2.3 第四修正案和变更技术

2.3.1 第四修正案

人民的人身、房屋、文件和财产不受无理搜查和扣押的权利不得侵犯，除非有正当理由，并有宣誓或誓言支持，并特别说明 被搜查的地方、被扣押的人或物。
——美国宪法第四修正案

执法机构拦截通信并搜查家庭和企业以收集犯罪活动的证据。 情报机构也这样做，以收集有关敌对政府和恐怖分子的活动和计划的信息。 美国宪法第四修正案和各种法律限制了他们保护无辜者和减少虐待机会的活动。 英国也有类似的传统，正如威廉·皮特在 1763 年的精彩声明中所表达的那样：

最穷的人可能会在他的小屋里挑战王室的所有力量。 它可能很脆弱； 它的屋顶可能会摇晃； 风可能会吹过它； 风暴可能进入； 雨可以进入——但英国国王不能进入。

在本节中，我们将考虑不断变化的技术（通信、监控技术、移动设备和海量数据库）、政府政策和法院判决如何影响执法机构获取信息的能力。 我们考虑政府入侵对隐私的新威胁，以及第四修正案是否以及如何保护免受这些威胁。

第四修正案限制了政府搜查我们的住宅和企业以及没收文件和其他个人物品的权利。 它要求政府有充分的证据来支持特定的搜查，并且需要法官批准搜查令。 但随着新技术的出现，我们的大部分个人信息在家中或医生和财务顾问的个人办公室不再安全。 它在我们无法控制的巨大数据库中，通常被复制到云端。 新技术允许政府在不进入我们家的情况下搜查我们的家，在我们不知情的情况下远距离搜查我们的人，并在交通站点不到两分钟的时间内在智能手机上提取数据。 对于每一项新技术，执法机构都会在没有搜查令的情况下进行搜查、扣押和拦截，认为第四修正案不适用。 在许多但不是所有的案例中，最高法院最终表示第四修正案确实适用，尽管在最高法院对特定技术做出裁决之前要经过数年，有时甚至数十年。

当我们考虑政府机构现在可以获得的所有个人信息时，我们可以反思最高法院法官威廉·道格拉斯 (William O. Douglas) 对政府仅访问某人支票账户记录的潜在滥用行为的担忧。 1974 年，他说：

从某种意义上说，一个人是由他开出的支票来定义的。 通过检查他们，代理人可以了解他的医生、律师、债权人、政治盟友、社会关系、宗教信仰、教育兴趣、他阅读的报纸和杂志，等等。 这些都与一个人的社会安全号码相关联，现在我们有了数据库，这些其他项目将丰富这个仓库，并使官僚们可以通过按一个按钮立即获得 1.9 亿具有颠覆性或有此动机的美国人的名字。

今天的读者不要错过最后一句话的讽刺：1.9 亿几乎是当时美国的全部人口。

美利坚合众国成立时，制定者在隐私、披露和监视的竞争价值之间建立了自由意志主义的平衡。 这种平衡是基于 18 世纪生活的技术现实。 由于酷刑和审问是唯一已知的渗透思想的手段，因此政府采取的所有此类措施都是法律所禁止的。 物理进入和窃听是渗透私人住宅和会议室的唯一手段； 因此，制宪者将私人窃听定为犯罪，并允许政府进入私人场所，但仅限于在严格的搜查令控制下进行合理搜查。 由于登记程序和警察档案是用来控制“有争议”人员自由流动的手段，因此欧洲警察的这种做法被美国政府的做法和流动边境生活的现实所排除。

—Alan F. Westin，《隐私与自由》

2.3.2 背景、法律和法院判决

本意见中规定的原则……适用于政府及其雇员对个人家庭的神圣性和生活隐私的所有侵犯。 构成犯罪本质的并不是破门而入、翻箱倒柜； 但这是对他不可剥夺的人身安全、人身自由和私有财产权利的侵犯。

——最高法院大法官约瑟夫·布拉德利，博伊德诉美国案，1886 年

电话交谈和窃听

在电话发明后的 10 年内，人们（政府内外）开始窃听电话。 在整个 20 世纪的大部分时间里，窃听的法律地位都在争论不休。 在接线员接听电话并且大多数人都有合用线路（几户人家共用一条电话线）的那些年里，接线员和爱管闲事的邻居有时会偷听电话交谈。 随着时间的推移，财富的增加和新技术的出现消除了党派线路和人工接线员，但电话仍然容易受到窃听。

联邦和州执法机构、企业、私家侦探、政治候选人广泛地使用了窃听技术。在 Olmstead v. United States (1928) 案中，最高法院裁定执法机构的窃听行为并不违宪，尽管国会可以禁止这种行为。 在 Olmstead，政府在没有法院命令的情况下在电话线上使用了窃听器。 最高法院将第四修正案解释为仅适用于人身入侵，并且仅适用于搜查或没收物质物品，而不适用于谈话。 Louis Brandeis 大法官持不同意见，认为第四修正案的起草者已尽其所能保护自由和隐私——包括谈话的隐私——免受政府基于当时可用技术的侵犯。 他认为法院应该将第四修正案解释为需要法院命令，即使新技术允许政府在不进入我们家的情况下访问我们的个人文件和谈话。

在 1934 年的《通信法》中，国会规定，除非得到发件人的授权，否则任何人都不能合法地拦截和泄露消息； 执法机构也不例外。 1937 年，最高法院裁定窃听违反了这项法律。 此后，数十年来，联邦和州执法机构以及地方警察在有和没有搜查令的情况下继续窃听。 FBI 对国会和最高法院的成员进行了窃听和窃听，在一个广为人知的案例中，FBI 在审判期间监听了被告与其律师之间的电话通话。 在许多情况下，执法机构会窃听涉嫌犯罪的人，但有时，他们也会窃听持有非传统观点的人、民权组织成员以及有权有势的政府官员的政治对手。 尽管有关于警方广泛使用窃听的宣传，但没有因此受到起诉。

在卡茨诉美国案中，最高法院于 1967 年推翻了奥姆斯特德案，裁定第四修正案确实适用于对话*，并且在某些情况下适用于公共场所。在这种情况下，执法人员在电话亭外面安装了一个电子监听和录音设备，以记录嫌疑人的谈话。法院表示，第四修正案“保护的是人，而不是地方”，并且一个人“寻求保护为私人的东西，即使是在公众可以进入的区域，也可能受到宪法保护。” 要闯入一个合理的人有合理的隐私期望的地方，政府人员需要法院命令。 即使在卡茨之后，政府和政客的非法或合法性值得怀疑的窃听仍在继续，尤其是在越南战争期间，记者、犯罪嫌疑人和其他人继续成为非法窃听的受害者。

** 政府代理人可能会确定从特定电话拨打的电话号码以及某人拨打电话的号码，而不是拦截电话内容所需的法庭审查和理由。**

电子邮件和手机对话

当电子邮件和手机还很新时，政府机构和其他人的拦截是很常见的。 据报道，在硅谷开车窃听手机通话是 20 世纪 80 年代流行的工业间谍活动。 Snoops 截获了政客和名人的手机对话。 1986 年电子通信隐私法 (ECPA) 将 1967 年 Katz 诉美国案中的窃听限制扩展到电子通信，包括电子邮件、无绳电话和移动电话。 ECPA 禁止在传输过程中拦截电子通信和数据的内容，除非政府机构持有搜查令。 ECPA 为执法机构制定了较弱的标准，以获取存储电子邮件的副本并收集有关通信的信息，例如呼叫号码、呼叫或电子邮件的时间和日期以及其他标头信息。 政府争辩说，人们通过允许 ISP 将他们的电子邮件存储在 ISP 的计算机上而放弃了他们对隐私的期望； 因此，第四修正案的严格要求将不适用。 在 ECPA 通过二十年后，联邦上诉法院裁定，人们确实期望存储在其 ISP 中的电子邮件具有隐私权，并且警方需要搜查令才能获得它。 隐私期望的概念仍然是许多法院判决的核心； 因此，我们进一步探索它。

对隐私的期望

尽管最高法院在 Katz v. United States 案中的判决在某些方面加强了第四修正案的保护，但它依赖合理的“隐私预期”概念来定义执法人员需要法院命令的领域，这产生了一些令人惊讶和负面的结果 为了隐私。 随着消息灵通的人们开始了解现代监控工具的功能，我们可能不再期望政府在实际意义上提供隐私。 这是否意味着我们不应该拥有它？

最高法院在史密斯诉马里兰案中承认了这个问题，其中指出，如果执法部门通过“与公认的第四修正案自由无关”的行为降低了对隐私的实际期望，这不应减少我们对第四修正案的保护。 然而，法院对“隐私期望”的解释非常严格。 它裁定，如果我们与我们的银行等企业共享信息，那么我们对这些信息的隐私没有合理的期望（美国诉米勒，1976 年），执法人员不需要法院命令来获得它。 这种解释似乎很奇怪。 我们确实希望我们提供给银行或其他金融机构的财务信息的隐私。 我们希望我们与少数人（有时是精心挑选的人）共享的多种信息的机密性，但许多法律和法院判决允许执法机构在没有法院命令的情况下从非政府数据库中获取信息。联邦隐私规则允许执法机构在没有法院命令的情况下访问医疗记录。 美国爱国者法案（在 2001 年恐怖袭击后通过）使政府可以在没有法院命令的情况下轻松访问多种个人信息，包括图书馆和财务记录。

酒店记录，或任何消费者-商业交易

洛杉矶的一项法律要求酒店收集和存储所有客人的信息，并允许任何洛杉矶警察在没有搜查令的情况下按需检查记录。 政府辩称，人们无权要求保护隐私，因为他们已经与酒店“共享”了信息。 该论点可用于消除与他人交易有关的几乎所有隐私。 联邦上诉法院裁定，洛杉矶法律允许警察在没有搜查令的情况下检查酒店记录的规定违反了第四修正案，因为客人记录是酒店的财产，而酒店有兴趣将其保密。 尽管这种方法不承认客户的隐私利益，但它至少为企业存储的有关人员的记录提供了一些保护。 执法机构是否会争辩说，如果企业与管理交易某些方面的另一家企业（例如，酒店预订网站）“共享”信息，他们将失去隐私权？

我们仅通过打字、点击和说话与 ISP、网站、电信公司和搜索引擎公司分享我们的在线活动。 当我们通过拼车应用程序找到一辆车时，我们会分享我们的位置信息——或者只是携带手机。 我们在网上购买的所有东西，以及我们通过会员服务观看的每个视频，都会成为公司业务记录的一部分。 我们在云端备份我们的照片和数据。 警察可以从我们家中受第四修正案保护的云存储公司得到什么？ 美国诉米勒案的判决早于互联网，但法院继续适用第四修正案不保护我们共享的信息的裁决。 隐私期望应如何适用于这些技术和服务？ 最高法院是否应该完善和更新其立场？

2.3.3 在新领域应用第四修正案

我们使用这些新技术并不表示我们对隐私不感兴趣。 政府监视我们的行踪、习惯、熟人和兴趣的想法仍然让我们毛骨悚然。 我们常常只是不知道它正在发生，直到为时已晚。

———Judge Alex Kozinski

搜索和跟踪移动设备

警察可以在没有搜查令的情况下合法地搜查被捕者，并检查该人身上（例如口袋里）或他或她够得着的个人财产。这样做的原因是为了找到并拿走武器，并防止该人隐藏或销毁证据。 但是，在警察搜查此人手机的内容之前是否需要搜查令？

手机通常包含联系人、最近通话信息、消息内容、文档、个人日历、照片、Web 浏览历史记录以及手机所在位置的记录。 它还可能包含书籍、健康信息和宗教应用程序。 对于许多人来说，电话是一个旅行办公室，包含专有和机密信息。 例如，律师的电话可能包含有关客户和案件的信息——受法律保护不能被警方访问。 智能手机上收集的大量信息正是第四修正案旨在保护的信息类型。 另一方面，一位反对搜查令要求的联邦政府律师表示，在获得搜查令所需的时间内，犯罪分子的同伙可以远程删除警方拘留的手机中的定罪证据。 在到达州最高法院的案件中，不同

州的法院对是否需要搜查令的问题作出不同的裁决。 2014 年，即 iPhone 推出七年后，最高法院在莱利诉加利福尼亚州案中一致裁定，警察不得在没有搜查令的情况下搜查一个人的手机内容。

执法人员每年追踪数千人的位置。 有时他们有法院命令这样做，有时他们没有。 他们需要一个吗？ 我们考虑两种技术：一种在公众视野中跟踪私人行为； 另一个在私人场所跟踪人们。

在没有搜查令的情况下，警方秘密地将 GPS 跟踪设备安装在嫌疑人妻子拥有的车辆上。 警察说不需要搜查令，因为他们可以看到这辆车在公共街道上行驶； 他们将 GPS 跟踪器描述为一种省力设备。 最高法院于 2012 年对美国诉琼斯案作出裁决，裁定支持第四修正案的保护。法院一致同意，车辆是第四修正案明确保护的个人“财产”之一。因此，警方需要搜查令才能在私家车上安装监控设备。 第二个论点是，在一个月内每天 24 小时跟踪一个人的位置，就像在这种情况下一样，不仅仅是在公共场合观察汽车经过； 它违反了一个人对隐私的期望。 法官们认识到，在跟踪不需要直接连接设备的案件时，隐私预期将是一个关键问题，但大多数法官选择留待未来再做决定。

假设一个人在家里，在朋友或爱人的家里，在教堂或医疗机构内，或在任何私人空间。 州、地方和联邦执法机构使用设备（通常称为黄貂鱼）通过定位人员的手机来定位人员，即使手机未在使用中也是如此。 黄貂鱼模拟了一个手机信号塔，特工们在他们认为这个人所在的区域驾驶或飞行。 当代理移动时，目标手机会在多个位置连接到 stingray。 然后，他们使用黄貂鱼数据对手机的确切位置进行三角测量。 有了这项技术，警察不需要进入私人场所或将任何东西实际附加到一个人的财产上。 联邦官员努力对黄貂鱼的使用及其工作原理保密。 美国公民自由联盟获得的文件显示，早在 2009 年，联邦官员就鼓励警方隐瞒他们正在使用这些设备的事实； 相反，他们会说跟踪信息来自机密来源。 当新闻报道开始出现时，执法机构争辩说，手机跟踪不需要搜查令，因为使用手机服务的人对手机传输到手机信号塔的位置数据没有隐私期望。 更有可能的是，大多数人没有意识到他们的手机会定期向附近的手机信号塔发送信号，或者没有考虑这样做的影响，也没有意识到他们可以被便携式手机信号塔模拟器跟踪，只是因为他们携带了电话。

在对黄貂鱼进行宣传和批评之后，美国司法部宣布了追踪手机的新政策。 最重要的变化是联邦特工必须获得法官的授权才能使用黄貂鱼类设备。 联邦政策不适用于地方和州警察，但一些州也采用了搜查令的要求。 在撰写本文时，最高法院尚未审理过有关该技术的案件，尽管多个州和联邦法院已裁定未经授权使用黄貂鱼和类似设备违反了第四修正案。

尽管趋势似乎是要求搜查令实时跟踪一个人的电话，但一些联邦上诉法院在涉及访问电话服务提供商存储的位置历史数据的案件中做出了不同的裁决。 电话公司有电话连接到的基站的记录，包括日期和时间。 因此，这些信息给出了一个人的移动的地图和时间线，尽管位置不精确，因为这个人在塔附近，而不是直接在塔上。 到目前为止，法院已裁定此信息与警方可以在没有搜查令的情况下访问的其他业务记录属于同一类别，因为我们已与公司共享信息，因此不期望隐私。

没有搜查令，政府不得将公民的手机变成追踪设备。

———U.S. District Judge William Pauley, 2016

“无创但深刻揭示”搜索

上面的标题来自 Julian Sanchez 对各种搜索和检测技术的描述。 许多听起来像科幻小说； 他们不是。 这些技术可以搜查我们的房屋和车辆，但不需要警察亲自进入或打开它们。 他们可以在我们不知情的情况下从远处搜查我们衣服下面的身体。 非侵入性但深度揭示的搜索工具（一些正在使用和一些正在开发中）包括检测许多特定药物和爆炸物的粒子嗅探器，无需打开卡车即可分析卡车货物分子成分的设备，热成像设备(用于查找热灯 例如，种植大麻)，

无人机在我们的后院或窗外盘旋，以及仅使用记录室内声波引起的植物叶子或薯片袋微小运动的视频图像来重建对话并通过声音识别说话者的算法 人们说话的地方。 这些工具显然具有有价值的安全和执法应用，但这些技术可用于在没有搜查令或可能原因的情况下对毫无戒心的人进行随机搜索。 正如桑切斯所指出的，我们生活在“一个法规繁多的国家，几乎每个人都在某个时候犯下了某种违规行为。” 在政府开始使用这些工具之前，例如，普通人从加拿大带药回家，自己酿造啤酒，或在家中存放违禁甜味剂或饱和脂肪（或将来可能违法的任何东西）之前，至关重要的是 隐私保护和自由，我们对它们的使用有明确的指导方针，特别是澄清这种使用何时构成需要搜查令的搜查。

在 2001 年的 Kyllo 诉美国案中，最高法院裁定警察在没有搜查令的情况下不得使用热成像设备从外面搜查房屋。法院指出，如果“政府使用不供公众使用的设备来探索以前在没有物理入侵的情况下不可知的家庭细节，则监视是一种‘搜索’。”这一推理表明，当技术 变得越来越广泛，政府可能会在没有搜查令的情况下将其用于监视。 该标准可能为市场、公众意识和技术的发展留出时间，以提供针对新技术的隐私保护。 这是一个合理的标准——法律对新技术的合理调整吗？ 还是法院应该在没有搜查令的情况下允许这样的搜查？ 或者政府是否必须满足第四修正案的要求，以便在技术存在之前需要搜查令的情况下对房屋进行每次搜查？

在 Kyllo 案的判决十多年后，执法机构在没有搜查令的情况下秘密使用建筑物外部的雷达设备来检测建筑物内的人的呼吸和活动。

老大哥会听吗？

我们在家里（和其他地方）使用越来越多的设备来响应口头命令。 许多公司都在销售用于电器和互联网的基于对话的界面，比我们在手机上的界面更复杂。 我们将在与另一个人交谈时与这些系统交谈，事实上，一些公司开发的系统具有个性。 为了使此类系统运行，麦克风必须始终打开。 将制定哪些原则或准则来使用或保护我们的对话？ 哪些规则将控制执法机构对麦克风的访问？

一个观察

我们讨论过的法庭案件涉及持械抢劫、谋杀和贩卖非法毒品的嫌疑人。 我们希望警察和检察官拥有合理的工具来抓捕和起诉暴力罪犯。 在讨论第四修正案的原则和案例时，记住禁止使用黄貂鱼和搜查手机的裁决并不意味着警察不能做这些事情可能是有用的。 这意味着他们必须出示证据来说服法官在这样做之前签发搜查令。 对于法院裁定不受第四修正案保护的信息（例如，您的手机服务提供商拥有的关于您使用手机的记录），执法机构自行决定或根据法院命令获取信息 标准低于搜查令。 即使一个机构有强有力的隐私保护政策，个别员工也可能以滥用或非法的方式访问或使用数据。 第四修正案的起草者非常清楚政府权力的滥用，并制定了权利法案来防止这种情况发生。

2.4 政府系统

Quis custodiet ipsos custodes? （谁会亲自看守守卫？）

—Juvenal，讽刺诗（1 世纪/2 世纪罗马）

2.4.1 视频监控与人脸识别

当监控摄像头开始出现在公共场所时，许多人将其视为对隐私的威胁，这是反乌托邦科幻小说中的场景。 然后，监控摄像头拍摄的照片有助于识别在伦敦地铁引爆炸弹的恐怖分子。 在骚乱者烧毁和抢劫英格兰的街区后，警方使用街头摄像机和面部识别系统的记录来识别骚乱者。 在波士顿马拉松爆炸案发生后，监控摄像头提供了炸弹袭击者的图像，他们很快就被确认了身份。 监控视频有助于识别袭击者或提供其他有助于调查布鲁塞尔、巴黎和尼斯恐怖袭击的信息。 现在无所不在的摄像头是一种有价值的保护还是一种深远的威胁——或者两者兼而有之？ 我们将在这里讨论相机和人脸识别的一些应用以及相关的隐私和公民自由问题。

早在过去十几年的恐怖袭击浪潮之前，英国是第一个在公共场所设置大量摄像头的国家； 目的是阻止犯罪。 英国一所大学的一项研究发现了监控摄像头操作员的一些滥用行为，包括收集色情镜头，例如人们在车内发生性行为，并将其展示给同事。 辩护律师抱怨说，检察官有时会销毁可能洗清嫌疑人嫌疑的镜头。 英国政府发布报告称，英国的闭路电视系统在打击犯罪方面作用不大。 这些摄像头唯一成功的用途是在停车场，它们帮助减少了车辆犯罪。

在人脸识别的首次大规模公开应用中，佛罗里达州坦帕市的警察在未通知与会者的情况下，扫描了进入 2001 年超级碗比赛（一些记者将其称为史努珀碗比赛）的所有 100,000 名球迷和员工的面部。 该系统在犯罪分子的计算机文件中搜索匹配项，并在几秒钟内给出结果。 美国公民自由联盟将在超级碗比赛中使用人脸识别系统比作计算机化的警察阵容，无辜的人在他们不知情或未经同意的情况下受制于他们。 坦帕在热门餐厅和夜总会附近安装了类似的系统。 控制室里的警察放大了个人面孔，并在他们的嫌疑人数据库中检查匹配项。 在两年的使用中，该系统没有识别出警方通缉的任何人，但它偶尔会把无辜的人识别为通缉犯。

人脸识别系统在 2000 年代初期的准确率很低，但随着技术的进步以及可匹配照片的可用性（例如，社交网络中标记的照片），人脸识别系统得到了改进。 警察或其他任何人现在都可以在街上拍下一个人的照片，并运行一个智能手机应用程序，该应用程序可以在流行的社交媒体网站上搜索个人资料图像以识别此人。

相机本身会引发隐私问题，但当与面部识别系统结合使用时，它们会严重侵蚀我们在公共场合的匿名性。 对年轻人实施宵禁是英格兰公共摄像机的用途之一。 此应用程序建议使用摄像机轻松监控特殊人群。 警方是否会使用人脸识别系统来追踪持不同政见者、记者和权势人物的政治对手——过去这些人是非法或可疑监视的目标？

一些城市增加了他们的摄像头监控程序，而其他城市则放弃了他们的系统，因为它们没有显着减少犯罪，或者因为它们的监控或维护成本太高。 （一些人赞成更好的照明和更多的警察巡逻——技术含量低且对隐私的侵犯较少。）多伦多市官员拒绝让警察接管他们的交通摄像头来监控抗议游行并确定其组织者。 加拿大隐私专员争辩说，该国的隐私法要求“收集到的每条个人信息都有明显的需要”以执行政府计划，因此记录大量公众的活动不是预防犯罪的可允许手段。

加州交通部拍摄了在特定区域行驶的汽车的车牌，然后联系车主对该区域的交通情况进行调查。 数以百计的司机抱怨，强烈反对政府机构进行他们认为不可接受的监视，即使该机构只拍摄他们的车牌，而不是他们的脸——用于调查，而不是警察行动。 许多普通人不喜欢在他们不知情的情况下被政府跟踪和拍照。

显然，相机和人脸识别系统的某些应用是合理的，有益于安全和预防犯罪的技术用途，而且显然需要控制和指导。

我们应该如何区分适当和不适当的使用？ 我们应该限制人脸识别系统等技术来抓捕恐怖分子和严重犯罪嫌疑人，还是应该允许它们在公共场所对人们进行筛查以找到那些未付停车罚单的人？ 有些摄像头是隐藏的。 人们是否有权知道何时何地使用相机？ 我们能否在技术中设计隐私保护功能，为其使用制定深思熟虑的政策，并在加拿大最高法院担心“隐私被消灭”之前通过适当的隐私保护立法？ 或者，美国有超过 3000 万个监控摄像头，现在已经来不及了吗？ 我们愿意在隐私与识别罪犯和恐怖分子之间做出哪些权衡？

允许国家代理人不受限制地进行视频监控会严重降低我们在自由社会中可以合理期望享有的隐私程度……我们必须始终警惕这样一个事实，即现代电子监控方法有可能，如果不受控制，破坏隐私。

-----Supreme Court of Canada

2.4.2 数据库

保护和侵犯

联邦和地方政府机构维护着数以千计的包含个人信息的数据库。 示例包括纳税申报表、财产所有权、医疗记录、离婚记录、选民登记、破产、止痛药等药物处方和逮捕记录。 其他包括申请政府拨款和贷款计划、专业和贸易许可证以及学校记录（包括儿童心理测试），还有很多很多。 政府数据库帮助政府机构履行职能、确定政府福利计划的资格、检测政府计划中的欺诈行为、征税并抓捕违法者。 政府活动的范围是巨大的，从抓捕暴力罪犯到许可发辫。 政府可以逮捕人、监禁他们并没收他们的资产。 因此，政府机构对个人数据的使用和滥用对自由和个人隐私构成了特殊威胁。 期望政府在隐私保护和遵守法律方面达到特别高的标准似乎是合理的。

1974 年的《隐私法》和 2002 年的《电子政务法》是有关联邦政府使用个人数据的主要法律。 尽管这项法律是试图保护我们在联邦数据库方面的隐私的重要一步，但它也存在问题。 引用一位隐私法专家的话说，《隐私法》存在“许多漏洞，执法不力，而且只有零星的监督”。 《电子政务法》增加了电子数据和服务的隐私法规——例如，要求机构对电子信息系统进行隐私影响评估，并在公众使用的机构网站上发布隐私政策：

- *将联邦政府记录中的数据限制为与政府收集数据的合法目的“相关和必要”的数据。*
- *要求联邦机构在联邦公报中发布其记录系统的通知，以便公众可以了解存在哪些数据库。*
- *允许人们访问他们的记录并更正不准确的信息。*
- *需要程序来保护数据库中信息的安全。*
- *禁止在未经本人同意的情况下披露其信息（有几个例外）。*

政府问责办公室 (GAO) 是国会的“监督机构”。 在过去的几十年里，GAO 发布了大量研究，显示隐私风险和违规行为以及隐私法的不合规性。 GAO 在 1996 年报告说，白宫工作人员使用了一个“秘密”数据库，其中记录了 200,000 人的记录（包括种族和政治信息），但没有适当的访问控制。 2006 年，GAO 对 65 个政府网站的研究发现，只有 3% 的网站完全符合联邦贸易委员会 (FTC) 为商业网站制定的关于通知、选择、访问和安全的公平信息标准。 （FTC 的网站不符合要求。）GAO 报告说，美国国税局 (IRS)、联邦调查局 (FBI)、国务院和其他使用数据挖掘来检测欺诈或恐怖主义的机构确实 不遵守收集公民信息的所有规则。 GAO 在医疗保险和医疗补助计划中用于传输医疗数据的政府通信网络的运行中发现了数十个弱点——这些弱点可能允许未经授权访问人们的医疗记录。

美国国税局是收集和存储该国几乎每个人的信息的几个联邦政府机构之一，并且是个人信息的主要二级用户。 年复一年，数百名美国国税局员工因未经授权窥探人们的税务档案而受到调查。 （在一次事件中，一名身为 Ku Klux Klan 成员的美国国税局雇员阅读了其 Klan 集团成员的税务记录，寻找收入信息，以寻找表明某人是卧底特工的收入信息。）这些滥用行为导致了一项对政府进行严厉处罚的法律 未经授权窥探人们税务信息的员工。 然而，几年后美国政府问责局的一份报告发现，虽然美国国税局做出了重大改进，但税务机构仍未能充分保护人们的财务和税务信息。 美国国税局员工能够在未经授权的情况下更改和删除数据，他们在没有擦除文件的情况下处理了带有敏感纳

税人信息的磁盘，并且丢失了数百盘磁带和软盘。 财政部监察长的一份报告称，美国国税局没有充分保护 50,000 多台笔记本电脑和其他存储介质上的纳税人信息。 2015 年，黑客能够通过在 IRS 网站上为纳税人创建新帐户来访问纳税人信息。 这个网站只需要最少的纳税人信息就可以创建账户，一旦账户创建，黑客就可以查看过去的纳税申报表和纳税情况。 美国国税局不得不关闭该服务，并通知数十万纳税人他们的信息存在风险。 在这种情况下，纳税人信息的泄露不是因为美国国税局系统遭到直接黑客攻击，而是因为账户创建政策薄弱。

对《隐私法》和《电子政务法》合规性的各种审查突出了这些法律的弱点。 例如，GAO 认识到大多数人不阅读《联邦公报》，因此建议采用更好的方式让公众了解政府数据库和隐私政策。 GAO 继续提倡对个人信息的使用进行更严格的限制，并修改《隐私法》以涵盖联邦政府收集和使用的所有个人身份信息，从而弥补使政府对个人信息的使用免于法律规定的漏洞。

政府使用私营部门资源

正如信息安全和隐私咨询委员会（政府咨询委员会）指出的那样，“隐私法没有充分涵盖政府对商业编译的个人信息数据库的使用。 关于联邦政府使用商业数据库，甚至使用从商业搜索引擎收集的信息的规定一直很模糊，有时甚至根本不存在。” 因此，机构可以通过使用私营部门来绕过隐私法的保护数据库和搜索，而不是收集信息本身。

在一个示例中，纽约市警察局向一家私营公司支付费用，以访问该公司的数据库，该数据库从全国各地的车牌阅读器收集数据。 阅读器安装在公寓大楼、办公园区和其他私人区域以及公共街道上。 该系统可以提供经常在特定位置看到或经常一起看到的车辆列表。 它还可以预测车辆在特定时间可能所在的位置。 该系统有助于定位凶手并在寻找罪犯方面具有明显的优势，但警察是否应该能够在没有法律或法院监督的情况下随意访问此类数据？ 这些数据，主要是关于无辜者的数据，是否应该提供给纽约警察局五年？

关于数据挖掘非政府数据库以发现恐怖分子和恐怖阴谋的提议继续出现。 我们总结了 Jeff Jonas 和 Jim Harper 提出的关于适用性的有趣观点，为此目的进行数据挖掘。 营销人员大量使用数据挖掘，花费数百万美元分析数据以找到可能成为客户的人。 可能性有多大？ 在营销中，百分之几的响应率被认为是相当不错的。 换句话说，昂贵、复杂的数据挖掘具有很高的误报率； 大多数被数据挖掘识别为潜在客户的人都不是。 许多收到有针对性的广告、目录和销售宣传的人没有回应。 垃圾邮件和弹出式广告会惹恼人们，但它们不会严重威胁公民自由。 但是，在寻找恐怖嫌疑人的数据挖掘中误报率很高。 数据挖掘可能有助于从大量消费者数据中挑选出恐怖分子，但适当的程序对于保护无辜但被错误选择的人至关重要。乔纳斯和哈珀争论使用方法寻找对大量人的隐私和公民自由威胁较小且成本效益更高的恐怖分子。

数据库示例：跟踪大学生

美国教育部提议建立一个数据库，以包含在美国学院或大学注册的每个学生的记录。 学院和大学将提供并定期更新记录，包括每个学生的姓名、性别、社会安全号码、专业、所修课程、通过的课程、学位、贷款和奖学金（公共和私人）。 政府将无限期地保留数据。 强烈的反对意见阻碍了这项提议的实施。 我们以它为例进行分析； 我们在这里提出的议题和问题适用于许多其他情况。

联邦政府每年花费数十亿美元用于向学生提供联邦助学金和贷款，但没有一种全面的方法来衡量这些项目的成功与否。 获得援助的学生会毕业吗？ 他们攻读什么专业？ 该数据库将有助于评估联邦学生援助计划，并可能导致计划的改进，并提供有关毕业率和实际大学费用的更准确数据。 跟踪教育管道中未来护士、工程师、教师等的数量的能力有助于制定更好的移民政策以及商业和经济规划。

另一方面，在一个地方收集如此多关于每个学生的详细信息说明了我们在第 2.1.2 节中描述的许多隐私风险。 政府很可能会为不属于原始提案的数据找到新的用途。 这样的数据库可能是身份窃贼的理想目标。 许多种类的信息

泄露都是可能的。 维护数据的工作人员有可能滥用； 例如，有人可能会发布政治候选人的大学记录。 毫无疑问，数据库中会有错误。 如果该部门将数据的使用限制在广义统计分析中，错误可能不会产生太大影响，但对于某些潜在用途，错误可能会造成重大损害。

该数据库的计划用途不包括寻找或调查违法学生，但它对执法机构来说是一个诱人的资源。 弗吉尼亚州的一项法律要求大学提供他们接受的所有学生的姓名和其他身份信息。 然后，州警察会检查性犯罪者登记处是否有任何人。 他们还可以检查什么？ 其他哪些政府机构可能想要访问联邦学生数据库？ 国防部会使用该数据库进行军事招募吗？ 如果雇主获得访问权限，会出现哪些潜在风险？ 未经学生同意，所有此类用途均为二次用途。

一些教育工作者担心，该数据库与公立学校数据库（从幼儿园到高中的儿童）之间的最终链接会创建对儿童行为问题、健康和家庭问题等的“从摇篮到坟墓”的跟踪。 此类数据已经面临风险：在针对加州教育部的诉讼中，法官准许提起诉讼的组织访问该部门保存的数百万学童的大量敏感数据。 尽管法官对数据的处理设置了限制，但在数据收集开始时，家长可能没有想到会出现这种访问权限。

政府监控其提供给大学生的助学金和贷款的有效性是有意义的，因此要求获得联邦资金或贷款担保的学生的学业进步和毕业数据是合理的。 但是，有什么理由要求所有其他学生的数据呢？ 对于统计和规划，政府可以进行自愿调查，就像企业和组织一样，没有政府的强制力必须这样做。 数据库的好处是否足以成为政府基本责任的核心，足以超过风险并证明对每个学生的如此多的个人数据进行强制性报告计划是合理的？

Note: 该提案的批评者，包括许多大学，指出了除隐私之外的其他风险和成本。 大学担心收集数据会导致联邦控制和干预大学管理的增加。 报告要求会给学校带来高昂的成本。 整个项目会给纳税人带来高昂的成本。

在考虑政府对个人数据使用或数据挖掘的每一个新系统或政策时，我们应该问很多问题：它使用或收集的信息是否准确有用？ 侵入性较小的方法会达到类似的结果吗？ 该系统会不会给普通人带来不便，同时又容易被犯罪分子和恐怖分子阻挠？ 风险有多大

2.4.3 公共记录：访问与隐私

许多联邦和州数据库中的一些包含“公共记录”，即可供公众使用的记录。 示例包括破产记录、逮捕记录、结婚证申请、离婚诉讼、财产所有权记录（包括抵押信息）、政府雇员的工资和遗嘱。 这些长期以来一直是公开的，但只能在政府办公室以纸质形式获得。 律师、私家侦探、记者、房地产经纪人、邻居和其他人都会使用这些记录。 现在在 Web 上搜索和浏览文件变得如此容易，越来越多的人出于娱乐、研究、有效的个人目的以及可能威胁他人的和平、安全、个人秘密和财产的目的访问公共记录 .

公共记录可能包括敏感信息，例如社会安全号码、出生日期和家庭住址。 亚利桑那州的马里科帕县是第一个将大量完整的公共记录放到网上的县，该县的身份盗用率在美国最高。 显然，公共记录网站应该保留某些敏感信息。 这样做需要决定要保护哪些类型的数据，并且可能需要对政府软件进行昂贵的修改。 一些地方政府采取了政策来阻止显示在线发布的文件中的敏感数据，一些州有法律要求这样做。

为了说明更多关于公共记录的问题和降低风险的方法，我们描述了几种专门的信息——私人飞机的航班信息、政治捐款和法官的财务报表——然后提出一些问题。

美国大约 12,000 架公司飞机的飞行员在飞行时提交飞行计划。 一些企业将从政府数据库中获得的航班信息与飞机登记记录（也是政府的公共记录）结合起来，以提供一种服务，告知特定飞机的位置、到达目的地等信息。 公司

报告由此产生的问题，从寻求签名的体育迷到对公司高管的死亡威胁。 还有谁可能需要这些信息？ 公共利益团体和记者——宣传个人使用政府或公务机； 竞争对手——确定另一家公司的高管与谁会面； 和恐怖分子——追踪高调目标的动向。 出于安全和隐私方面的考虑，美国联邦航空管理局现在允许私人飞机所有者向公众屏蔽他们的航班信息。

政治竞选委员会必须要求并报告捐赠者的姓名、地址、职业、雇主和捐赠金额给总统候选人。*这些信息对公众开放。过去，主要是记者和竞争对手的竞选活动对其进行了审查。 既然它在网上而且很容易搜索，任何人都可以找到他们的邻居、朋友、雇员和雇主支持的候选人。 我们还可以找到知名人士的地址，他们可能更愿意将地址保密以保护他们的安宁和隐私。

联邦法律要求联邦法官提交财务披露报告。这些报告可供公众使用，目的是确定某位法官是否可能在特定案件中存在利益冲突。 当一家在线新闻机构起诉在网上发布报道时，法官反对报道中的信息可能会泄露家庭成员在哪里工作或上学，从而使他们面临被告对法官生气的风险。 最终，报告上线，删除了一些敏感信息。

信息获取便利性的变化改变了将某些类型的数据公开的优点和缺点之间的平衡。 每当访问发生重大变化时，我们都应该重新考虑旧的决定、政策和法律。 将所有财产所有权记录公开的好处是否超过我们在练习 2.36 中描述的隐私风险和盗窃风险？ 报告小额政治捐款的好处是否超过隐私风险？ 或许。 关键是应该定期提出和解决此类问题。

我们应该如何控制对敏感公共记录的访问？ 根据法官财务报表的旧规定，当它们在纸上时，请求访问的人必须签署一份披露其身份的表格。 法官的报告向公众公开，但访问这些报告的人员的记录可以阻止意图伤害他人的人。 这是一个明智的规则，但我们可以在线实施类似的系统吗？ 用于在线识别和验证人员身份的技术正在开发中，但它们还不够普及，无法供访问 Web 上敏感公共数据的每个人使用。 将来我们可能会经常使用此类工具，但这会引发另一个问题：我们如何区分需要身份验证和签名才能访问的数据与公众应该可以自由匿名查看的数据，以保护查看者的隐私？

2.4.4 国民身份证系统

在美国，国家身份识别系统始于 1936 年的社会保障卡。近几十年来，社会安全号码问题以及对非法移民和恐怖主义的担忧促使人们越来越多地支持更复杂、更安全的国家身份识别系统。 反对其中一些提案是基于对隐私和潜在滥用（以及成本和实际问题）的担忧。 在本节中，我们将回顾社会安全号码、有关国民身份证系统的各种问题以及真实身份法案，这是将驾驶执照转变为国民身份证的重要一步。

社会安全号码 (SSN) 的历史说明了国家身份识别系统的使用是如何增长的。 当 SSN 于 1936 年首次出现时，它们专供社会保障计划使用。 政府当时向公众保证，不会将这些号码用于其他目的。 仅仅几年后，即 1943 年，罗斯福总统签署了一项行政命令，要求联邦机构将 SSN 用于新的记录系统。 1961 年，美国国税局开始使用它作为纳税人识别号，因此必须向美国国税局报告金融交易的雇主和企业需要它。 1976 年，州和地方税务、福利和机动车辆部门获准使用 SSN。 1988 年的联邦法律要求父母提供 SSN 才能为孩子取得出生证明。 在 1990 年代，联邦贸易委员会鼓励征信机构使用 SSN。1996 年的一项法律要求各州为职业执照、结婚执照和其他类型的执照收集 SSN。尽管政府另有承诺，SSN 已成为通用的身份识别号码。

似乎很少（如果有的话）政府机构和其他组织认识到安全对于用于多种用途的识别号码的重要性。 SSN 通常出现在财产契约等文件中，这些文件是公共记录（可在线获取）。 几十年来，许多大学都使用 SSN 作为学生和教职员工的 ID 号码； 这些数字出现在身份证和班级花名册上。 我 (TH) 任教的一所大学使用我的名字和我 SSN 的最后四位数字作为我的公共电子邮件地址。 （它已经结束了这种做法。）SSN 印在 Medicare 计划中数百万人的 Medicare 卡上。 弗吉尼亚州将 SSN 列入已公布的选民名单，直到联邦法院裁定要求 SSN 进行选民登记是违宪的。 国会要

求所有驾照都显示驾驶员的 SSN，但由于强烈抗议，国会在几年后废除了该法律。 一些雇主使用 SSN 作为标识符并将其放在徽章上或应要求提供。 美国农业部无意中将超过 35,000 名农民的 SSN 包含在一个网站上，该网站发布了有关向农民提供贷款和赠款的详细信息。

从金融机构到本地有线电视公司的各种企业都要求您提供 SSN，或者在您打电话给他们时的最后四位数字。 这意味着他们将号码存储在他们的记录中。 在第 2.1.2 节和第 5 章中，我们列出了许多黑客窃取数百万此类包含 SSN 的消费者记录的事件。 知道您的姓名并拥有您的 SSN 的人可以不同程度地轻松访问您的工作和收入历史记录、信用报告、驾驶记录和其他个人数据。 SSN 的广泛使用使我们面临欺诈和身份盗用的风险。 加利福尼亚州一所初级学院的兼职英语教师使用班级名单上提供的一些学生的 SSN 开设欺诈性信用卡账户。 窃取数百万人社会安全号码的黑客大规模使用或出售这些号码进行金融欺诈。

SSN 的使用范围太广，无法安全地识别某人。 社会保障卡很容易伪造，但这无关紧要，因为索取号码的人很少索要卡，而且几乎从不验证号码。 社会保障局本身过去常常在不核实申请人提供的信息的情况下发卡。 由于 SSN 的问题，犯罪分子可以轻松地创建虚假身份，而无辜、诚实的人则遭受个人信息泄露、逮捕、欺诈、信用评级被破坏等。

政府和企业逐渐认识到粗心使用 SSN 的风险以及我们不应该如此广泛使用它的原因。 各州法律现在禁止企业和组织要求提供 SSN 。如果他们不需要它。SSN 并不是一个通用的、安全的识别号码，尝试将其用作一个号码的尝试不仅失败了，而且还损害了隐私和财务安全。 接下来，我们将研究更广泛、更安全、数字连接的国民身份证系统的计划。

新的美国国民身份证系统

很明显，需要一个安全的 ID 系统来取代社会安全号码，并用于需要识别人员身份的各种政府用途。 近年来，各政府机构提出了新的国民身份证系统。 这些卡将有大量应用，包括公民身份、就业、健康、税收、财务或其他数据，以及指纹或视网膜扫描等生物识别信息，具体取决于具体提案和提倡它的政府机构 . 在许多提案中，身份证还可以访问各种数据库以获取更多信息。

国家身份证系统的倡导者描述了许多好处，其中一些取决于用于大量政府和私人应用程序的卡：

- *您将需要实际的卡，而不仅仅是一个数字，来验证身份。*
- *这些卡比社会保障卡更难伪造。*
- *如果身份证取代所有其他形式的身份证，一个人只需要携带一张卡，而不是像我们现在的各种服务分开一张卡。*
- *身份验证将有助于减少私人信用卡交易和政府福利计划中的欺诈行为。*
- *使用身份证来验证工作资格可以防止人们在美国非法工作。*
- *罪犯和恐怖分子将更容易追踪和识别。*
- *因涉嫌非法入境美国而被警方骚扰或拘留的公民—这是一些少数族裔人群的常见问题—将能够出示身份证以确认他们的公民身份。*

那些对多功能国民身份证系统持谨慎态度的人认为，它们是对自由和隐私的严重威胁，身份证系统中的错误可能会产生毁灭性的影响。 “请出示证件”是与警察国家和独裁政权相关的要求。 根据南非臭名昭著的通行证法，人们携带通行证或身份证件，按种族对他们进行分类，并控制他们可以生活和工作的地方。 在第二次世界大战期间的德国和法国，身份证明文件包括个人的宗教信仰，这使得纳粹很容易抓捕和驱逐犹太人。 在美国，政府机构从人口普查局获得了日裔美国人的位置数据（用于二战期间的拘留）和各种邮政编码中阿拉伯血统人数的数据（2001 年恐怖袭击后） ，暗示可以在自由国家发生的群体定位类型。 Peter Neumann 和 Lauren Weinstein 警告说，支持国家身份证系统的数据库和通信综合体会带来风险：“过度监视和严重侵犯隐私的机会几乎是无限的，伪装、身份盗窃

和严厉的机会也是如此。 大规模的社会工程。”

一些身份证系统的目标是“一卡社会”，只携带一张卡的便利性吸引了很多人。 但是，现在，如果您丢失了学生证等，您仍然可以使用信用卡购物、看医生和开车。 单卡 ID 丢失或被盗将阻止许多活动。 同样，系统中的错误可能是毁灭性的。 例如，在五年期间，美国退伍军人事务部错误地将 4200 多名领取退伍军人福利的人归类为死亡；它停止发送他们的支票。 尽管受影响的人数占每年死去的退伍军人的比例很小，但影响却很严重，例如，导致一些人无力支付房租。 如果一个人被错误地归类为一卡系统中的死亡，其影响将更加严重。 这样一张卡片是否如一位评论家所说的那样是“存在的许可”？

某些形式的身份证明，例如军人的护照和身份证，具有高度的安全性。 （也就是说，获得一个需要对申请人进行身份验证，而且它们很难伪造。）重要的是，用于此类应用程序的 ID 卡能够可靠地识别用户。 超市俱乐部卡这样做并不重要。 显然，我们要问国民身份证应该扮演什么角色。 一些基本应用包括税收目的、选民身份识别、社会保障和医疗保险以及政府福利身份识别。 还有什么？ 如果我们将新的国民身份证号码用于多种用途，包括各种业务的在线和电话识别，我们很快就会遇到一些与 SSN 相同的问题：黑客会窃取号码并获得对许多系统的访问权限 其中需要号码而不是卡。

另一个问题是法律是否应要求公民始终携带身份证。 如果该卡连接到许多数据库，就像在某些提案中那样，警察在街上拦住某人时可以访问哪些信息？ 应谨慎对待具有大量用途和连接的国家 ID 系统的计划。

我们需要更多地考虑身份识别系统的多样化。

—Jim Harper

REAL ID

REAL ID Act 试图通过制定驾驶执照的联邦标准（以及州颁发的身份证，适用于没有驾驶执照的人）来开发安全的国民身份证。 许可证必须符合这些标准才能被联邦机构用于识别。 此类用途包括机场安检和进入联邦设施。 言下之意，它们包括为联邦政府工作和获得联邦福利。 政府很可能会增加许多新用途，就像它对社会安全号码所做的那样。 企业以及州和地方政府已经要求使用联邦批准的卡来进行许多交易和服务。 联邦政府支付美国大约一半的医疗费用（例如，Medicaid、Medicare、退伍军人福利以及许多联邦资助的计划），因此不难想象需要驾驶执照才能获得联邦医疗服务并最终 它成为事实上的国民医疗身份证。

REAL ID Act 要求，要获得联邦批准的驾驶执照或身份证，每个人都必须提供地址、出生日期、社会安全号码和在美国的合法身份的文件。机动车辆部门必须验证每个人的信息，部分方法是访问联邦数据库，例如社会保障数据库。这些部门必须扫描申请人提交的文件，并将其以可转让的形式存储至少 10 年（使机动车记录成为身份窃贼的理想目标）。 许可证必须满足减少篡改和伪造的各种要求，必须包含个人照片，并且信息必须采用机器可读的形式。

REAL ID Act 将核实身份的责任加在了个人和州机动车辆部门身上。 许多州反对这项授权及其高昂的成本（估计为数十亿美元），20 多个州最初通过了拒绝参与的决议。 没有联邦批准的驾驶执照的州的居民可能会遇到严重的不便。 当国会在 2005 年通过 REAL ID 时，它将于 2008 年生效。国土安全部多次延长截止日期。 到 2020 年 10 月，所有乘坐商业航班在美国境内旅行的人都必须持有 REAL ID 身份证或运输安全管理局可接受的其他身份证明。

其他国家的例子

世界上大约有一半的国家建立了某种形式的国民身份证制度。 在其中许多国家/地区，18 岁以上的公民必须携带该卡（或在被要求时出示），并且必须出示有效的身份证才能投票。

日本于 2002 年推出的国家计算机登记系统为每个公民分配了一个 ID 号码，旨在简化政府项目的管理程序并提高其效率。 该系统遭到了非常强烈的抗议：人们抱怨隐私保护不足、可能被政府滥用以及容易受到黑客攻击。 几个城市拒绝参与。 2015-2016 年，日本引入了新系统 My Number。 该号码和相关的身份证旨在链接税收、养老金、医疗、就业和婚姻状况记录。 连接银行可以添加记录，以便 My Number 卡取代信用卡和借记卡。

印度政府正在为其 12 亿人建立一个全国身份证数据库，其中包括每个人的照片、指纹和其他生物识别数据、出生日期和其他信息。 其目的包括提供身份证明、改善政府服务的提供以及在该国抓捕非法人员。 公民自由团体提出隐私异议，印度最高法院限制了身份证号码的应用，并下令不强制要求提供。

当有关该计划弱点的电子邮件从政府办公室泄露时，英国一项不受欢迎的昂贵的强制性国民身份证计划陷入僵局。

爱沙尼亚拥有约 130 万人口，拥有成功的现代国家身份证系统。 其 ID 智能卡可验证在线投票的身份，用于医疗保健和在线银行业务，并包含使人们能够签署数字文档的加密密钥。 国家规模是爱沙尼亚体系成功的重要因素吗？

纳粹德国、苏联和种族隔离时期的南非等地都有非常强大的身份识别系统。 诚然，身份识别系统不会造成暴政，但身份识别系统是暴政经常使用的非常好的行政系统。

—Jim Harper

2.4.5 NSA 和秘密情报收集

国家安全局 (NSA) 的目的是收集和分析与国家安全有关的外国情报信息，并保护美国政府的通信和与国家安全有关的敏感信息。 1952 年，一项秘密总统命令成立了 NSA。尽管其网站称 NSA/CSS（NSA 和中央安全局）的规模与较大的财富 500 强公司之一相当，但其预算仍然是秘密。 美国国家安全局建造并使用功能极其强大的超级计算机来处理它收集和存储的海量信息。 由于政府对他们的敏感材料进行加密，因此美国国家安全局长期以来一直在密码学上投入大量资源，并拥有非常先进的密码破译能力。

由于美国国家安全局使用的方法不符合第四修正案，因此在法律上仅限于拦截美国境外的通信（有一些例外）。 纵观其历史，该机构因秘密违反对美国境内人员监视的限制而引发了很多争议。 在 1960 年代和 70 年代，美国国家安全局监控特定美国公民（包括民权领袖马丁路德金和反对越南战争的艺人）的通讯。 一个国会委员会（丘奇委员会，由参议员弗兰克·丘奇担任主席）发现，自 20 世纪 50 年代以来，美国国家安全局一直在秘密非法收集国际电报，包括美国公民发送的电报，并从中搜索外国情报信息。 结果，国会通过了 1978 年外国情报监视法 (FISA)，为国家安全局制定了监督规则。 法律禁止该机构在没有授权的情况下收集大量电报，也禁止在没有法院命令的情况下编制要观看的美国人名单。 该法律设立了一个秘密的联邦法院，即外国情报监视法院，向美国国家安全局发出授权令，以拦截它可能表明是外国势力特工或参与恐怖主义或间谍活动的人的通信。

财富、旅行和贸易的增加产生了更多的国际交流——使交流渠道变得混乱，并可能使美国国家安全局更难发现感兴趣的信息。 然后，计算机系统处理能力的大幅提升使美国国家安全局能够过滤和分析无辜者的大量通信，而不是只针对特定的嫌疑人。 在网络空间中，我们的电子邮件、电话交谈、推文、搜索、购买、财务信息、法律文件等与军事、外交和恐怖主义通信混在一起。 NSA 对所有信息进行筛选，分析通过 Internet 传输的信息包，并收集任何感兴趣的信息。 这种拦截活动极具争议性，因为 NSA 在没有法院命令和 FISA 法院批准的情况下处理和收集美国人的数据。

2006 年，一名 AT&T 员工描述（宣誓）美国国家安全局在 AT&T 交换设施中设立的秘密安全室。 从这个房间，美国国家安全局可以访问 AT&T 用户的电子邮件、电话和 Web 通信。 美国国家安全局建立了一个包含数百万美国人的电话和电子邮件记录数据库。 政府争辩说，国家安全局没有拦截或窃听电话，也没有收集个人身份信息。 它使

用复杂的数据挖掘技术来分析呼叫模式，以了解如何检测恐怖组织的通信。 监控计划的反对者说，国家安全局未经授权收集记录是非法的，电话公司提供这些记录也是非法的。 国会于 2008 年通过了 FISA 修正案，追溯保护 AT&T（以及协助 NSA 的其他实体）免受诉讼。 一些针对 NSA 的监控程序的诉讼仍在通过法院进行。 FISA 修正案包括限制国内监视的条款，但总的来说它减少了以前的保护。

2013 年，为 NSA 工作的安全承包商爱德华·斯诺登 (Edward Snowden) 下载了大量有关 NSA 活动的文件。 许多人最终被公开释放。 这些文件表明，除其他外，美国国家安全局可以搜索任何人在互联网上进行的大多数活动； 它直接从雅虎、Facebook、谷歌和微软等几家美国主要科技公司的服务器收集数据； 它要求电话记录 Verizon 所有美国客户的数据（并禁止 Verizon 与其客户讨论信息发布问题）； 它监视欧洲主要国家的领导人； 它监控数百万未被指控犯有恐怖主义或与恐怖活动有关联的外国人的通讯。 尽管记者之前曾报道过其中一些活动，但这份关于美国国家安全局监视计划的细节和范围的文件震惊了许多美国人和外国人。

NSA 已经建立了巨大的数据中心来存储、解密和分析数十亿字节的通信和文件。70 现在无法解密的内容会存储起来，以便在开发出更快的计算机或更好的算法时进行解密。 公民自由主义者担心国家安全局正在收集大量与恐怖主义或外国情报无关的普通商业和个人加密数据。

我们如何评估美国国家安全局收集大量通信数据和在线活动的计划？ 正如我们过去经常看到的那样，监视和收集监视数据的秘密程序存在巨大的滥用潜力，当调查人员错误地认为某人的交易看起来可疑时，它们会威胁到无辜者的声誉、安全和自由。 当我们的政府了解我们所有行动、运动和偏好的细节时，官方对持不同政见者、政治对手或少数群体的镇压就变得更容易了。 当个别员工可以在几乎没有监督的情况下记录一个人的在线活动时，他们就可以监视熟人，事实上，公布的文件显示，一些 NSA 员工监视他们的“爱情兴趣”。 但是，在任何大型组织中都可能发生的这种个人滥用行为，是否是收集信息以保护国家的必要性的一个小代价？ NSA 是否在做国家安全机构必须做的事情？ 我们经历了恐怖主义的可怕影响，包括来自美国境内的袭击。 过去，对安全的国内外威胁有着明显的区别，NSA 和 FBI 的角色明显不同，法律限制也不同。 防止恐怖袭击需要的工具不仅仅是在犯罪发生后收集有关嫌疑人的信息。 我们不知道是谁在策划袭击，但必须找出答案。 我们的法律应该允许国家安全局做什么？ 当它违反现行法律时，我们应该如何应对？

2.5 保护隐私：技术与市场

2.5.1 开发隐私工具

许多个人、组织和企业在某种程度上帮助满足隐私需求：

- 个人程序员在 Web 上发布免费的隐私保护软件。
- 企业家建立新公司以提供基于技术的隐私保护。
- 大型企业响应消费者需求并改善政策和服务。
- 隐私权信息交换所等组织提供了极好的信息资源。
- 电子隐私信息中心等维权组织向公众通报信息、提起诉讼并倡导更好的隐私保护。

技术的新应用通常可以解决由于其他技术的副作用而出现的问题。 在“技术人员”意识到网站使用 cookie 后不久，他们编写了 cookie 禁用程序并在 Web 上提供它们。阻止弹出式广告的软件在此类广告出现后不久就出现了。公司出售扫描间谍软件的软件； 有些版本是免费的。 有几家公司提供称为匿名器的服务，人们可以通过这种服务匿名上网，不留下任何可以识别他们或他们的计算机的记录。 某些搜索引擎不会以以下方式存储用户搜索查询 允许将它们链接到一个人。71 公司提供产品和服务以防止转发、复制或打印电子邮件。 （律师是主要客户之一。）有些服务可以在用户指定的时间段后完全删除电子邮件或短信（在发件人和收件人的手机上）； 一款流行的消息传递应用程序会在收件人查看照片后的几秒钟内删除照片。 如果我们的笔记本电脑、平板电脑或手机被盗或丢失，我们可以远程加密、检索和/或擦除文件。

对在线活动的广泛和隐藏跟踪导致要求在浏览器中设置“禁止跟踪”(DNT)。 浏览器将 DNT 设置发送到用户访问的网站。 默认值应该是多少？ 隐私保护的默认设置似乎是打开 DNT。 但是，数字广告联盟和其他商业团体与美国政府达成协议，如果用户打开 DNT 设置，则尊重该设置。 当一些浏览器默认设置 DNT 时，一些广告商选择完全忽略它。 因此，在这一点上，一个常见的默认设置是 DNT 是“未设置”的，并且可以由每个用户打开或关闭。 对于忽略 DNT 设置的站点，我们可以在我们的浏览器中安装免费的插件来阻止 Web 活动跟踪器。

这些是保护隐私的产品和技术应用的极少数例子，但它们并不能解决所有问题。 了解、安装和使用隐私工具可能会让非技术人员、受教育程度较低的用户（大部分公众）望而生畏，因此在设计系统时考虑到隐私保护、构建保护功能并制定隐私保护政策非常重要。

2.5.2 加密

密码学是将数据隐藏在众目睽睽之下的艺术和科学。

—Larry Loen

免费提供的工具可以拦截传输中的数据，如果没有受到保护，小偷或黑客可以在被盗或被黑的计算机上读取数据。如果肇事者被抓获并定罪，法律将对这些行为进行惩罚，但我们也可以使用技术来保护自己。 加密是一种技术，通常在软件中实现，它将数据转换为对任何可能拦截或查看它的人来说毫无意义的形式。 数据可以是电子邮件、商业计划、信用卡号码、图像、医疗记录、手机位置历史等。 收件人站点（或自己的计算机上）的软件对加密数据进行解码，以便收件人（或所有者）可以查看消息或文件。 人们通常甚至不知道他们正在使用加密，因为软件会自动处理它。 例如，当我们将信用卡号发送给在线商家时，该软件会对其进行加密。 WhatsApp 等电话应用程序会自动加密通话和消息。

隐私和安全专家将加密视为确保通过计算机网络发送的消息和数据的隐私的最重要的技术方法。加密还可以保护存储的信息免受入侵者和员工的滥用。 它可以保护在办公室外携带的笔记本电脑和其他小型数据存储设备上的数据。

加密通常包括编码方案或密码算法，以及特定的字符序列（例如，数字或字母），称为密钥，算法使用这些字符序列对数据进行编码或解码。 使用数学工具和强大的计算机，有时可以“破解”旧的或弱的加密算法——也就是说，在没有密钥的情况下解码加密的消息或文件。

现代加密技术非常安全，并且具有超越保护数据的灵活性和多种应用。 例如，它用于创建数字签名、身份验证方法和数字现金。 数字签名技术使我们能够在线“签署”文件，为贷款申请、商业合同等节省时间和纸张。 其他应用程序提供身份验证； 例如，美国医学协会向医生颁发数字凭证，实验室网站可以在医生访问以获取患者测试结果时对其进行验证。

数字现金系统和其他基于加密的隐私保护交易方式，例如比特币、莱特币和瑞波币，可以让我们以电子方式进行安全的金融交易，而无需卖家从买家那里获取信用卡或支票账号。 他们结合了信用卡购物的便利性和现金的匿名性。使用此类方案，很难将不同交易的记录链接起来形成消费者档案或档案。 这些技术既可以为消费者提供与其交互的组织相关的隐私保护，也可以为组织提供保护以防止伪造、空头支票和信用卡欺诈。 然而，现金交易使政府更难发现和起诉那些“洗钱”非法活动所得、赚取未向税务机关报告的金钱，或为犯罪目的转移或花费金钱的人。 因此，许多政府反对真正匿名的数字现金系统。 一些系统包括执法和税收的规定。 数字现金的潜在非法使用长期以来一直存在于真实现金中。 直到最近几十年，随着支票和信用卡的使用越来越多，我们才失去了在大多数交易中使用现金时从营销人员和政府那里得到的隐私。

匿名和密码技术可能是保护隐私的唯一途径。

—Nadine Strossen, former president of the American Civil Liberties Union

2.5.3 屏蔽广告

我们探讨了在线广告的问题、屏蔽广告的道德规范，以及对广告屏蔽的反应，因为广告屏蔽会引发几个问题，作为应用第 1 章介绍的伦理理论的练习，并说明解决问题的各种方法。

屏蔽广告的道德规范

跳动的、刺耳的、烦人的、侵入性的广告出现在我们的手机、电脑屏幕和其他设备上。 其中一些会减慢我们想要的内容的下载速度； 有些会耗尽电池电量。 有些跟踪在线活动并收集可能被滥用的个人信息。 有些广告会安装恶意软件。

一个广告行业组织估计，美国 26% 的互联网用户安装了广告屏蔽器。当 Apple 发布了一个支持应用程序屏蔽广告的移动操作系统版本时，数十万用户在一周内安装了广告屏蔽应用程序。 作为回应，一些软件开发商和网络出版商开始质疑屏蔽广告或向数百万用户出售工具的道德规范。 为什么？ 广告为免费视频和图片网站、免费社交网络以及网络上的大量免费内容付费。 广告有助于支持小型在线出版商并引起公众的注意。 那些质疑屏蔽广告（或提供这样做的工具）道德的人着眼于长远，担心如果太多人屏蔽广告，许多免费内容可能会消失，工作可能会流失——对整个社会产生负面影响。 创建、销售或使用广告拦截器是否合乎道德？

忽略或屏蔽广告并不新鲜。 当人们在拥有互联网和录像机之前观看广播电视时，广告会提示该上厕所或该去厨房吃点心了。 当录像机问世后，人们开始快速浏览广告。 跳过为免费电视内容付费的广告是否不道德？ 在我们继续讨论时，请考虑您对电视和互联网或移动广告的回答是否一致，如果不一致，请确定导致不同立场的特征。

道义学家的观点：

屏蔽广告并不违反禁止说谎的道德禁令。 如果我们屏蔽广告，我们是否在窃取免费内容？ 广告商和网络出版商不相信这一点。 他们免费向观众提供他们的材料； 他们了解并非所有人都会查看或响应广告。

康德强调使用理性——道德行为应该是理性的——道德规则应该普遍适用于所有人。 让我们考虑一下广告拦截是不道德的立场的含义。 不屏蔽广告就够了吗？ 假设我们不屏蔽广告，但我们忽略它们。 对于许多广告，托管广告的网站只有在人们点击或点击广告时才会付费。 我们必须点击每个广告吗？ 最终，即使点击广告也是不够的。 广告商不会继续为广告付费，除非它们产生足够数量的销售、会员、签名——或者广告商想要的任何东西。 每个人都必须购买我们看到的所有广告吗？ 当然不是。 广告支持内容的延续需要一定数量的人购买广告产品或服务。 这似乎并不能证明在个人设备上屏蔽广告的普遍道德禁令是合理的。

其他道德方法对于考虑广告拦截的更广泛社会后果以及创建和推广这样做的工具更有用。 我们接下来考虑它们。

功利主义分析：
功利主义者评估后果的消极和积极效用。 广告拦截器的一些负面影响是：

- 小型网络出版商可能会失去广告收入。
- 曾经免费的内容变得不可用或变得昂贵。
- 人们（作家、广告商等）可能会失去工作。
- 使用广告拦截器的人可能会错过了解和购买他或她想要的产品的机会。

一些积极因素是：

- 增加隐私：免于入侵是隐私的一方面。 减少商业主义的入侵。
- 改进了系统性能。
- 更愉快的在线体验。

我们如何量化这些？ 广告拦截的大部分负面影响取决于这样一个假设，即对广告的反应将大幅下降，足以对广告行业本身产生负面影响，并减少有价值内容的可用性。 由于广告拦截而给出版商造成的损失的报告和预测以数十亿美元计，但差异很大。 我们如何确定内容消失的可能性、消失的数量以及丢失的内容的价值？ 一些出版商可能会找到其他收入来源来保持在线，例如，来自慈善组织或众筹的支持。 有些人可能会将他们的精力和技能投入到其他项目上，这些项目比他们失败的项目对他们和公众更有用。

我们如何衡量那些在广告或出版业失业的人的负面效用与不断提出创新的社会的活力？ 是否存在所有存在的网站和工作应该永远存在的时间点？ 或者再过一年或一个月？

我们如何量化没有广告的积极效用？ 大量快速安装广告拦截器的人可能认为该实用程序非常高。 广告拦截的一些积极效用很难识别和衡量，因为它们来自未来的替代方案，而这些替代方案直到后来才出现。 例如，为了响应有关广告拦截的问题，软件开发人员创建了可以拦截某些广告但允许符合干扰性较低标准的广告的应用程序。 这可能会导致广告商采用新标准来消除最烦人的广告。 因此，我们应该回到上面的广告拦截积极列表并添加广告质量改进

应用 John Rawls 的想法：
在罗尔斯看来，如果一种行为会使处于最不利地位的人的境况变得更糟，那么这种行为就是不合乎道德的。 如果我们放眼全球，最弱势群体不会使用互联网或为出版商或广告商工作。广告拦截器的使用与他们无关，或者几乎无关。如果我们要考虑一个亚群中的弱势群体，我们如何决定是哪一个？ 可能在出版或广告行业失去工作的人并非处于最不利地位； 他们可能受过教育。 如果太多人屏蔽广告，大量以前免费的内容消失或需要付费，使用互联网的低收入人群的境况就会更糟。

做出决定
在第 1 章中，我们还讨论了自然权利、积极权利和消极权利，以及一些思考伦理的其他方法。 我们将这些应用于

广告拦截作为练习。此处的简要分析说明了针对基于长期、间接且通常不可预测的后果的活动制定普遍道德规则的问题。 人和情况之间存在太多差异。 关于动态社会和经济中的后果有太多未知数。 当效果存在如此多的不确定性时，不得出志愿活动不道德的结论似乎是个好主意。这是否有助于您决定是安装广告拦截器还是创建并销售广告拦截器？ 这样做可能不是不道德的，但我们可以评估这些论点并就我们更愿意做什么得出个人结论。 由于我们认为它会产生的影响以及我们希望产生的影响，因此不做道德上可以接受的事情当然没有错。

广告拦截者和发布者的回应

正如我们上面提到的，一些广告拦截器的开发人员为他们不会拦截的可接受广告制定了标准。 其他人向广告商收取费用，以允许他们的广告通过区块。 Firefox 和 Google 的 Chrome 浏览器会阻止 Adobe Flash 广告。 就像互联网内容过滤器（我们将在第 3 章讨论）一样，这些产品可以争夺喜欢其特定政策的用户。 《纽约时报》测试了一条消息，告诉人们广告需要为内容付费。 它发现 40% 的人将他们的广告拦截器设置为允许来自纽约时报的广告。

Facebook 选择不向广告拦截器付费以允许广告通过。 相反，它选择使用技术：它宣布将使用技术使广告拦截器更难在桌面服务（尽管不在移动设备上）上拦截广告。Facebook 阻挠那些安装广告拦截器的人的愿望是错误的吗？ 我们在开始本节时担心屏蔽广告可能是错误的，因为广告为免费内容付费。 脸书是免费的； 广告为此付费。

一些播客应用程序允许用户向前跳过，当然，一些用户可以跳过广告。 据新闻报道，播客公司表示，减少广告跳过的最佳方法是让广告具有娱乐性。这些响应样本表明，技术、市场、教育和创造力在改善在线广告体验方面发挥着重要作用。

2.5.4 保护个人数据的政策

收集和存储个人数据的企业、组织和政府机构有道德责任（在许多情况下有法律责任）保护数据不被滥用，并预测风险并为它们做好准备。 这些团体必须不断更新安全政策以涵盖新技术和新的潜在威胁，雇主必须对携带个人数据的人进行有关风险和适当安全措施的培训。

一个设计良好的敏感信息数据库包括几个防止泄露、入侵和未经授权的员工访问的功能。 每个有权访问系统的人都应该有一个唯一的标识符和密码。 系统可以通过对用户 ID 进行编码来限制用户执行某些操作，例如更改、创建或删除，从而只允许访问特定的信息和操作。 例如，医院的记账员不需要访问患者结果的实验室测试。 计算机系统通过跟踪有关每个数据访问的信息来创建审计跟踪，包括查看记录的人的 ID 和查看或修改特定信息。

审计跟踪可以在以后帮助追踪未经授权的活动，从而阻止许多侵犯隐私的行为。包含消费者信息、Web 活动记录或手机位置数据的数据库是赋予企业竞争优势的宝贵资产，因此此类数据库的所有者有兴趣防止泄露和无限分发。

包含消费者信息、Web 活动记录或手机位置数据的数据库是赋予企业竞争优势的宝贵资产，因此此类数据库的所有者有兴趣防止泄露和无限分发。 这包括为数据提供安全性和开发减少损失的操作模式。 因此，例如，通常不出售邮件列表； 他们是“租来的”。 承租人不会收到地址的副本（电子或其他方式），而是提供要邮寄的材料。 然后由一家专业公司进行邮寄。这降低了未经授权复制给少数公司的风险，这些公司的诚实和安全声誉对其业务很重要。其他应用程序也使用受信任第三方的这种想法来处理机密数据。 例如，汽车租赁公司可以访问第三方服务来检查潜在客户的驾驶记录。 服务查验机动车部门记录和上报相关信息； 汽车租赁公司看不到司机的记录。

网站运营商向进行隐私审计的公司支付数千美元，有时甚至数百万美元。 隐私审计员检查信息泄漏，审查公司的隐私政策及其对该政策的遵守情况，并评估其网站上的警告和解释，以在网站请求敏感数据时提醒访问者，等等。 数百家大型企业设有首席隐私官或合规官职位，负责指导和监督公司隐私政策。 正如美国汽车协会对酒店进行评级一样，各种组织提供认可印章，符合其隐私标准的图标公司可以在网站上发布。

大公司利用其经济影响力来改善消费者隐私。 IBM 和 Microsoft 停止在未发布明确隐私政策的网站上投放广告。 Walt Disney Company 和 InfoSeek Corporation 也做了同样的事情，此外，停止在他们自己的网站上接受来自未发布隐私政策的网站的广告。 直销协会采用了一项政策，要求其成员公司在与其他营销人员共享个人信息时告知消费者，并为人们提供退出选项。 许多公司同意限制敏感消费者信息的可用性，包括未列出的电话号码和有关儿童的所有信息。

当然,还有许多企业没有严格的隐私政策,还有许多企业不遵守自己规定的政策。这里描述的例子代表了一种趋势，而不是隐私乌托邦，并建议负责任的公司可以采取的行动。

2.6 保护隐私：理论、权利和法律

在第 2.3 节中，我们考虑了与隐私保护相关的法律和第四修正案原则的某些方面。 第四修正案保护消极的隐私权（一种自由）免受政府的侵犯和干涉。 本节主要讨论其他人、企业和组织收集或使用的个人数据的权利和法律保护的相关原则。

我们将法律补救措施与技术、管理和市场解决方案分开，因为它们有着根本的不同。 后者是自愿的，种类繁多，不同的人或企业可以从中选择。 另一方面，法律是通过罚款、监禁和其他处罚来执行的； 因此，我们应该更仔细地审查法律依据。 隐私是我们可以处于的状态或状态，例如身体健康或财务安全。 我们应该在多大程度上拥有它的合法权利？ 它仅仅是消极权利还是积极权利（在第 1.4.2 节的意义上）？ 法律应该走多远，市场的自愿相互作用、公共利益团体的教育努力、消费者的选择、责任等等应该留给什么？

2.6.1 隐私权

直到 19 世纪后期，法院在支持社会和商业活动隐私的法律判决中，都基于产权和合同。 不承认独立的隐私权。 1890 年，塞缪尔·沃伦（Samuel Warren）和路易斯·布兰代斯（Louis Brandeis)77（后来成为最高法院法官）发表了一篇名为“隐私权”的重要文章，认为隐私不同于其他权利，需要更多保护。 麻省理工学院哲学家朱迪思·贾维斯·汤姆森（Judith Jarvis Thomson）认为，旧观点更为准确，即在侵犯隐私即侵犯某人权利的所有情况下，侵犯的是与隐私不同的权利。 78 我们提出了一些主张和 这些论文的论点，然后我们考虑有关保护隐私的法律的各种其他想法和观点。

本节的一个目的是展示哲学家、法律学者和经济学家在试图阐明基本原则时进行的各种分析。 另一个是强调原则的重要性，即制定一个理论框架，在这个框架内就特定问题和案例做出决定。

沃伦和布兰代斯：不可侵犯的人格

1890 年 Warren 和 Brandeis 文章的主要批评对象是报纸，尤其是八卦专栏。 沃伦和布兰代斯强烈批评媒体“越界……明显的礼节和体面的界限”。 他们最关心的信息类型是个人信息。外表、陈述和行为以及人际关系（婚姻、家庭和其他）。79 Warren 和 Brandeis 的立场是，人们有权禁止发布关于他们自己的事实和他们自己的照片。 Warren 和 Brandeis 争辩说，例如，如果有人写了一封信说他与妻子发生了激烈的争吵，那么收信人就不能公布该信息。 他们的这一主张基于除隐私外没有任何财产权或其他权利。 这是不受干扰的权利的一部分。 Warren 和 Brandeis 将他们对隐私权的捍卫建立在他们经常引用的短语“人格不受侵犯”的原则之上。

针对其他不法行为的法律——例如诽谤、诽谤、诽谤、侵犯版权、侵犯财产权和违约——可以解决一些侵犯隐私的行为，但沃伦和布兰代斯认为，仍然有许多其他法律没有涵盖的侵犯隐私行为 . 例如，发布个人或商业信息可能构成违反合同（明示或暗示），但在许多情况下，披露信息的人与受害人没有合同。 那么，这个人并没有违反合同，而是侵犯了受害者的隐私。 当有人散布关于我们的虚假和破坏性谣言时，诽谤、诽谤和诽谤法会保护我们，但它们不适用于真实的个人信息，这些信息的曝光会让我们感到不舒服。 沃伦和布兰代斯认为后者应该受到保护。 它们允许发布普遍感兴趣的信息（新闻）、在信息涉及他人利益的有限情况下使用以及口头发布等例外情况。 （他们在广播和电视出现之前就开始写作，因此口头出版意味着受众非常有限。）

Judith Jarvis Thomson：质疑隐私权

朱迪思·贾维斯·汤姆森（Judith Jarvis Thomson）持相反观点。 在检查了几个场景后，她明白了她的观点。

假设您拥有一本杂志。 您的财产权包括拒绝让他人阅读、销毁甚至查看您的杂志的权利。 如果有人对您的杂志做

了您不允许的任何事情，那么那个人就是在侵犯您的财产权。 例如，如果有人使用双筒望远镜从邻近的建筑物看到您的杂志，则该人侵犯了您禁止他人看到它的权利。 该杂志是普通新闻杂志（不是敏感的隐私问题）还是您不希望别人知道您阅读的其他杂志并不重要。 被侵犯的权利是您的财产权。

您可能有意或无意地放弃您的产权。 如果你心不在焉地将杂志留在公园的长椅上，有人可能会拿走它。 如果您在家里有客人时将它放在咖啡桌上，那么有人会看到它。 如果您在公共汽车上阅读色情杂志，有人看到您并告诉其他人您阅读色情杂志，那么该人并没有侵犯您的权利。 此人可能正在做一些不礼貌、不友好或残忍的事情，但不是侵犯权利的事情。

我们对人身和身体的权利包括决定向谁展示我们身体各个部位的权利。 通过在公共场合走来走去，我们大多数人都放弃了不让别人看到我们脸的权利。 当一名穆斯林妇女遮住脸时，她是在行使不让别人看到的权利。 如果有人在家里用望远镜偷看我们洗澡，那他们就是在侵犯我们的人身权。

如果有人为了获取一些信息而殴打您，那么殴打者就是在侵犯您免受人身攻击的权利。 如果信息是一天中的时间，则隐私不成问题。 如果信息比较私密，那么打者就侵犯了你的隐私，但侵犯的权利是你不受攻击的权利。 另一方面，如果一个人和平地询问你和谁住在一起或者你的政治观点是什么，那么这个人没有侵犯任何权利。 如果您选择回答并且不签订保密协议，那么此人不会通过向其他人重复信息来侵犯您的权利，尽管这样做可能是不考虑他人的。但是，如果此人同意不重复该信息，但后来又重复了，则该信息是否敏感都无关紧要； 此人违反保密协议。

在这些例子中，如果不侵犯某些其他权利，例如控制我们的财产或人身的权利、免受暴力攻击的权利或订立合同的权利（并期望它们得到执行），就不会侵犯隐私 ）. Thomson 总结道，“我认为，在任何据称侵犯隐私权的情况下，询问该行为是否属于侵犯任何其他权利，如果不是，该行为是否真的侵犯了权利。”80
对沃伦和布兰代斯以及汤姆森的批评 Warren 和 Brandeis 立场的批评者 81 认为，他们的隐私概念过于宽泛，无法提供可行的原则或定义来得出侵犯隐私权的结论。 他们对隐私的看法与新闻自由相冲突，似乎几乎任何未经授权的提及某人的行为都侵犯了该人的权利。

汤姆森的批评者提出了侵犯隐私权（不仅仅是对隐私的渴望）的例子，但没有侵犯其他权利。 有些人认为汤姆森关于我们人身权的概念含糊不清或过于宽泛。 她的例子可能（也可能不会）成为考虑其他权利可以解决隐私问题这一论点的令人信服的论据，但没有有限数量的例子可以证明这样的论点。

两篇文章都没有直接反驳另一篇。 他们的侧重点不同。 Warren 和 Brandeis 专注于信息的使用（发布）。 汤姆森专注于它是如何获得的。

应用理论
理论论证如何适用于当今的隐私和个人数据？在整个沃伦和布兰代斯，令人反感的行为是公开个人信息——其广泛、公开的分发。 自从他们的文章出现以来，许多法院的判决都被采纳了这种观点。82 如果有人公布了你看过的所有电影的列表（以印刷形式或通过在网络上公开），那将违反沃伦和布兰代斯的隐私概念。 如果有人公布了他或她的消费者资料，一个人可能会赢得官司。 但在当前消费者数据库、Web 活动监控、位置跟踪等方面，有意发布并不是主要关注点。 如今收集的个人信息数量之多可能会让沃伦和布兰代斯感到震惊，但他们的文章允许向对此感兴趣的人披露个人信息。 言下之意，他们并不排除向汽车租赁公司披露个人的驾驶记录，而该人想从中租车。 同样，Warren 和 Brandeis 似乎也不反对向某人试图购买保险的人寿保险公司披露有关某人是否吸烟的信息。 他们的观点不排除使用（未发布的）消费者信息进行有针对性的营销，尽管他可能不会赞成社交网络的内容可能也会让沃伦和布兰代斯感到震惊和震惊。 他们的立场将严格限制包含其他人以及朋友的位置和活动的照片的共享。

Warren 和 Brandeis 论文以及 Thomson 论文的一个重要方面是同意。 如果一个人同意收集和使用信息，他们认为不会侵犯隐私。

交易

我们还有另一个难题需要考虑：如何将隐私的哲学和法律概念应用于自动涉及多个人的交易。 下面的场景将说明这个问题。

一天，在 Friendlyville 的小农场社区，乔从玛丽亚那里买了五磅土豆，玛丽亚将这五磅土豆卖给他。 （我们以这种重复的方式描述交易，以强调交易涉及两个人和双方。）

Joe 或 Maria 可能希望交易保密。 他自己的马铃薯作物歉收可能会让乔难堪。 或者 Joe 在 Friendlyville 可能不受欢迎，Maria 担心镇民会因为她卖给他而生气。 无论哪种方式，如果 Maria 或 Joe 向镇上的其他人谈论购买或出售土豆，我们都不太可能认为这是对对方权利的侵犯。 但假设乔要求保密作为交易的一部分。 玛丽亚有三个选择：

1. 她可以同意。
2. 她可以说不； 她可能想告诉别人她把土豆卖给了乔。
3. 如果乔支付更高的价格，她可以同意对交易保密。

在后两种情况下，乔可以决定是否购买土豆。 另一方面，如果 Maria 要求保密作为交易的一部分，Joe 有三个选择：

1. 他可以同意。
2. 他可以说不； 他可能想告诉别人他从玛丽亚那里买了土豆。
3. 如果 Maria 收取更低的价格，他可以同意对购买保密。

在后两种情况下，玛丽亚可以决定是否出售土豆。

隐私包括对自己信息的控制。 交易是关于 Maria 的事实还是关于 Joe 的事实？ 似乎没有令人信服的理由证明任何一方比另一方拥有更多的权利来控制有关交易的信息。 然而，这个问题对于有关使用消费者信息的法律政策决定至关重要。如果我们要将对交易信息的控制权分配给其中一方，我们需要一个坚实的哲学基础来选择哪一方获得它。（如果双方订立了保密协议，那么他们就有遵守保密协议的道德义务。如果协议是合法的合同，那么他们就有尊重它的法律义务。）

哲学家和经济学家经常使用简单的两人交易或关系，例如 Maria-Joe 情景，试图阐明问题中涉及的原则。 关于 Maria 和 Joe 的观察和结论是否适用于复杂的大型社会和全球经济，其中交易的一方通常是企业？ 所有交易实际上都是人与人之间的，即使是间接的。 因此，如果交易信息中的财产权或隐私权属于其中一方，我们需要一个论证来说明现代经济中的交易与 Friendlyville 中的交易有何不同。 在本节后面，我们将描述两种关于消费者交易信息监管的观点：自由市场观点和消费者保护观点。 消费者保护观点建议区别对待各方。

个人数据的所有权

一些经济学家、法律学者和隐私倡导者建议赋予人们对自己信息的财产权。 财产权的概念即使适用于无形财产（例如知识产权）也很有用，但将此概念用于个人信息时存在问题。 首先，正如我们刚刚看到的，活动和交易通常涉及至少两个人，每个人都有合理但相互冲突的权利要求来拥有有关交易的信息。 一些个人信息似乎与交易无关，但在

分配所有权时仍然存在问题。 你拥有你的生日吗？ 或者你妈妈拥有它？ 毕竟，她是活动中更积极的参与者。

分配个人信息所有权的第二个问题来自拥有事实的概念。 （版权保护计算机程序和音乐等知识产权，但我们不能保护事实。）事实的所有权会严重损害社会中的信息流动。 我们将信息存储在电子设备上，但我们也将其存储在我们的脑海中。 我们能否在不侵犯他人的思想自由和言论自由的情况下拥有关于我们自己的事实？

尽管分配个别事实的所有权存在困难，但另一个问题是我们可以拥有我们的“个人资料”，即描述我们的活动、购买、兴趣等的数据集合。 我们不能承认我们的眼睛是蓝色的这一事实，但我们确实有合法权利控制对我们摄影图像的某些使用。 在几乎所有州，我们都需要一个人的同意才能将他或她的形象用于商业目的。 法律应该以同样的方式对待我们的消费者资料吗？ 法律是否应该以同样的方式对待我们收集的搜索查询，因为它们可能被用来识别我们的身份？ 我们如何区分关于一个人的一些事实和“个人资料”？

理查德波斯纳法官：信息产权的经济论据

理查德波斯纳法官，一位广泛研究法律与法律之间相互作用的法律学者。经济学，给出了关于如何分配信息产权的经济论据。83 他指出，信息具有经济价值和个人价值。 确定企业、客户、客户、雇主或雇员是否可靠、诚实等对我们很有价值。 个人和业务往来有很多机会进行虚假陈述，从而剥削他人。 波斯纳的分析得出的结论是，在某些情况下，个人或组织应该拥有信息财产权，而在其他情况下，他们不应该拥有。 也就是说，一些信息应该在公共领域。

如果信息对社会有价值并且发现、创建或收集的成本很高，则信息产权是合适的。 没有对此类信息的产权，投资于发现或收集信息的个人或企业将不会从中获利。 结果是人们会产生更少的此类信息，从而损害社会。 因此，法律应该保护，例如，商业秘密，这是企业大量支出和努力的结果。 第二个例子是个人信息，例如一个人的裸体外观。一个人获得它并不昂贵，但实际上我们所有人都重视保护它，而隐瞒对社会来说并不昂贵。 因此，将此信息的产权分配给个人是有意义的。

一些隐私倡导者希望保护可能导致拒绝工作或拒绝某种服务或合同（例如贷款）的信息。 他们提倡限制共享可能有助于对人们做出负面决定的信息——例如，房东共享一个包含租户付款历史信息的数据库。 波斯纳认为，一个人不应该对负面的个人信息或其他信息的财产权，这些信息的隐藏有助于人们进行虚假陈述、欺诈或操纵。 此类信息应属于公共领域。 这意味着一个人不应该有权禁止他人收集、使用和传播它，只要他们不违反合同或保密协议并且不通过窃听私人通信或其他方式获取信息或者其它任何禁止手段。

近几十年来，立法的趋势并没有遵循波斯纳的立场。 波斯纳观点的一些批评者认为，道德理论，而不是经济原则，应该是产权的来源。

2.6.2 法律法规

一个基本的法律框架

定义和执行合法权利和责任的良好基本法律框架对于复杂、强大的社会和经济至关重要。 它的任务之一是执行协议和合同。 合同——包括订立合同的自由和法律制度对其条款的执行——是一种实施灵活多样的经济交易的机制，这些交易随着时间的推移发生在彼此不了解或根本不了解彼此的人之间。

我们可以将合同执行的理念应用到企业和组织公布的隐私政策中。 例如，Toysmart 是一家基于网络的益智玩具销售商，它收集了大约 250,000 名访问其网站的访问者的大量信息，包括家庭概况、购物偏好以及儿童的姓名和年龄。 Toysmart 曾承诺不会泄露这些个人信息。 尽管如此，当公司申请破产时，它背负着巨额债务，几乎没有任何资产——除了价值很高的客户数据库。 Toysmart 的债权人希望出售数据库以筹集资金偿还债务，因此 Toysmart 提出

出售数据库，引起了抗议风暴。 与 Toysmart 的保单是与数据库中的人签订的合同的解释一致，破产法庭的和解协议包括销毁数据库。

法律系统的第二个任务是为合同未明确涵盖的情况设定默认值。 假设一个网站没有发布关于它如何处理它收集的信息的政策。 网站运营商对信息应享有哪些合法权利？ 许多网站和线下企业表现得好像默认是他们可以做任何他们选择的事情。 一个强大的隐私保护默认设置是他们只能将信息用于他们收集信息的直接和明显的目的。 法律体系可以（并且确实）为传统上和大多数人认为是隐私的敏感信息（例如医疗和财务信息）设置特殊的保密默认值。 如果企业或组织想要将信息用于默认之外的目的，则必须在其政策、协议或合同中指定这些用途，或者请求同意。 许多业务往来没有书面合同，因此法律规定的默认条款会产生很大影响。

基本法律结构的第三项任务是规定对刑事犯罪和违约行为的处罚。 因此，法律可以规定对违反隐私政策和疏忽丢失或披露企业和其他人持有的个人数据的处罚。 责任法的制定者必须在过于严格和过于宽松之间取得平衡。 如果过于严格，它们会使一些有价值的产品和服务变得过于昂贵而无法提供。 如果太弱，它们将不足以激励企业和政府机构为我们的个人数据提供合理的安全保护。

规定
隐私保护的技术工具、市场机制和商业政策并不完善。 这是监管法律的有力论据吗？ 监管也不完善。 我们必须通过考虑有效性、成本和收益以及副作用来评估监管解决方案，就像我们评估其他类型的技术引起的问题的潜在解决方案一样。 我们在此简要说明几点。 有数百种隐私法。 当国会通过隐私等复杂领域的法律时，法律通常会规定总体目标，而将细节留给政府机构，由政府机构编写成百上千页的法规，有时长达数年。 复杂的情况很难制定出合理的规定，因此法律法规往往会产生意想不到的效果或解释。 有时会在没有意义或人们根本不想要它们的地方应用法规。

儿童在线隐私保护法 (COPPA) 说明了意外后果的问题。 COPPA 要求网站在收集 13 岁以下儿童的个人信息之前必须获得父母的许可——这是一个非常合理的想法。 COPPA 通过后，由于遵守其要求的费用和潜在的责任，一些公司删除了所有 13 岁以下儿童的在线资料，一些公司取消了他们的免费电子邮件和儿童主页，一些公司完全禁止 13 岁以下儿童。 Facebook 的使用条款禁止 13 岁以下的儿童加入，但《消费者报告》估计有数百万 13 岁以下的儿童无视该规定加入。 没有 13 岁以下成员的虚构意味着没有必要提供保护他们的机制。

监管通常会产生高昂成本，既有企业（以及最终消费者）的直接美元成本，也有隐性或意外成本，例如服务损失或增加的不便。 例如，禁止广泛同意协议，而是要求对个人信息的每次二次使用明确同意的法规具有经济学家称之为“高交易成本”的属性。 同意要求可能非常昂贵且难以实施，以至于它消除了大多数信息的二次使用，包括那些消费者认为合意的信息。

2.6.3 对比观点

当被问及“如果有人起诉你败诉了，他们是否需要支付你的法律费用？” 超过 80% 的受访者表示“是”。 当从相反的角度问同样的问题时：“如果你起诉某人败诉了，你是否应该支付他们的法律费用？” 大约 40% 的人说“是”。

许多撰写关于隐私的学者和倡导者的政治、哲学和经济观点各不相同。 因此，他们对各种隐私问题的解释和解决方案的方法往往不同，尤其是当他们考虑法律法规来控制企业收集和使用个人信息时。*我们对比两种观点。 我们称它们为自由市场观和消费者保护观。

自由市场观

倾向于以市场为导向解决隐私问题的人倾向于强调::

- *作为消费者或企业的个人订立自愿协议的自由； 个人品味和价值观的多样性；*
- *技术和市场解决方案的灵活性；*
- *市场对消费者偏好的反应；*
- *合同的有用性和重要性；*

以市场为导向的解决方案倡导者强调许多志愿组织提供消费者教育、制定指导方针、监督企业和政府的活动，并迫使企业改进政策。 这些倡导者可能采取强烈的道德立场，但强调道德的作用与法律的作用之间的区别。

收集和使用个人信息的自由市场观点强调知情同意：收集个人数据的组织（包括政府机构和企业）应明确告知提供信息的人他们是否会保密（来自其他企业、个人和政府） 机构）以及他们将如何使用它。 这些组织应对违反其既定政策的行为承担法律责任。 这种观点可以将不可见的信息收集视为盗窃或入侵。

自由市场观点强调契约自由：人们应根据自己的判断自由签订协议（或不签订协议）披露个人信息以换取费用、服务或其他利益。 企业应该可以自由提供此类协议。 这种观点尊重消费者根据自己的价值观为自己做出选择的权利和能力。 市场支持者期望消费者承担与自由相伴的责任——例如，阅读合同或了解理想的服务是有成本的。 自由市场观点包括信息的自由流动：法律不应阻止人们（或企业和组织）在不侵犯权利（例如，不盗窃、侵入或违反合同义务）的情况下使用和披露他们独立或非侵入性发现的事实。

我们不能总是期望在任何产品、服务或工作中都能准确地获得我们想要的属性组合。 正如我们可能无法在每家比萨餐厅都买到无奶酪比萨或找到一辆具有我们想要的确切功能的汽车一样，我们可能并不总是能够同时获得隐私和特别折扣或免费服务。 如果不同意向雇主提供某些个人信息，我们可能无法在没有广告的情况下获得某些网站，或无法获得特定的工作。 在与他人互动时，这些妥协并不罕见或不合理。

出于多种原因，市场支持者倾向于避免限制性立法和详细监管。 过于宽泛、设计不当和模糊的法规扼杀了创新。 在权衡和成本的现实世界中，政治制度是一个比市场更糟糕的制度来决定消费者想要什么。 立法者不可能事先知道人们愿意用多少金钱、便利或其他利益来换取更多或更少的隐私。 随着时间的推移，企业会对数百万消费者通过购买表达的偏好做出反应。 针对很多人表达的对隐私的渴望，市场上提供了各种各样的隐私保护工具。 市场支持者认为，要求特定政策或禁止某些类型合同的法律侵犯了消费者和企业主的选择自由。

这种观点包括对窃取数据者和违反保密协议者的法律制裁。 它要求企业、组织和政府机构对由于安全措施不当或疏忽而导致的个人数据丢失负责。 为了鼓励创新和改进，这种观点的倡导者更倾向于在公司丢失、不当披露或滥用数据时进行处罚，而不是规定个人信息持有者必须遵守的详细程序。

自由市场观点认为隐私是一种“好”，既是因为它是可取的，也是我们可以通过购买或交易在经济中获得不同数量的东西，比如食物、娱乐和安全。 正如有些人选择用一些安全换取刺激（蹦极、骑摩托车）、金钱（购买便宜但安全性较低的产品）或便利，有些人选择不同程度的隐私。 至于安全，法律可以提供最低标准，但它应该允许市场提供广泛的选择以满足个人偏好的范围。

消费者保护观点

强有力的隐私监管的倡导者强调我们在本章中提到的个人信息的令人不安的使用，数据库错误的代价高昂和破坏性的结果，以及个人信息因丢失、被盗和粗心大意而泄露的难易程度。 他们主张更严格的同意要求，对消费者的法律限制分析、禁止某些类型的合同或协议披露数据，以及禁止企业收集 ｏｒ 存储某些类型的数据。 例如，他们敦促法律要求公司对个人信息的二次使用制定选择加入政策，因为对于喜欢它的消费者来说，选择退出选项可能不够明

显或不够容易。 消费者保护观点将禁止对二次使用的弃权和广泛的同意协议。

这种观点的重点是保护消费者免受企业的滥用和粗心大意，以及他们自己缺乏知识、判断力或兴趣。 消费者保护观点的倡导者强调，人们没有意识到其他人可能使用他们的信息的所有方式，也不了解同意披露个人数据的风险。 那些强调消费者保护的人对以免费设备和服务换取个人信息或同意监控或跟踪的计划持批评态度。其中许多倡导者支持禁止收集或存储个人数据的法律，在倡导者认为风险比信息对想要收集数据的企业的价值更重要的情况下，这些数据可能会产生负面影响。消费者倡导者和隐私“绝对主义者”玛丽加德纳琼斯反对消费者同意传播个人数据的想法。 20 多年前，她说：“你不能指望一个忙于谋生的普通消费者坐下来理解同意的含义。 他们不明白使用他们的数据对他们意味着什么。” 现在理解数据收集和使用方式的含义更加困难。 美国公民自由联盟隐私和技术项目前主任表示，知情同意不足以提供充分保护。 她敦促研究健康记录保密性的参议院委员会“重新审视传统上对个人同意的依赖，将其作为隐私法的关键。”

那些强调消费者保护观点的人会争辩说，第 2.6.1 节中描述的 Friendlyville 的 Joe-Maria 情景与复杂的社会无关。 个人与大公司之间的权力不平衡是原因之一。 另一个是，在 Friendlyville，有关交易的信息只流传给乔和玛丽亚认识的一小部分人。 如果有人得出不准确或不公平的结论，乔或玛丽亚可以与此人交谈并提出他或她的解释。 在更大的社会中，信息在许多陌生人之间传播，我们常常不知道谁拥有这些信息，也不知道他们根据这些信息对我们做出了什么决定。

大多数消费者无法与企业实际协商合同条款。 在任何特定时间，消费者只能接受或拒绝商家提供的东西，而拒绝商家的条款就意味着得不到想要的产品或服务。 如果我们想为房子或汽车贷款，我们必须接受贷款人目前提供的任何条件。 如果我们需要一份工作，由于工作的经济必要性，我们可能会同意披露个人信息而不是我们的真实偏好。 个人对提供搜索引擎的大公司没有任何有意义的权力，例如，无论他们是否知道或接受公司关于使用他们的搜索查询的政策。

在消费者保护看来，商家自律是行不通的。 企业隐私政策薄弱、模糊或难以理解，企业有时不遵守其规定的政策。消费者施压有时是有效的，但有些企业却视而不见。 相反，我们必须要求所有企业采用保护隐私的政策。 为消费者提供的软件和其他技术隐私保护工具需要花钱，而且很多人买不起。 无论如何，这些工具远非完美，因此不足以保护隐私。

消费者保护观点将隐私视为一种权利，而不是我们讨价还价的东西。 例如，电子隐私信息中心和 Privacy International 联合主办的网站闪现“隐私是一种权利，而不是偏好”和“通知是不够的”88 后者表明他们将隐私视为一种积极的权利， 或索赔权（在第 1.4.2 节的术语中）作为一种消极权利，隐私允许我们使用匿名技术并避免与那些请求我们不希望提供的信息的人互动。 作为一项积极的权利，这意味着我们可以阻止他人谈论我们。民主与技术中心的一位发言人在给国会的一份声明中表达了这一观点，他说我们必须将这样的原则纳入法律，即人们应该能够“自行决定何时、如何以及在多大程度上共享他们的信息 ”

2.7 欧盟隐私法规

欧盟（EU）有一项全面的数据保护指令（1995 年通过）。90* 它涵盖了个人数据的处理，包括收集、使用、存储、检索、传输、销毁和其他行为。 该指令规定了欧盟成员国必须在其本国法律中实施的公平信息原则。 有几个类似于图 2.1 中的前五个原则。 欧盟有一些额外的或更严格的规则。 仅当个人明确同意或处理是履行合同或法律义务所必需的，或公共利益的任务或官方机构完成任务（或其他一些原因）所必需时，才允许处理数据。 未经个人明确同意，不得处理特殊类别的数据，包括民族和种族出身、政治和宗教信仰、健康和性生活以及工会会员身份。 即使当事人同意，成员国也可能禁止处理此类数据。 有关刑事定罪的数据处理受到严格限制。

*更新版《通用数据保护条例》预计将于 2018 年生效。

这些例子说明了欧盟和一些成员国更严格的规则和法律。

- 谷歌在 2012 年修改了其隐私政策，允许该公司整合其从各种服务中收集的会员信息。 欧盟辩称，普通用户无法理解如何谷歌根据新政策使用他们的数据，这违反了欧盟的隐私法规。
- 德国一家法院表示，Facebook 在其会员协议中的某些政策（例如，授予 Facebook 使用会员在 Facebook 上发布或存储的材料的许可）在那里是非法的。
- 德国政府要求 Facebook 停止对德国用户运行人脸识别应用程序； 它违反了德国隐私法。
- 由于严格的隐私法，谷歌已经关闭或不再更新一些欧洲国家的街景。
- 欧盟为社交网站制定了法律指南，建议网站应在较高级别设置默认隐私设置，允许使用假名，限制他们保留不活跃用户数据的时间，并删除长时间不活跃的帐户告诉用户，只有在该人同意上传照片时才能上传该人的照片

虽然欧盟对私营部门收集和使用个人信息的规定比美国严格得多，但一些公民自由主义者认为，这些规定没有提供足够的保护，防止政府机构使用个人数据。 尽管该指令规定数据的保存时间不应超过必要的时间，但欧洲国家/地区要求 ISP 和电话公司将客户通信记录（日期、目的地、持续时间等）保留最多两年，并将其提供给执法部门 机构。 欧盟表示需要这一要求来打击恐怖主义和有组织的犯罪。

欧盟严格的隐私指令并不能阻止发生在美国的一些相同的个人数据滥用行为。 例如，在英国，信息专员报告说，数据经纪人利用欺诈和腐败的内部人员来获取个人信息。 与美国一样，非法数据服务的客户包括记者、私家侦探、收债员、政府机构、跟踪者和寻求数据用于欺诈的罪犯。

欧盟数据隐私指令禁止将个人数据传输到欧盟以外的国家，这些国家不具备其认为的充分的隐私保护系统。 该指令的这一部分给在欧洲内外开展业务的公司带来了重大问题。 数以千计的国际公司在美国的服务器上处理和/或存储欧洲客户、员工或成员的数据。 价值数十亿美元的跨境业务处于危险之中。 欧盟制定了一项安全港计划，根据该计划，遵守一系列类似于数据保护指令原则的隐私要求的欧盟以外的公司可以从欧盟接收个人数据。 在披露美国国家安全局广泛监视和收集私人数据系统后，欧盟法院终止了安全港计划，并于 2016 年用一项名为“隐私盾”的新计划取而代之，该计划具有更严格的规定。

许多隐私倡导者将美国的隐私政策描述为“落后于欧洲”，因为尽管美国有涵盖医疗信息、视频租赁、驾照记录等特定领域的隐私法，但它没有全面的联邦立法来规范个人数据 各个领域的收集和使用。 这是由美国和欧洲不同的文化和传统造成的。 例如，欧洲国家往往更强调声誉的法律保护，而美国宪法则非常重视言论自由。 一般来说，欧洲更强调监管和集中化，尤其是在商业方面，而美国传统上更强调合同、消费者压力、市场灵活性以及对执法滥用行为的惩罚，例如针对欺诈和不公平商业行为的执法。

欧盟被遗忘的权利

在一个西班牙男子起诉要求谷歌删除显示在搜索结果中的某些文件的链接的案件中，欧盟法院于 2014 年裁定数据保护指令包括“被遗忘的权利”： person 可以要求搜索引擎公司阻止某些类型信息的链接出现在某些搜索结果中（例如，搜索此人的姓名）。 具有足够公共利益的信息除外。 标准和例外是模糊和主观的。 在裁决后的第一年，谷歌收到了删除近一百万个链接的请求，并批准了大约 35%。（如果请求被拒绝，一个人可以向政府机构提出上诉。）处理这些请求的谷歌咨询委员会表示，许多案件很容易（例如，某些涉及儿童的项目或未经个人许可发布的半裸照片） ，但有些极难决定。 被遗忘权可以产生连锁效应：一家报纸报道了一个案例，其中谷歌同意删除指向该报发表文章的链接的请求。 提出最初请求的人随后请求删除讨论第一次删除的文章的链接。

起初，当谷歌应欧洲的请求屏蔽链接时，它只屏蔽来自欧洲版本的搜索引擎，而不是来自 google.com。 法国政府命令谷歌不仅要阻止在 google.fr 上的搜索，还要阻止在欧洲人可以使用的 google.com 上的搜索。 在 google.com 上屏蔽将强制欧盟公民在世界范围内被遗忘的权利，在不承认这种权利的国家。 谷歌通过阻止其所有全球搜索引擎上的链接而妥协，但仅限于来自请求阻止的人所在国家/地区的搜索。 因此，例如，美国或德国的人仍然可以使用 google.com 查找有关在法国被封锁的法国人的信息。 法国监管机构拒绝了这一妥协，继续坚持要求谷歌在全球范围内屏蔽这些链接。

对言论自由、政治自由和民主没有强有力保护的政府经常使用自由国家的审查法作为他们自己的一些借口。 俄罗斯援引欧盟的先例，通过了一项关于被遗忘权的法律，但它缺乏关键的保障措施，包括某些涉及公共利益或公众人物信息的例外情况。 欧盟正致力于将其被遗忘权应用于数据库和网络搜索以外的其他领域。