,同时也是对民族和文化自豪感象征的攻击。很自然地,回应包括宗教(自 1950 年代以来最高级别的教堂出席率)、爱国主义(以对总统的高支持率的形式)以及对某些人的偏执。很自然,随着对袭击的记忆消退,社会会因为不同的核心价值观而重新两极分化。

奇怪的是,当他们被提醒他们终有一死时,保守派和自由派都会对外国学生写的反美文章采取更加两极分化的观点 除了在第一次提醒他们宪法的实验中,在这种情况下保守派比自由派更积极地捍卫学生的言论自由权 [1564]。

因此,一位试图在袭击发生后让一个国家团结起来的国家领导人应该不断提醒人们他们为什么而战。这就是最好的领导者所做的,从丘吉尔的无线电广播到罗斯福的炉边谈话。近年来,一些国家对恐怖主义采取了两党合作的方式 比如德国面对巴德尔-迈因霍夫帮,英国面对爱尔兰共和军。在其他情况下,政客们屈服于利用散布恐慌来获得连任的诱惑。

阿拉巴马大学对 200,000 多篇关于 2005 年至 2016 年美国发生的 136 次不同袭击事件的文章进行的一项研究表明,穆斯林袭击事件获得的新闻报道比其他恐怖袭击事件多 357% [1026]。伊斯兰教

极端分子有 78.4% 的时间被标记为恐怖分子,而极右翼极端分子只有 23.6% 的时间被确定为恐怖分子。政治领导确实很重要。也许最近最好的回应是新西兰总理杰辛达·阿德恩 (Jacinda Ardern) 对基督城枪击案的回应;她不仅立即将其描述为恐怖主义,而且拒绝透露枪手的姓名。另一方面,匹兹堡犹太教堂枪击事件被美国总统简单描述为“邪恶的大屠杀行为”。在每种情况下,媒体都会跟进 [1335]。

这里的动态是什么,哪种方法最有效?

### 26.3.3 机构的作用

有一个完整的学术主题 公共选择经济学 致力于解释为什么政府会按照他们的方式行事,它的创始人之一詹姆斯·布坎南 (James Buchanan) 也因此获得了 1986 年的诺贝尔奖。正如他在获奖演讲中所说的那样,“经济学家应该停止提供政策建议,就好像他们受雇于一个仁慈的暴君一样,他们应该关注做出政治决策的结构。”许多政府行为可以用公共部门决策者个人面临的激励来解释。官员建立帝国是很自然的,因为他们的排名是根据他们的控制范围而不是他们产生的利润。同样,政客们会最大化他们连任的机会,而不是公众的抽象福利。理解他们的决定需要方法论的个人主义 分析个别总统、国会议员、将军、警察局长和报纸编辑面临的激励,而不是一个国家的潜在得失。我们知道在制度设计上要谨慎,这样他们的领导者的激励与它的目标是一致的 我们给公司经理股票期权,让他们像股东一样行事。但这在政体中更难。总统和总理的等价物是什么?

国家利益如何界定?

公共选择学者认为,市场和政治都是交换工具。在前者中,我们寻求单独优化我们的效用,而在后者中,我们做同样的事情,但使用集体行动来实现我们在市场上由于外部因素或其他失败而无法实现的目标。政治进程因此容易出现特定类型的失败。代际讨价还价很难:政客现在很容易借钱买选票,然后把账单留给还不能投票的下一代。但为什么有些国家的公共债务比其他国家严重得多?简短的回答是制度很重要。政治结果关键取决于限制政治行动的规则。

尽管公共选择经济学是在 1960 年代为应对公共财政问题而出现的,但它也有一些明显的教训。宪法很重要,因为它们设定了政治游戏的基本规则。行政结构也是如此,因为社会也是自利的代理人。例如,在英国,对 9/11 事件的最初反应是增加安全部门的预算;但这亿美元左右并没有为安全工业联合体提供真正的猪肉。因此,所有的宠物项目都落空了 ,政治选美比赛由国民身份证赢得,这是一个宏伟的项目,其原始形式将耗资 200 亿英镑 [1182]。华盛顿内部人士评论说,入侵伊拉克的决定也涉及类似的动力:尽管 2001 年的入侵

尽管阿富汗的军事行动取得了成功,但它并没有给五角大楼的大亨们带来多大的作用,他们的职业生涯一直在组装坦克、主力舰和战斗轰炸机的舰队,也没有给国防工业带来多少回报。事实上,美国空军上校 Karen Kwiatkowski 在伊拉克战争开始时退休,描述了情报评估是如何被政治操纵的,后来竞选国会 [1113]。类似的事情在第一次世界大战之后被说出来,这被归咎于“死亡商人”。

特别值得关注的机构必须是媒体,无论是老式媒体还是正在接管其某些功能的社交媒体。

俗话说,“如果它流血,它就会领先”;坏消息比好消息卖得更多。
媒体所有者的自身利益与想要连任的政客、想要建立帝国的官员以及想要出售安全设备的供应商的利益结合在一起。他们发现并放大了爱国主义的暂时现象以及恐怖袭击自然而然灌输的对英雄的需求。恐慌让政治家登上头版并帮助他们控制议程。许多社交媒体平台的推荐算法学会了促进恐惧和愤怒,因为它们增加了人们在平台上花费的时间和他们点击的广告数量。

## 26.3.4 民主回应

然而,人们也会随着时间的推移而学习。全世界对 9/11 的反应很强烈;四年后,即 2005 年 7 月,四名自杀式炸弹袭击者在伦敦的公共交通工具上炸死 52 人,炸伤约 700 人。发生 - 如果你在那里运气不好,但生活还在继续。 6

随着人们学习,政治精英也可能学习。约翰·穆勒 (John Mueller) 撰写了历届美国政府对恐怖主义态度的历史 [1350]。
肯尼迪、约翰逊、尼克松和福特总统无视恐怖主义。卡特总统对伊朗人质危机非常重视,就像 9/11 一样,一开始他在民意调查中获得了巨大的提升,但后来结束了他的总统任期。他的国务卿赛勒斯万斯后来承认,他们应该淡化这场危机,而不是给予绑架美国外交官的伊朗“学生”不当的信任。里根总统大多无视挑衅,但屈服于黎巴嫩人质问题的诱惑,将武器运往伊朗以确保他们获释。然而,一旦他摆脱了这个错误,他的收视率很快就恢复了。在美国,人们厌倦了布什总统基于恐惧的政策,并选举了奥巴马总统,他的路线是“9/11不是吓票的方式世纪”。英国的情况也差不多,玛格丽特·撒切尔 (Margaret Thatcher) 在将恐怖分子视为普通罪犯后两次连任。后来,托尼·布莱尔玩起了恐惧游戏,他的离开让人们松了一口气;他的继任者戈登·布朗禁止大臣们使用“反恐战争”一词,大卫·卡梅伦的政府继续这样做。成熟的选民更喜欢勇敢地对抗恐怖分子的政治家

6 媒体也跟着这样做了几天:然后恐慌情绪爆发了。部长们似乎需要一两天的会议来整理他们的购物清单,并决定他们将试图从议会中摆脱出来的东西。

而不是将它们用作竞选连任的道具。

最严厉的老师可能是冠状病毒。多年来，大流行病一直位居英国风险登记册的首位，但为应对大流行病所做的准备远远少于反恐措施，其中许多措施都是炫耀而不是有效的。这种资源分配不当给我们造成的损失看起来比任何恐怖分子所梦想的要多得多。美国和英国政府在 2000 年代通过谈论一个基地组织小组窃取核弹并在纽约或伦敦引爆它来为酷刑辩护。然而，与 1918-19 年大流行中死亡的 50-1 亿人相比，在一个大城市发射的 10 kT 原子弹爆破弹药可能会夺去 50-100,000 人的生命。恐怖言论以牺牲公共卫生为代价提振安全机构，使美国、欧洲、印度和非洲的政府无视 2003 年 SARS 的教训 这与中国、新加坡、台湾和韩国的政府不同。

## 26.4 检查

我在第一版中写道，“1990 年代关于加密货币政策的辩论可能是一场更大的战斗的试运行，这场战斗将涉及匿名、审查制度和版权。”到第二版时，我注意到“版权法已基本稳定下来”，正是在 2008 年，内容分发的权力从音乐巨头和好莱坞转移到了苹果和亚马逊等科技公司。我还注意到“在过去几年中，审查制度已成为一个更大的问题”。十年后的现在，审查制度成为重中之重。它有两个方面：国家审查和服务公司的内容过滤。

统治者长期以来一直在审查书籍，尽管印刷机的发明使他们的工作变得更加困难。当约翰·威克利 e 于 1380-1 年将圣经翻译成英语时，他发起的罗拉德运动与农民起义一起遭到镇压。但是，当威廉·廷代尔 (William Tyndale) 在 1524-5 年再次尝试时，印刷让他把这个词传播得如此之广，以至于王子和主教们无法压制它。他们把他烧死在火刑柱上，但那时已经印刷了 50,000 多册新约，宗教改革正在进行中。在那次挫折之后，打印机得到了严密的许可和控制；直到十八世纪，事情才缓和下来。

如今的审查出于各种动机。大多数国家屏蔽儿童性虐待图片；在 1990 年代，随着互联网繁荣的兴起，政府开始在互联网上寻找一些处理方式，并且出现了一种观点，即所有州都同意应该禁止的一件事是儿童性虐待的图像。在适当的时候，2004 年网络犯罪公约要求签署国禁止 18 岁以下儿童的性图片。大多数政府走得更远，阻止某些仇恨言论。英国禁止通过美化恐怖主义来“激化”年轻人的网站。最后，审查制度有时由法院实施。

互联网的发明使审查员的工作在某些方面变得更容易，但在其他方面却变得更加困难。当局更容易下令更改很多人不关心的材料：例如，法院发现一家报纸犯有诽谤罪，命令删除违规材料。改变历史

当它由图书馆的物理副本组成时,物理记录是不可能的,而人类知识在少数公司的服务器上的集中 从亚马逊的电子书系统到主要新闻机构的服务器 让我们,某种意义上,回到15世纪。当局也更容易观察到被拒材料的传输,因为他们可以比物理包裹更容易地监控电子通信。另一方面,如今每个人都可以成为出版商;许多真正令人不快的在线材料来自数以百万计的个人匿名发布到社交媒体、报纸的评论页面以及他们希望骚扰和恐吓的个人。审查员已经学会了利用这一点。十年前,中国有数以万计的人压制异议言论,而现在他们有数以百万计的公民志愿者来压制异见言论。曾经,言论稀少,审查员试图让发言者保持沉默;现在是听众的注意力稀缺,所以不同的策略起作用了。

为了梳理这些问题,让我们看看一些背景。

## 26.4.1 独裁政权的审查

当我写这本书的第二版时,我对中国政府审查所有在线内容的尝试会失败持谨慎乐观的态度。

然而,那里的当局在压制党控制之外的任何形式的组织和人类团结方面变得越来越有效。

到 2006 年,观察家们注意到,对地方新闻事件的在线讨论导致了“公众舆论”的出现,这是第一次不受媒体管理者的控制 [1470]。当时中国有 1.37 亿互联网用户,其中四分之一的人口生活在大城市,而“中国防火墙”已经是一个复杂的控制系统,可以对从色情到宗教材料等一系列材料进行纵深防御。政治异议 [1469]。防御在三个层次上起作用。

首先,有外围防御。中国的边界路由器对 IP 地址进行过滤,以阻止访问已知的“不良”网站,如美国之音和 BBC;他们还使用 DNS 缓存投毒。 TCP级别的深度数据包检测用于识别包含“法轮功”等违禁词的电子邮件和网页;这种联系被拆除了。十年前,大部分工作都是在这个级别完成的。如今,由于大多数 trac 都是加密的,所以这并不容易。 2020 年,防火墙开始使用加密服务器名称指示 (ESNI) 删除 TLS 1.3 trac,因为这会阻止审查员告知 trac 将去往哪个子域;到 7 月初 [433],这已超过 trac 的 30%。

其次,有应用程序级别的防御,现在可以完成大部分工作。
如今,有些服务被屏蔽,有些则没有,这取决于服务提供商是否准备好帮助政权进行监视和审查。谷歌和 Facebook 基本上被封锁;中国反而推广了腾讯、阿里巴巴和百度。既然最重要的边界是企业边界而不是国家边界,中国政府已将其产业政策与其政治结合起来。这是一个很大的变化;十年前我们从不相信中国会建立一个完整的中资生态系统

在线服务提供商以阻止西方的影响。语言是一个障碍,但也存在强大的技术障碍:边界防御现在的重点是阻止中国居民可以用来使用未经批准的服务的 Tor 和 VPN。

第三,存在社会防御。十年前就有3万名网警;现在有更多的公民参与了这个过程,与其试图阻止所有持不同政见者的言论,不如将其淹没。忠诚的公民应该发表大量支持政府的评论,并激怒任何批评当局的人,无论是地方的还是国家的。社会信用体系为人们的这种亲社会行为提供了积极的分数,而他们可能会因为任何被认为是反社会的行为而被扣分。在线监控正在与物理空间监控相结合,例如通过具有人脸识别和情绪识别功能的闭路电视摄像机 这在藏族和维吾尔族等少数民族反叛人口的地区尤为激进。自 2014 年以来,新疆的“再教育”系统率先融合了西方“反恐战争”和毛泽东社会控制的技术,导致数十万穆斯林在评分系统的基础上被拘留输入包括嫌疑人是否定期祈祷或手机上是否有 VPN。

美国国会谴责该政权犯有“危害人类罪”:数十家承包商公司已被列入制裁名单 [359]。

因此,中国似乎正在使用民粹主义但专制的技术赢得审查之战。俄罗斯的互联网相当开放,虽然政府有一个盟友接管了主要的社交网络,并组织了巨魔军队来压制对手,但反对派政治家阿列克谢纳瓦尔尼拥有自己的拥有数百万观众的 YouTube 频道,并试图审查员 Telegram 遭到街头抗议。普京以“数字主权”法进行反击,使他能够命令互联网服务提供商安装监控和审查设备。

阿拉伯之春也很重要。这一系列的起义于 2010 年 12 月在突尼斯开始,当时一名街头小贩穆罕默德·布瓦齐兹 (Mohamed Bouazizi) 在一名官员没收他的商品并羞辱他后自焚。抗议活动是使用 Facebook 和其他社交媒体组织的,导致政府垮台,并蔓延到邻国。埃及政府连同利比亚和也门的政府也垮台了;在埃及的案例中,一名谷歌员工 Wael Ghonim 在警方将一名男子殴打致死后转变为互联网活动家,因为他怀疑他有他们参与毒品交易的视频证据。叙利亚政府几乎垮台,但在一场造成数十万人死亡、数百万人流离失所的内战中进行了反击。

其他一些阿拉伯国家,如巴林,遭受了严重的动荡和镇压。正如我在 2020 年所写的那样,只有突尼斯成功地向民主过渡。在埃及,一位军事独裁者被另一位取代;利比亚一片混乱,也门和叙利亚一样,饱受战争折磨。世界上的独裁者得到的教训是,要想继续掌权,最好学习中国的做法。阿拉伯国家确实对互联网进行审查(大多数欠发达国家也是如此),但使用 VPN 或 Tor 仍然很容易攻破它们的基础设施。他们还购买用于批量监视和有针对性工作的工具包;有关阿联酋如何雇佣美国雇佣军建立相当于 NSA 的描述,请参阅 Bing 和 Schectman [247]。

阿拉伯之春在多大程度上是技术的作用,而在 2011 年,Facebook 和谷歌等公司在事情似乎进展顺利的情况下,在多大程度上只是营销炒作?目前还不清楚。一些崛起的民众很少使用互联网,尤其是利比亚和也门的民众;另一方面,2007 年缅甸的一场叛乱是由互联网催化的,尽管只有 1% 的人口可以上网 [1471]。在阿拉伯世界,卡塔尔半岛电视台可能比互联网做得更多,它播放该地区其他地方起义的新闻视频。

## 26.4.2 过滤、仇恨言论和激进化

民主国家关于仇恨言论的法律差异很大。一方面,美国对言论自由有宪法保护;法国和德国也是。但解释不同。法国和德国都禁止销售纳粹备忘录 rabilia,仇恨言论（ Volksverhetzung ）在德国几十年来一直是一种犯罪行为。 2018 年 1 月,当局开始对在线服务提供商强制执行,如果任何拥有超过 200 万客户的服务提供商未在 24 小时内删除任何此类材料,将被处以 500 万英镑的罚款。

无论服务公司对消除坏学生的成本怎么说 ,德国的例子表明他们可以在必要时做到。许多国家现在禁止恐怖主义材料和极端暴力,其定义从来都不是直截了当的。不仅要禁止斩首视频,还要禁止所有谋杀视频,例如贩毒团伙射杀不还债的顾客,这似乎是一件好事。但它很快就会变得复杂。执行此类政策的平台最终会删除当地杀戮和侵犯人权行为的证据

海外。

您放在网上的大部分资料已经被自动过滤,以查找当地法律或平台服务条款禁止的资料。 Facebook 前首席信息安全官亚历克斯·斯塔莫斯将隐私和审查制度之间的紧张关系描述为一个范围:人们希望 WhatsApp 等端到端加密聊天是私密的而不是被审查的,广播媒体是被审查的而不是私密的,并且很难接受 在中间,比如 Facebook 群组。到目前为止,大多数社交媒体都受到审查。平台差异很大； Facebook 可能是最严格的,甚至禁止裸体7;尽管它对特朗普总统的仇恨言论比其他人宽容得多,但作为回报,它似乎在反托拉斯方面受到的关注要少得多 [1790]。专制国家越来越积极地迫使服务公司屏蔽他们认为非法的内容;例如,Facebook 的服务在 2020 年初在越南变得缓慢,直到该公司同意压制异议 [1506]。

试图发现被禁止内容的人工智能系统背后是成千上万的内容审查员。过滤是昂贵的,成本不仅是经济上的,还有人力上的;我们已经看到越来越多的新闻报道关于员工的心理伤害,他们不得不整天观看帮派谋杀和恐怖分子斩首、虐待动物、虐待儿童和其他联合国的视频

7Facebook 禁止女性乳头照片,但不禁止男性乳头照片,因此 2019 年,数十名裸体女性在纽约示威,将男性乳头的照片举在自己的照片上;男人和女人用女性乳头的照片展示 [616]。

愉悦 [1438]。许多主持人在欠发达国家;正如我们在那里倾倒了很多令人不快的垃圾一样,我们也倾倒了很多互联网上最讨厌的垃圾 [414]。将审查外包给大型服务垄断企业也是有问题的。他们以准司法的方式行事,规范着数十亿人的言论,但没有我们期望的政府决策的透明度和正当程序。世界看到他们允许有钱有势的人滥用权力而无视弱者。公司依附于权力然后试图指导政治言论也许是不可避免的;这已成为对整个科技行业的强烈抵制的一个因素。

争论的焦点之一是美国 1996 年《通信规范法》(CDA) 第 230 条,其中规定“交互式计算机服务的提供者或用户不得被视为另一信息内容提供者提供的任何信息的发布者或发言人”,因此平台不对用户提供的不良学习承担责任;它还让平台可以自由删除任何“淫秽、淫荡、好色、肮脏、过度暴力、骚扰或其他令人反感的内容”。在通过 CDA 时,国会担心对内容进行审核的公司可能会被视为出版商并对所有内容(包括侵犯版权和诽谤)承担责任,而没有这样做的公司将被视为分销商并逃避责任。我们如何在不扼杀创新的情况下获得民用互联网?第 230 条使像 YouTube 和 Facebook 这样的公司成为可能,但保护其商业模式基于报复色情、诽谤或从非法枪支销售中分一杯羹的网站 [1419]。它还使服务公司能够获得国家的一些权力。那时候,互联网有 10 到 2000 万用户,其中大部分是极客;现在大多数人类活动都在网上进行,由少数美国公司担任 200 多个国家的审查员、检察官和法官是不可持续的。因此,CDA 和其他地方的类似法律开始被削减:美国 2018 年制定了性追踪法,欧洲 2019 年制定了版权法 [1598]。紧张局势只会变得更糟。

在制定限制言论的法律时,最好停下来看看历史背景。 Tim Wu 的“注意力商人”[2050] 是自 1830 年代第一批大众市场报纸出现以来的宣传史,充斥着可怕的犯罪报告和专利药品广告;这为政客们提供了第一个工业大众市场渠道。收音机紧随其后,并被希特勒巧妙地使用。其次是电视,它的本质是由广告塑造的;人们发明了智力竞赛节目、肥皂剧和其他许多东西来吸引眼球。第二个有用的观点是 Yochai Benkler 分析 2016 年美国大选的“网络宣传”。他追溯了政治两极分化的历史,并认为造成这种结果的根本原因不是技术或俄罗斯的干涉,而是过去 20 年来发展起来的左右不对称的媒体系统;左翼和中右翼是基于事实的,而右翼是宣传反馈回路 [227]。第三个观点是前 Google 员工 Tristan Harris 对推荐系统的批评:平台的算法了解到,为了最大限度地延长人们在网站上花费的时间,应该向他们提供引发恐惧、焦虑和愤怒的文章。

政府对假新闻的反应大多是无效的。最有能力的可能是芬兰,自沙皇时代以来,它一直是俄罗斯宣传的目标。自 2014 年以来,其政府一直在学校和其他地方推广批判性思维和媒体素养,使其成为每个公民的工作

发现和反击旨在播种分裂的信息。在英国,我们制定了旨在取悦小报而不是反对它们的法律。中小学教师和大学教授应该报告似乎有被激进化风险的学生,并制定程序来确定研讨会或其他谈话是否会使他们激进化;还有一些法律禁止在线材料,这些材料可能会使他们误入歧途。如果始终如一地采用这种方法,可能会导致沙特阿拉伯 [1263] 宗教机构制作或资助的大部分文学作品遭到禁止,但短期内不会针对我们最大的武器出口客户采取行动。白人至上主义者至少是一个威胁,他们在英国脱欧运动期间谋杀了英国议会的一名成员;但我们的政府并不热衷于打击他们,那些因在竞选活动中花费过多金钱(包括俄罗斯的钱)而违法的人最终并没有入狱,而是成为了政府的核心人物。总的来说,互联网审查让政府声称它在做某事,但实际上效果不佳,并且破坏了我们的外交官可能对世界独裁者发表的关于言论自由的任何言论。我宁愿执行现有的关于煽动谋杀(和竞选资金)的法律,公开其他政治材料,让警察监控到最糟糕地点的交通,并培训他们更好地使用现有法律 [642 ]. 从长远来看,关键是教育,正如芬兰所表明的那样。

至于针对穆斯林学生,这直接违背了犯罪学证据。为数不多的加入极端主义组织的英国学生是那些在社会上缺乏尊重的人,也许被同龄人拒绝,正在寻找身份认同但在父母的宗教信仰中找不到 - 然后陷入了一小群其他心怀不满的年轻人。

他们受到激进传教士的影响,他们提供理想、社区、亲情、关怀和兄弟情谊。白人男孩激进化为白人至上主义团体并没有太大的不同 。 Max Abrahms 的研究还表明,恐怖分子加入他们的运动大多是为了寻求社会团结;这就是为什么他们从孤独的年轻人而不是从政治活动家中招募人员。他们的团体成为成员所依附的机构,而不是变革的推动者;这就是为什么他们可以用增加的暴力来回应明智的和平提议,并沉迷于与类似群体的自相残杀的冲突 [6]。事实上,正如 Lydia Wilson 在采访了大量前往叙利亚加入 Daesh 并最终被关进库尔德监狱的年轻人后指出的那样,年轻人(偶尔还有女性)通过加入恐怖组织来找到自己身份的过程或犯罪团伙无异于通过加入宗教、体育俱乐部或舞蹈乐队来寻找身份 [2022]。我们在第 2.5.1 节中讨论过的 Gamergate 剧中 Zoe Quinn 最近对愤怒的在线暴徒的体验得出了大致相同的结论 [1567]。加入极端组织以寻求社会团结的人需要将自己视为好人;你需要破坏它,你不能通过排除它们来做到这一点。

由于所有这些原因,将恐怖组织建模为理性的经济行为者是不明智的,并且试图根据类似的假设来防止激进化也是不明智的。最好的方法是拥有一个不排斥人的环境 学生可以在住宅的楼梯上、小组教学小组和项目小组中认识来自不同背景的其他人 以及数百种运动和学生社团可供选择,所以每个人

可以找到一个帮派属于。这就是伟大的大学一直以来的运作方式
反正。

## 26.5 取证和证据规则

我们最后一个主要的警务主题是如何从计算机、手机和其他电子设备中恢复信息以用作证据。在过去的二十年中,这变得越来越成问题,首先是因为数据量巨大;其次,虽然大部分资金是从手机和笔记本电脑等平台上获取的,但越来越多的资金被保存在需要文书工作的云服务上,而且往往会有相当长的延误。不断上升的成本和运营困难导致执法部门更具选择性,各州很少干预所有类别的在线危害。结果,许多坏人,从网络犯罪分子到变态分子、恶霸和极端分子,都在网上活动而几乎完全不受惩罚。

### 26.5.1 取证

至少从 1980 年代开始,计算机取证就一直是警方面临的一个日益严重的问题;到 2000 年代初,设施和员工培训已经无可救药地落后了。在 2010 年代,所有东西都转移到了网上,这让事情变得更糟。如今,当警察突击搜查一个小型毒贩时,他们可以得到六部手机、几台笔记本电脑以及保存他位置历史记录的导航器或 Fitbit 等小工具。嫌疑人可能还拥有数十个网络邮件、社交网站和其他服务帐户。我们有各种巧妙的方法从数据中提取信息 例如,您可以从 CCD 阵列 [1192] 的模式噪声中识别出哪个相机拍摄了一张照片,甚至可以使用它来找出照片的哪些部分可能已被篡改。

然而,数字材料作为证据的使用取决于法律和经济学。材料必须合法收集,无论是有搜查令还是同等权力;法医必须保持监管链,这意味着能够让法庭确信证据在事后没有被篡改。这意味着使用值得信赖的工具来制作数据的证据副本;记录所做的一切;并有办法适当地处理发现的任何私人材料(例如特权律师-客户电子邮件,或嫌疑人雇主的商业秘密)。传统的计算机取证方法在标准教科书中有所描述,例如 Sammes 和 Jenkinson [1644]。

自从世界转向智能手机和云服务以来,重心已经转移到少数向警察和情报机构出售移动取证工具的公司。他们为警察部队提供信息亭,使不熟练的警察能够下载手机内容,并使用手机上的令牌从云中嫌疑人的帐户下载数据。一些警察部门正在努力解决法律问题(例如苏格兰警察,他们在没有搜查令的情况下不会使用“云取证”),但许多人只是获取并保留所有数据。

在交易的更复杂的一端,取证和反措施之间存在军备竞赛。警察部队过去总是关闭 PC ,以便为检方和辩护律师复制硬盘。网络钓鱼团伙通过让他们的网络钓鱼软件驻留在内存中来利用这一点,这样证据就会自毁。而且自从笔记本电脑开始配备适当的加密功能后,风险就会成倍增加。到 2013 年,当 FBI 逮捕丝绸之路地下毒品市场的创始人 Ross Ulbricht 时,一名特工的任务是把手伸进笔记本电脑以阻止 Ulbricht 关闭它,而他已经有了合适的电源线来插入它在[482]中。

在过去,卷入警方调查并没收计算机的个人和小企业可能要等上数年才能取回,即使他们只是旁观者,或者即使他们被指控但最终被无罪释放。如今,由于云服务,人们拥有防扣押的异地备份。由于嫌疑人的资料存放在海外服务器上,这些服务也让警方的日子更难过。我在第 26.2.8 节中提到的 Facebook 和 GCHQ 之间的斗争起源于 2013 年 3 月,两名恐怖分子在 Woolwich 军营附近谋杀了一名英国士兵 Lee Rigby,他们用汽车碾过他,然后刺伤了他。当他们在犯罪现场,面对警察时,Facebook 立即向警方和安全部门提供数据,但一旦两人被枪杀并被送往医院,请求必须通过英国/美国相互法律援助条约。这涉及向美国驻伦敦大使馆提交警方备案表格,然后在华盛顿司法部进行详细审议。这些表格经常被退回,因为英国警察局人员不了解美国法律并且填写不正确。即使一切顺利,FBI 也可能需要六周时间才能在加利福尼亚州门洛帕克的 Facebook 上提供文书工作并收集数据。所以我们发现我们已经从一个在突袭后警察会拥有你的数据而你不会的世界变成了一个你仍然拥有你的数据但警察没有的世界 - 除非你合作,或者除非你是一个足够严肃的坏人,值得外交官花时间和关注。

大约从 2017 年开始,出现了第三种选择:云取证。这实际上意味着你的手机被警方的取证亭黑了,并放弃了对你的电子邮件、你的照片、你的 Facebook 和你的其他云服务的访问令牌。一些英国警察认为这很好;他们将下载的数据视为“静态数据”,就好像它是在手机本身上找到的一样并永久保存。其他人则认为只能通过同意或进一步的授权才能获得。获取云数据的动机很强烈,但所涉及的机制(窃听电话然后冒充用户)可能会让大多数公民感到不公平。现在越来越多的设备正在获取附加的云服务和应用程序。警方是否会在未来通过扣押司机的手机并使用它从制造商的服务器下载汽车日志来调查交通违法行为?这是 2020 年的当前政策主题:例如,英国隐私监管机构要求制定法定行为准则 [958]。碰巧的是,法院已经对可以使用哪些证据制定了一些规则。

## 26.5.2 证据的可采性

当法院在 1960 年代首次面对计算机证据时,人们对其可靠性有很多担忧。不仅仅是数据是否准确的工程问题,还有计算机生成的数据是否不能作为传闻的法律问题。不同的立法机构以不同的方式处理这个问题。在美国,大部分法律都可以在《联邦证据规则》中找到,其中 803(6) 允许将计算机数据作为记录引入,“由知情人在当时或附近制作,或根据由知情人传输的信息制作,如果在定期开展的业务活动过程中保留……除非信息来源或准备方法或情况表明缺乏可信度。英国类似,英美法系国家(包括加拿大、澳大利亚、南非和新加坡)的电子证据规则由Stephen Mason[1236]分析。

“书面”和“签名”的定义很有趣,并且因司法管辖区而异。在英国,法院认为电子邮件就像写信一样:签名的本质是签名者的意图 [2042, 2043]。美国的做法同样务实。 2000 年,国会颁布了《全球和全国商业电子签名法》(“ESIGN”)法案,该法案赋予消费者同意某事的任何“声音、符号或过程”的法律效力。因此,按下电话键盘(“按 0 表示同意或按 9 终止此交易”),单击超链接进入网站,或单击软件安装程序上的“继续”,消费者同意接受合同[669]。这使得点击生效许可证在美国完全有效。尽管如此,Docusign 已经建立了一项提供数字签名的业务,为那些想要更炫耀的公司提供服务。

在欧洲,于 2000 年生效的电子签名指令对高级电子签名赋予了特殊的效力,这基本上是指使用智能卡或硬件安全模块生成的数字签名。

欧洲的智能卡行业认为这会为他们赚到很多钱,但多年来一直没有起色。在许多国家,纸质支票被伪造的风险由依赖方承担:如果有人在我的账户上伪造支票,那么这不是我的签名,我也没有授权银行从我的账户中扣款;因此,如果他们疏忽地依赖伪造的签名并这样做,那就是他们的了望。但是,如果我曾经接受过一种先进的电子签名设备,那么无论我是否真的做出了签名,我都会对任何看起来是由该设备做出的签名负责!

这一点,再加上智能卡没有可信的用户界面以及大多数人用作界面的 PC 很容易被破坏的事实,使得这种电子签名没有吸引力。在进一步游说之后,欧洲通过 eIDAS 法规 (910/2014) 更新了法律,该法规要求自 2018 年以来所有提供公共服务的组织都接受电子签名,从而提高采用的激励措施。许多欧盟国家现在坚持认为您使用这样的签名来报税,而不是允许它。根据所用技术的认证,签名可以是“高级”或“合格”的层次结构,并且必须接受合格的电子签名用于以前需要手写十签名的任何目的。数十款标志性创作产品获得正式认证并推向市场。使用的保证机制

以多种方式证明此类产品存在缺陷,我将在后面的第 28.2.7.2 节中讨论。欧盟委员会适当地提供了参考实施,以帮助政府开始验证所有签名； 2019 年,其中发现了漏洞,可以让任何公民冒充任何其他公民 [429]。

## 26.5.3 出了什么问题

警方调查可能会出现很多问题,计算机化的调查也不例外。一个古老的陷阱是依赖于从争议一方的系统中提取的证据,而没有对其可靠性提出足够的怀疑。回想一下 12.4.3 节中描述的 Munden 案例。一名男子在抱怨未经授权从他的银行账户提款后,被错误地指控并被错误地判处欺诈未遂罪。在上诉中,他的辩护团队得到法院的命令,要求银行向辩护专家开放其系统,就像对检方所做的那样。银行拒绝了,银行对帐单被裁定不予受理,案件告吹。从那以后,同样的事情发生了多次,包括我在第 14.4 节中讨论的两起涉及宵禁标签的恐怖案件。

我所知道的最严重的计算机证据失败是 Operation Ore。在美国邮政服务突击搜查德克萨斯州的一个色情网站后,他们发现了数十万个信用卡号码,他们认为这些号码被用来购买儿童性虐待图片,其中约有八千个来自英国持卡人。在 2000 年代初期,大约 3,000 所房屋遭到搜查,直到警方最终意识到大多数持卡人可能是信用卡欺诈的受害者。刑警队在对查获的材料进行初步分析时使用了不熟练的人员 ,而且学起来很慢因为他们专注于获得色情定罪,因为他们没有快速处理所有查获的计算机的法医能力,因为他们不了解信用卡欺诈（他们更愿意将其留给银行)并且出于政治原因（首相托尼·布莱尔亲自下令进行突击搜查）。因此,数千人的生活中断了数月甚至数年,邓肯·坎贝尔 (Duncan Campbell) 在 [375, 376] 中讲述了警察拙劣和掩盖真相的悲惨故事。对一些人来说,警方搞砸的揭露来得太迟了;三十多个人,面对起诉,自杀了。至少其中一位,驻直布罗陀英军司令大卫·怀特准将似乎是无辜的 [886]。

印尼和巴西组织并拍摄虐童事件的歹徒似乎并没有受到严肃追究。美国处理这个案子要好得多。在同一台服务器上发现了大约 300,000 个美国信用卡号码,但美国警方将这些数据用于情报而不是证据,识别关注的嫌疑人 例如与儿童打交道的人 并悄悄调查他们。一百多个实际虐待儿童的定罪随之而来。

有时系统被故意设计为不提供证据;一个例子是微软在 1990 年代与美国政府的反垄断斗争中出现令人尴尬的电子邮件后采取的政策。该公司的反应是,所有电子邮件在一段固定的时间后都会被丢弃,除非有人采取积极行动来保存它们,许多其他公司也效仿了

套装。另一个例子是服务公司在 2010 年代中期采用端到端加密的举措,因此他们无法访问客户消息记录,也不必雇用数百名律师来处理请求。

然而,计算机取证的最大问题一直是资金短缺。尽管情报机构可以使用所有很酷的技巧从计算机系统中提取信息,但除偶尔发生的大案件外,县缉毒队通常没有预算进行基本的计算机取证。他们甚至不能将每一包白色粉末 o 送到实验室,看看它是否非法。在正常情况下,他们只能使用容易获得的数字材料,例如合作证人手机上的消息副本,直到 2016-8 年左右出现手机取证亭并从没收的手机中获取大量数据边际成本低。因此,即使在制定健全的法律程序之前,使用信息亭的压力也很大。当然,未经专业培训的正规警察使用取证工具会增加未来误判的风险。司法教育也是一个问题;很少有法官了解概率论,事实上,英国上诉法院拒绝接受基于贝叶斯定理的证据分析。除了否认数学的法院系统的不公正之外,还有一个实际问题,即被告面临计算机证据,这些证据是错误的结果,或者只是被歪曲,可能没有实际的方法来证明他们的清白。

## 26.6 隐私和数据保护

隐私和数据保护是美国和欧洲采取不同路径的主题之一。集中利益（例如企业想使用我们的个人信息来剥削我们)通常会压倒分散利益（例如个人希望控制我们的个人信息），通常的补救措施是法律。补救措施并不完美,因为集中的利益游说立法者并将试图控制他们设立的任何监管机构。由于历史原因,欧洲比美国监管得更多。

2014 年 5 月,美国总统科学技术顾问委员会 (PCAST) 发表了“大数据:技术视角”[1546],由此产生的鸿沟得到了有力的强调。这份报告的作者包括谷歌的 Eric Schmidt 和微软的 Craig Mundie,描绘了一幅充满智能对象连接到云服务器的世界的图景,在这个生态系统中,传感器向云分析报告,云分析反过来向用户（例如广告商)提供信息. PCAST 警告说,语音和手势界面的普及意味着很快,地球上每个有人居住的空间都将配备麦克风和摄像头,它们的输出将被集中处理以提高能源效率。他们争辩说,不能对传感器施加隐私控制,因为它们太多了;它们不应强加于中央服务聚合器;因此,控制必须落在信息的使用方式上。

不到两周后,欧洲法院不同意。西班牙律师马里奥·科斯特哈·冈萨雷斯 (Mario Costeja Gonz`alez) 抱怨说,搜索他的名字会出现两篇关于拍卖他收回的房产的古老媒体报道

屋。他要求西班牙数据保护当局命令谷歌停止提供这些结果,因为它们已经过时且不再相关。谷歌辩称,它只是在报道一份报纸的内容。此案提交给了欧洲法院,欧洲法院认为冈萨雷斯胜诉,创造了一种被媒体充分渲染但不准确地称为“被遗忘权”的东西,后来从 2018 年起将其编入欧洲的《通用数据保护条例》。谷歌和其他在线服务供应商必须建立机制,让人们可以抱怨“不充分、不相关或不再相关,或与处理目的相比过度”的搜索结果,并将其删除。这些机制是有争议的:Gonz`alez 的结果在西班牙从谷歌搜索中删除,但欧洲监管机构希望它们在全球范围内删除。

谷歌的支持者声称,这会干扰其在美国的言论自由权。

这种裂痕是如何产生的?

## 26.6.1 欧洲数据保护

对技术破坏隐私的恐惧并不是最近才出现的。早在 1890 年,Warren 和 Brandeis 法官就警告过“最近的发明和商业方法”对隐私构成的威胁 特别是摄影和调查性新闻 [1988]。在 1960 年代初期银行、税务人员和福利机构开始使用计算机后,人们开始担心如果我们所有的交易都可以被整理和分析,那么隐私会受到影响。在欧洲,商界争辩说,只有政府才能提供足够多的计算机来构成严重的隐私威胁。这成为一个人权问题,因为盖世太保在大多数欧洲国家和东方的共产主义秘密警察部队都鲜为人知8。

从 1969 年的德国黑森州开始出现拼凑而成的数据保护法。由于技术变化的速度,成功的法律都是技术中立的。他们的共同主题是监管机构(无论是在国家还是州一级),个人数据的用户必须向其报告,并且谁可以指示他们停止和制止不当处理。实际效果通常是通过大量特定领域的实践准则来表达一般法则。

随着时间的推移,跨国企业的处理也成为一个问题,人们意识到纯粹的地方或国家举措可能对他们无效。根据经合组织 1980 年颁布的自愿行为准则 [1476],数据保护在 1981 年 1 月的欧洲委员会公约中得到巩固,该公约于 1985 年 10 月生效 [475]。

虽然严格来说这个公约是自愿的,但许多州因为担心失去进入数据处理市场的机会而签署了它。它要求对个人信息采取某些最低限度的保护措施,这通常意味着保存在可识别的人或数据主体上的任何数据,例如银行账户

8 在德国,隐私现在已写入宪法,甚至超过了“反恐战争”。最高法院裁定 2001 年警方为 30,000 多名来自穆斯林占多数的国家的男学生或前学生创建档案的行动违宪 尽管没有人因此被捕。它裁定只能在应对具体威胁时进行此类演习,而不是作为预防措施 [344]。

详细信息和信用卡购买模式。数据主体有权检查他们持有的个人数据,如果记录不准确则更改记录,了解他们是如何处理的,并且在许多情况下防止他们在未经他们同意的情况下将其传递给其他组织。几乎涵盖了所有商业数据。有国家安全方面的豁免,但并不像间谍们希望的那样完整:当发现来自处理银行间支付指令的 SWIFT 的数据在没有经过授权的情况下被复制到国土安全部时,引起了很大的争议。数据主体的知识; SWIFT 最终同意停止在美国处理欧洲数据 [1485, 1486]。

实施质量差异很大。例如,在英国,玛尔·加雷特·撒切尔 (Mar garet Thatcher) 毫不掩饰地尽可能少地遵从;建立了一个数据保护机构,但缺乏资金和技术专长,并且为政府和行业提供了许多豁免9。在将隐私权写入其战后宪法的德国,数据保护机构成为适当的执法机构。许多其他国家,如澳大利亚、加拿大、新西兰和瑞士,在 1980 年代和 1990 年代初通过了类似的隐私法:一些国家,如瑞士,采用德国模式,而其他国家,如冰岛和爱尔兰,则效仿英国模式。

到 1990 年代初期,各国法律之间的差异已造成贸易壁垒。一些企业通过将数据处理转移到美国来完全避免控制。因此,数据保护最终在 1995 年通过数据保护指令 [647] 提升到欧盟法律的地位。这设定了比以前更高的最低标准,对健康、宗教、种族和政治联盟等高度敏感数据的控制特别严格。它还着手防止个人信息在没有合同或条约强制执行的类似控制的情况下被运送到美国等“数据避风港”。

英国的实施也很少,远远达不到欧洲的要求 [597]。例如,数据控制者可以假装轻度匿名化的信息不再是个人信息,只要他们自己不拥有重新识别它所需的辅助数据即可。由于同时是公共部门的隐私顾问和隐私执行者,信息专员办公室不堪重负,并且存在严重冲突;执法部门不愿对咨询部门的同事赞扬的系统采取行动。爱尔兰的执法力度甚至更弱 过去 50 年的产业战略一直是吸引美国公司的欧洲总部。因此,除了低公司税外,都柏林政府将其数据保护办公室设在波塔灵顿这个人口不到 10,000 人的小镇,只给它 30 名员工,并且不允许它公布调查结果。

这让法国和德国等拥有更严格隐私法的国家非常恼火,以至于他们推动了通用数据保护条例 (GDPR),该条例于 2016 年通过并于 2018 年 5 月生效。这是欧洲游说最多的立法曾经,欧洲议会的委员会讨论了 3,000 多项修正案 [82];它得到了帮助

9在一个你期望有豁免的情况下,没有;在膝上型电脑或 PC 上记录人员身份的记者有正式责任按要求将此信息的副本提供给数据主体。

根据斯诺登的披露,尽管在那之前它已经酝酿了一段时间 10。 GDPR 直接影响所有欧盟成员国,消除了英国或爱尔兰引入漏洞的回旋余地;但是游说者已经在法规中得到了很多（特别是“研究”,无论是科学的还是市场营销的）。对正常企业的主要影响是迫使他们记录他们对个人信息的所有使用,并事先写下每一种使用的法律依据;一旦遇到挑战,仅仅尝试解决问题是不够的。对于信息密集型企业,其影响可能更为重大,并且已经有关于 Facebook 高管如何游说修改法规的有趣披露 有效地利用爱尔兰总理恩达肯尼作为他们在布鲁塞尔的倡导者 [1418] .

尽管游说者插入了许多例外条款,但 GDPR 仍在为监管机构提供反击的工具。法国对谷歌处以 50 米罚款,原因是谷歌未能充分告知用户其数据同意政策或给予他们足够的控制权来控制其信息的使用方式 [1534]。不能再强迫或推定同意这一事实可能会成为一个大问题,并且还有许多其他案例正在处理中。

## 26.6.2 美国的隐私法规

在美国,企业大多设法说服政府将隐私主要留给“自我监管”。尽管州和联邦法律错综复杂,但它们都是针对具体应用的,而且是零散的。一般来说,联邦政府记录和通信中的隐私受到监管,而商业数据在很大程度上不受控制。为数不多的监管孤岛包括 1970 年的《公平信用报告法》,该法案管理信用信息的披露,与欧洲规则大体相似;视频隐私保护法或“博克法案”,在华盛顿一家报纸公布法官罗伯特博克被提名为美国最高法院法官后的视频租赁历史后颁布;在女演员丽贝卡·谢尔 (Rebecca Schae er) 被一名聘请私家侦探寻找她地址的痴迷粉丝谋杀后,《驾驶员隐私保护法》(Drivers Privacy Protection Act) 的颁布是为了保护 DMV 记录的隐私;以及我在第 9 章中讨论过的保护医疗记录的《健康保险流通与责任法案》。大多数州还有泄露披露法,该法要求公司在遇到任何危及居民个人信息的安全故障时通知他们。在数量惊人的情况下,一些侵权行为也为民事诉讼提供了依据;有关调查,请参见 Daniel Solove [1801]。

第一个开始让 CEO 关注隐私的案例发生在 2006 年,当时 Choicepoint 支付了 1000 万美元来解决联邦贸易委员会提起的诉讼,因为它未能正确审查订户并让骗子购买超过 160,000 名美国人的个人信息,导致至少 800 起“身份盗用”案例 [671]。 2007 年,连锁店 TJ Maxx 有 4570 万客户的信用卡信息被盗 [1159]； 2010 年,阿尔伯特·冈萨雷斯 (Albert Gonzales) 因此事被判入狱 20 年,据估计,此次违规使公司损失了 8 亿美元。 FTC 起诉 Facebook 对隐私设置进行欺骗性更改,并于 2011 年就在 IPO 之前达成和解,要求它获得用户同意才能进行某些更改和

10斯诺登揭露了一些令人发指的滥用职权,例如 GCHQ 大规模收集 Operation Optic Nerve 中的雅虎视频聊天,包括亲密视频聊天 [14]。

对其进行 20 年的审计 [181]。 2014 年 5 月,Target 的首席执行官 Gregg Steinhafel 在 2014 年 5 月被解雇,原因是去年 12 月有超过 1 亿个信用卡号码被黑客入侵； CIO 也被更换了 [702]。美国 11和其他地方 12 的最高管理层大屠杀仍在继续,将网络安全稳步提升到公司议程的首位。

2018 年,加州通过了消费者隐私法,即加州消费者隐私法 (CCPA)。这是在一项隐私投票倡议之后进行的,如果它进行了投票并获得通过,将会确立更严格的隐私法。此次投票是在 Cambridge Analytica 丑闻之后进行的,在 2016 年竞选期间,8700 万用户的 Facebook 数据在他们不知情或不同意的情况下被收集,并用于针对行为广告。大型科技公司的辩护是谈判新法律而不是投票倡议,这样他们就可以在以后对其进行修改,甚至被联邦法律推翻。 CCPA 有点类似于欧洲数据保护法:它授权消费者请求删除个人信息、选择退出其销售以及以能够将其传输给第三方的格式访问它。

由于美国第一修正案,欧洲被遗忘的权利是不可能的。 CCPA 可以由州检察长执行,也可以通过私人行动执行。现在一个真正重要的政策问题是这项法律是否逐渐被其他州复制,或者大型科技公司是否设法阉割它 13。但美国并不是这里唯一认真的参与者。

## 26.6.3 碎片?

自 1998 年以来,欧洲法律禁止公司将个人数据发送到法律未提供类似保护或其他保障措施的国家/地区的组织 - 实际上,这指的是美国和印度。解决这个问题的第一个尝试是安全港协议,根据该协议,美国或印度的数据处理商将向其欧洲客户承诺遵守欧洲法律。 2000 年,欧盟委员会通过了一项行政决定,大意是这将提供“充分的保护”。然而,对于认为自己的权利受到侵犯的欧盟公民来说,它没有任何实际的追索权。

杀死安全港的案件是由奥地利律师马克斯·施雷姆斯 (Max Schrems) 针对 Facebook 提起的。在斯诺登事件曝光后,他辩称,爱尔兰（其欧盟总部)的 Facebook 将他的数据传递给美国进行处理是非法的,因为美国的法律和惯例没有提供免受公共当局监视的保护,特别是 NSA,它可以通过 Prism 收集所有信息。欧洲法院同意并在 2015 年推翻了安全港原则。美国和欧盟随后同意用一种名为“隐私盾”的新安排取而代之。

11索尼的 Amy Pascal,2014 年,FACC 的 Walter Stephan,2016 年,Equifax 的 Richard Smith,2017 年;也许我们可以注意到雅虎的 Marissa Meyer,她在 2017 年没收了她的奖金和股票,甚至可能还有 Uber 的 Travis Kavalnick,他的继任者公布了一个被掩盖的黑客事件。

12英国 TalkTalk 的 Dido Harding,2017 年;新加坡综合健康信息系统的 Bruce Liang,2019 年;也许我们也可以算上大众汽车公司的马丁·温特科恩和奥迪汽车公司的鲁珀特·施泰德,他们主持了该公司破解其汽车尾气排放的工作。

13他们的游说者已经在攻击它,但正如我在 2020 年写的那样,有一项投票倡议
这将使它在加利福尼亚州的法律中根深蒂固,并使其超出州立法者的控制范围。

如果欧盟公民认为美国国家安全局可能监视他们,他们可以向其投诉并增加监察员 [1474]； Max 也将此提交给欧洲法院,该法院于 2020 年 7 月正式将其推翻 [1683]。被告是爱尔兰数据保护专员,她花了将近 3 分钟的时间来捍卫自己的立场,即在欧盟总部设在爱尔兰的美国科技公司粗暴对待隐私法时,她有权视而不见。法院还裁定,隐私机构有义务在收到投诉后采取行动。它还明确表示,根据美国法律,美国国家安全局有权免费访问非美国人的数据,这与美国公司将欧盟公民的数据保存在美国的监管和控制之下是不一致的14。

许多在美国处理数据的公司在此期间退缩了,迫使客户在与他们做生意之前同意共享他们的个人数据。这有着悠久而肮脏的历史（这是医疗保险公司将您的数据出售给制药公司的方式）,欧洲法院允许继续使用标准合同条款 (SCC) 来保护数据。但这并不简单。首先,数据控制者必须确定数据所在的国家/地区具有足够的保护水平,其次,您不能简单地将此类条款强加给 GDPR 世界中的消费者,因为明确禁止强制同意.当美国法律允许不受限制地访问外国人在美国领土上的数据并且斯诺登披露记录了这种访问的系统使用（以及从欧盟法律的角度来看,滥用)时,很难看出美国公司如何能够建立充分性。

因此,这正在发展成为一场真正的战斗,对世界服务器场的定位和控制方式和地点产生真正的影响。一些消息灵通的公司认为他们最终将不得不在欧洲并根据欧洲法律处理欧洲数据;微软将德国的一个数据中心置于德国受托人的控制之下几年,但后来改变了主意,而谷歌则在慕尼黑进行了数年的隐私研究和开发。美国的公众舆论与欧洲并无太大不同:大多数美国人认为他们的个人数据现在不那么安全,监视资本主义的风险大于收益,他们不了解正在发生的事情,他们有没有控制权,公司和政府都不对滥用行为负责,但他们别无选择。哦,还有 20% 的人在过去 12 个月内遭受过某种在线欺诈 [144]。

与此同时,数据保护法正在进入新的领域,它提供了一种应对滥用行为的方法。例如,在英国脱欧公投后,英国信息专员对 Facebook 处以 500,00015 英镑的罚款,原因是 Facebook让剑桥分析公司收集了全球 8700 万人的个人数据,并将其用于针对英国脱欧公投和美国 2016 年总统大选的竞选广告[957]。由于市场营销和政治宣传中的许多现代实践都涉及数据保护法下的违法行为,这为监管提供了空间

14 欧洲人权法院还有一个悬而未决的案件,由 Big Brother Watch 针对美国的大规模监视 [420] 提起,该案件已获准向大法庭上诉。如果以同样的方式进行,欧洲法院的判决将扩大到那些属于欧洲委员会但不属于欧盟的国家,例如英国和俄罗斯。

15英国的罚款是 GDPR 之前的数据保护法允许的最高金额;从那时起,最高限额为被告营业额的 4%,这应该会使欧洲的处罚与美国的处罚保持一致。

创新。在美国,联邦贸易委员会使用广告真实法来惩罚违反隐私政策或之前关于用户隐私的协议的公司;
Facebook 在适当的时候被联邦贸易委员会罚款 50 亿美元。自剑桥分析丑闻爆发以来,电子隐私信息中心
16一直在争论 Facebook 违反了 2011 年与 FTC 达成的和解条款。

## 26.7 信息自由

信息往往从弱者流向强者,增强了他们的权力并使其他人更难追究他们的责任。正如詹姆斯麦迪逊所写:

> 一个没有大众信息或获取信息的手段的大众政府只是闹剧或悲剧的序幕,或者两者兼而有之。
>
> 知识将永远统治无知:一个想要成为自己统治者的民族,必须用知识赋予的力量武装自己。

水门事件后,国会通过了《信息自由法》,其他国家也纷纷效仿;英国在 199717 年获得了一个。已经尝试了更激进的版本:在冰岛和瑞士的一些州公布纳税申报表,这种做法减少了逃税,因为富人担心低申报收入会带来社会地位的丧失。最激进的版本是由 David Brin 在“透明社会”[322] 中提出的。他推断,数据采集、传输和存储成本的下降将使当局可以使用无处不在的监控技术,因此唯一真正的问题是我们其他人是否也可以使用这些技术。他描绘了两种未来之间的选择 一种是公民生活在对中国式警察制度的恐惧中,另一种是公务员通过公众监督承担责任。他认为基本上所有信息都应该公开 包括,例如,我们所有的银行账户。摄像头将会存在:它们是监控摄像头还是网络摄像头?

社交媒体似乎经常将我们推向那个方向。无论如何,《信息自由法》通常允许公民索取国家持有的信息的副本,除非有充分的理由拒绝提供,并有助于确保公民与国家之间的信息流动不完全是单向的.

然而,透明度会导致有趣的争论。许多欧洲国家都有清白的法律,根据罪行的严重程度,大多数刑事定罪会在一段时间后被撤销,2019 年,宾夕法尼亚州、犹他州和加利福尼亚州紧随其后 [607]。但是既然网络搜索引擎已经存在,那么这些法律如何执行呢?你是否在报纸上的审判报道中标记了罪犯的名字并注明了有效期,并通过法律强制搜索和档案服务尊重他们?谷歌西班牙案给了我们答案:定罪期满的人有权在搜索中禁止使用它,尽管它可能会保留在报纸档案中,供那些知道去哪里找的人使用。

16 完全披露:我是他们顾问委员会的成员。
17托尼·布莱尔后来形容这是他最大的错误。

这是数据保护和信息自由之间边界不断变化的一个例子。另一个是对前儿童性别的监控,一些州的法律要求公开罪犯登记册,英国发生骚乱,因为周日报纸和至少一名前罪犯点名无辜者被私刑处死。第三个是犯罪统计数据的发布:房主反对他们的社区被污名化,如果数据过于细化,可能会存在个体受害者被识别的风险。有关更多示例,请参阅有关推理安全的第 11.1 节。

## 26.8 小结

公共政策越来越多地与安全工程师的工作纠缠在一起。
如果我们用美元来衡量,政府最关心的一个问题就是情报;与打击网络犯罪相比,一个典型的政府在收集有关其真实和潜在敌人的信息方面花费的资金要多一百倍。情报收集还与防御性安全和隐私相冲突,这两者在历史上都排在第二位。然而,自从斯诺登的爆料清楚地表明了美国在全球范围内收集数据的规模,以及针对盟国的“五眼联盟”行动,平衡开始发生变化,其影响已经通过隐私和数据保护法传播,尽管速度缓慢且有一定影响到目前为止,对机构本身影响不大。也许当分析完成后,斯诺登对机构能力的影响将主要是技术性的（通过让人们更多、更智能地使用密码学）,而政策影响可能是遏制一些过度的“监视”资本主义”通过让隐私对更多人更加重要。美国和欧洲处理隐私的方式之间的压力越来越大,从中期来看,我们可能会看到更多的本地化 美国公司必须将欧盟公民的数据保存在欧洲的服务器上,甚至可能在欧洲受托人的控制下.其他国家也开始效仿。

审查制度是一个真正的问题;一些国家,如中国,直接禁止许多美国大型服务公司,同时越来越多的国家要求他们不仅要删除辱骂性材料,还要删除冒犯当地政治敏感性的材料。互联网仍然让那些不像中国那么远的国家更难审查颠覆性内容,但我们十年前的乐观情绪已经随着阿拉伯之春的失败而消散。即使是发达国家也推动大型服务公司大规模审核和过滤用户生成的内容,尽管成本高且复杂,但端到端加密服务除外,它正在变得普遍。美国在线禁止用户住在斯肯索普已经 25 年了,无论我们谈论的是版权、激进化、骚扰还是假新闻,大规模过滤仍然会引发一系列政策问题。

在 9/11 袭击后激起的恐惧气氛推动了安全工业综合体的增长,随着世界威权主义者购买监视系统以跟踪其人口,中国和阿拉伯之春又吹来了一股风。这导致了计算机的普及和

侵蚀我们的安全、自由和生活质量的网络开发工具。这种扩散得到了西方政府的帮助和教唆,他们应该更了解这一点,并且随着社交媒体公司和其他公司被纳入越来越多的内容筛选作为开展业务的条件,这种扩散势必会扩大。了解和反击监控生态系统,同时减轻在线危害是安全工程师的首要任务,他们有能力参与公共生活无论是直接参与,还是通过我们的写作和教学。研究也有帮助。个别学者不能指望在大众媒体上与国家领导人竞争,但多年来对数据和知识的精心积累能够而且将会削弱他们的借口。我的意思不仅仅是了解为什么极端的机场安检措施是浪费金钱;我们还必须传播关于政府行为不当背后的经济学和心理学知识,及其在本应用于大流行病防备的安全战区上花费的可怕后果。

## 研究问题

技术政策涉及科学、工程、心理学、法律和经济学之间复杂的相互作用。严肃的跨学科研究仍然太少,加速这一过程的举措几乎肯定是一件好事。自 2002 年以来,我一直致力于建立安全经济学研究社区;自 2008 年以来,我们每年举办一次关于安全和人类行为的研讨会,邀请心理学家、人类学家和哲学家参与。

但我们需要更多,更多。历史学家、社会学家和政治学家在哪里? （也许如果有第四版,我们会添加哲学家。）

## 进一步阅读

技术政策论点非常容易脱离现实,许多为了吸引注意力和金钱而产生的恐慌（例如“网络恐怖主义”）是现代等同于出现在中世纪地图上以掩盖制图师无知的怪物.工程师应该寻找主要来源 从 RV Jones [992] 等经验丰富的内部人士撰写的材料到 Ed Snowden 泄露的数千份文件。至于信息战技术在英国脱欧公投和2016年美国大选中的运用,Carole Cadwalladr的电影《The Great Hack》不容错过。

Whit Die 和 Susan Landau 有一本关于窃听和加密政策历史的好书,他们长期参与了政策制定过程[558],NRC 对加密政策的研究也很有影响力 [1411]。

我的网站上有一段视频,从欧洲的角度讲述了加密货币战争的历史。

出口管制的历史与苏联在 1970 年代和 80 年代试图购买美国的计算机、半导体和能源技术以及美国和法国情报界阻止并提供它们的工作有关

误导性信息:参见 Gus Weiss 的回忆录,他是参与这项工作的 CIA 特立独行者 [723]。

关于在线审查的资源包括 Reporters without Borders,他们出版了一本关于如何规避审查的“博主和网络持不同政见者手册”,其中有许多关于博客如何帮助不那么自由的国家开放媒体的案例历史 [1594 ].

计算机取证的标准工作是 Tony Sammes 和 Brian Jenkinson [1644],而 Privacy International 有一项关于手机取证的调查 [1555],司法部的“Guidelines for Searching and Seizing Computers”也受到一些关注 [550] .有关早期计算机犯罪案例的历史,请参阅 Peter Neumann [1429] 和 Dorothy Denning [539]。英美法系国家关于计算机证据的标准著作是斯蒂芬·梅森 [1236]。

关于隐私与数据保护的话题,有大量文献,但据我所知没有简明的最新指南。最近的材料可以在 EPIC [631]、EFF [618]、FIPR [708] 和 EDRi [643] 以及 Max Schrems [1683] 等组织的网站上找到。

至于围绕过滤煽动性内容和宣传的政策问题,对我来说最发人深省的两本书是 Tim Wu [2050] 和 Yochai Benkler [227] 的书,而 Facebook 的前 CISO Alex Stamos 现在讨论科技公司的过滤政治广告的观点 [999]。

最后,举报人 Chris Wylie [2052] 在书中以及 Carole Cadwalladr 基于他和其他人提供的信息 [363] 的新闻报道中讲述了 Cambridge Analytica 丑闻的最终故事。