人”一词同时还意味着“与‘众’不同”，也就是说个人的事物为个人所有，与其他公众所有的事物相区分。此外，“众”不足以描述信息性隐私权制度的预期特性。在我们的法律体系中，无主物被推定可以归属于任何人，一旦有人取得了该无主物，此人就获得了该无主物的所有权。信息性隐私权的拥护者则反其道而行，他们主张法律必须保障个人对其私人信息的控制。我们无法用语言描述，在没有法定所有权或实际所有权的情况下，人们如何对事物加以控制，也就是说，我们无法描述出一项既不为公众所有，也不为个人所有的事物。

我们注意到，学者往往将隐私权放在所有权理论的背景下进行讨论，这种做法显然回避了隐私权与所有权之间的实际关系。一些哲学家认为，隐私权只有在被归结为财产利益时才具有意义。也许事实确实如此，但这也是由于所有权理论将其自身的认知结构强加于社会现实所造成的。由于人们惯于对客体的所有权进行分析，因此，一旦人们将个人身份信息视为与其自身相分离的客体，所有权分析就会自然而然地紧随其后。然而，与此同时，由于所有权讨论排斥对其他特性的分析，因此人们会越来越难以看到信息具有的其他特性。如此一来，所有权理论就成为我们描述与判断社会现实经验的主要依据。

如果我们不将个人身份信息视为一项“事物”，不将其视为所有权的客体，那么，我们应该如何对其进行分析呢？对于一般性的隐私权或特殊性的信息性隐私权而言，又存在哪些概念上的差别？哲学家与法学学者用了数十年的时间才为隐私权提出了一个引人注目的定义，将之定义为一种人身利益或人格利益。与所有权理论相比，隐私权理论显得较为模糊不清；在所有权理论中，事物之间的界限是十分清晰明了的，而在隐私权理论中，人们很难弄清人格尊严的界限为何。因此，讨论所有权的第三个原因是，尽管所有权理论可能会将隐私权问题过分简单化，但是它能够较为清晰地反映出隐私权的界限。

一种观点认为隐私权的意义仅仅在于确定财产利益的分配，另一种观点认为，隐私权所涉及的问题并不仅限于所有权范畴，还涉及其他因素。上述两种观点之中，哪一种是正确的呢？将隐私权置于极具诱惑力的所有权语境下进行讨论，是否就能够为信息性隐私权之争分出胜负？换句话说，进行所有权分析的风险有多大？要回答以上这些问题，我们必须先对“所有权”的含义进行充分的探究。

文的第六部分将探索一种能够为上述不同理解所支持的信息性隐私权理论，笔者将首先讨论个人实现自主决策，主张自我权利所必需的发育条件。

## 六、发展：动态的信息性隐私权理论

习惯上，我们在判断个人身份信息交易是否合法时，总会将其与是否侵害个人自由联系起来。但是，本文的讨论已经表明，在长期实践检验中，如果个人本身就是享有隐私权的主体，此时再讨论涉及个人隐私的交易是否侵害个人自由无疑是非常肤浅的。用华丽的辞藻对个人自由大加修饰的做法掩盖了这样一个事实，即从一个更为基础的角度来看，信息性隐私权讨论主要围绕他人的自治权而展开，信息处理商依据其作为信息所有者、信息交易者、信息出卖者、信息传播者以及信息选择者的权利将他人客体化。如果我们真的希望从实际上与理论上进一步促进个人自由的发展，那么，前述现象的出现不得不说是一个很古怪的结果。

因此，为了改变这种古怪的结果，我们真正需要的是一套动态的信息性隐私权理论，并将注意力集中于实现事实上的信息自治所需具备的条件。该套理论的形成必须以充分权衡各种利弊为基础。本部分将分析以自治权为基础的信息性隐私权保护制度的理论基础与实践基础，并主张社会在运用上述信息性隐私权保护方法时，不应对有利于公众获取信息的一系列重要的社会及政治利益造成破坏。

### （一）信息性隐私权的价值

现行信息性隐私权政策是以市场为基础制定的。该制度通过赋予隐私权市场交易价值或者提高对行为人的信息披露要求对他人隐私权进行保护，这种隐私权保护制度完全以个人喜好为基础，好比按个人喜好决定黑色皮鞋比棕色皮鞋好看或是红酒比白酒好喝一样不严谨。但是，信息性隐私权却具有极为重要的基础性价值。赋予他人一定程度的免受审查与免受其他人分类拣选的自由，对个人与集体都具有十分重要的非工具性价值。

信息自治与公平公正地对待社会中的每一个人具有同等重要的价

值。从 Kant 到 Rawls，他们都主张尊重每个人的基本尊严并在法律原则与社会实践中平等地对待每个人，这也是西方社会核心的哲学传统。[①] 主张对信息性隐私权给予强力保护的观点认为，上述原则清晰而具体地指出了应当如何对待个人隐私信息：该观点的支持者认为，我们应该禁止信息处理行为，这种行为把人类视为可交易信息的集合，并且根据人们经济上或基因上的有利条件，将他人划分为潜在客户、出租人、邻居、雇员或保险客户等。《欧洲数据保护指令》的起草者对人们渴望获取信息的特点极为赞同，该指令明确规定："本指令基于天赋之人权与自由而制定。"[②]

但是，从规范优先原则向欧盟的公平信息实践模式的跨越，却有待进一步的解释。至少从理论上讲，即便是基于市场基础而形成的可交易的信息性隐私权制度，也是与保证个人尊严与平等的首要规范性要求相一致的，它将每一个人都视为自治且理性的行为人，并假设每一个人都平等地享有认识与追求个人最大程度幸福的权利。但是实际上，正如上文第三部分以及第四部分所述，与前述理性行为人假设存在出入的是，个人在信息处理实践中只享有较少的选择权与自治权。而存在这样出入的原因就在于，理性行为人的假设无法告诉个人如何在事实上获取信息自治权——这正是有待于我们提高与完善的地方。

使个人享有信息自治权的过程不是一蹴而就的。我们必须对信息处理过程进行深入了解，并且就当前的信息化世界得出自身的结论。我们必须学会如何选择，但在这之前，我们必须首先对某些事情进行深入了解。信息理论中存在这样一个悖论："自治"意味着与某些关键机构完全脱离并完全不受外界的任何影响。但是从信息塑造行为的角度来讲，能否实现自治本质上取决于周边的环境。如果我们能够保证"自治"不会在商人的影响下堕落成一种简单的、纯粹受经济利

---

① See Immanuel Kant, The Metaphysics of Morals 73 – 74, 231 – 232 (Mary Gregor ed. & trans., Cambridge Univ. Press 1996) (1797); John Rawls, A Theory of Justice (rev. ed. 1999).

② See Council Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O. L (L. 281) 31, at art. 1 (1).

行区别讨论。初次销售原则的制定初衷在于，由于创造性作品的广泛传播具有重大的社会意义，并且有形商品是可以自由转让的，因此社会利益高于作者收取初次销售以外的额外报酬的利益。相比之下，对个人身份信息使用的持续限制有利于保护个人的人格尊严利益与自治权益，自由传播信息的社会利益无法凌驾于上述利益。相反，正如本文第六部分第（一）点所指出的，社会利益与个人利益实际上是基本统一的。

有人可能会反驳，这些规定对同意的界定太过严苛，这会导致个人没有选择让与信息性隐私权的余地。然而，这一观点实际上犯了本文第三部分所讨论的概念范畴上的错误，忽略了选择权的制度性参数。社会必须对有效同意的构成条件作出界定，这也是合同法的意义所在。毫无疑问，信息性隐私权规定会对个人身份信息所涉及的集体决策产生影响，因此我们必须对同意的成立条件进行严格的界定。如果信息性隐私权是实现个人自我决定与集体自我管理的一项基本要求，那么，这类“强制”就是必不可少的，何况这种规定根本算不上是一种强制。

最后，为了确保信息实践的公平，有效的信息性隐私权立法还必须对同意以外的其他事项作出规定。认为单凭知情同意制度就足以保护他人在个人身份信息使用过程中的利益的观点，是非常美国式的观点。国际社会一致认同的公平信息实践原则为他人提供了许多实质性与程序性的其他方面的保护。公平信息实践原则尤其关注信息处理过程中的透明度问题、信息收集过程中的审查问题、他人使用自己的个人身份信息的问题、纠正不准确信息的机会，以及信息处理商的法律责任。[①] 这些规定通过一些简单有效的程序敦促销售商履行双方订立的合同条款，遵守公平竞争的基础标准，从而从理论上与事实上确保信息处理商对个人承担相应的法律责任。

责任不仅包括集体责任，还包括个人责任。正如本文第四部分第

---

① See Council Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O. L (L. 281) 31, at Arts. 10 - 21; Guidelines Governing die Protection of Privacy and Transborder Flows of Personal Data, OECD Doe. C (80) 58 (Final) (1980).

但是，我们同样可以通过帮助销售商了解消费者整体的渴望与偏好，设计出一种能够使信息免受侵扰的信息系统。我们还可以设计一种帮助消费者寻找销售商的信息系统，在保留代理中介的同时保障消费者的选择权。

最后，我们必须认识到，想要实现有意义的自主选择必须靠技术上与法律上的共同努力。但是，法律至少可以并且应当监理一套全新的制度参数，从而激励隐私权保护技术的进步。仅凭法律不足以实现信息性隐私权的建立与完善，但是，法律的确是实现上述目标的起点。

学者的推崇，并且在最近的联邦政策建议中被反复提及。该方案主张建立个人信息交易市场，该交易市场与其他普通货物交易市场无异，在该市场中，个人信息应当被明码标价并被有效分配。这一市场化方案有很多吸引人的地方，但是仅就现有概念分析，这一方案是非常不完整、不成熟的。该方案未能解决当交易各方的隐私权合同约定不明确时，适用什么兜底规则来处理个人信息的流通问题。无论是从效率的角度还是从社会公益的角度，笔者均认为应该将以下规则作为兜底规则适用——当合同约定不明确时，仅允许具有“功能性的必要性”（functionally necessary）的个人信息进行流通，除非信息所有人明确表示同意信息流通。第四部分将学术争论与实务中的政策制定相结合，呼吁美国国会制定《网络空间隐私权法》（Cyberspace Privacy Act），用以调整美国网络交易过程中网络空间记录并生成的个人信息隐私权的保护问题。

笔者的研究存在一个很重要的限制，即笔者并未对“州政府在开展发放公共福利、税费征收或者通过网络空间预防犯罪等政府活动时，哪些行为可能侵犯公民隐私权”这一问题进行探讨。取而代之的，本文关注的焦点在于私营机构，关注私营机构如何在网络空间这一存有他人思想、信息等商品且鲜有管制的领域对他人的个人信息进行加工处理。政府侵犯公民隐私权的问题同样存在且同样重要，但笔者之所以将政府问题暂时搁置，部分原因在于，该问题已经得到了大量关注。[①] 与之相反，私营机构在涉及公民隐私权的问题上受到的审查则非常宽松，这是毫无道理的。私营机构对他人个人信息的利用已经达到可以与政府对他人个人信息的利用相竞争的程度。[②] 在此前提之下，笔者从探讨“网络空间隐私权”（cyberspace privacy）这一术语的构成要件开始。首先，笔者对“隐私权”（privacy）一词进行

① See, e. g., The Privacy Protection Study Comm., Personal Privacy In An Information Society 345 - 391 (1977); U. S. Dep't of Health, Educ. & Welfare, Secretary's Advisory Committee On Automated Personal Data Systems, Records, Computers, And The Rights of Citizens at xx (1973).

② See John Markoff, Remember Big Brother? Now He's a Company Man, N. Y. TIMES, Mar. 31, 1991, at E7.

是，我们从近年的文献资料中无法提炼出能够取代传统观点的新兴观点。实际上，理论复杂性和数据资料的缺乏使得决定制定者被置身于一个进退维谷的境地。正如 Ayres 和 Gertner 在文章中所阐述的，当一个默认规则在理论上被判断为高效可行时，“人们会心怀希望，希望法律制定者能够使得该默认规则在实践中得到落实和执行”。[①] 从这个角度来看，追求效率的决定制定者应当做的是什么？笔者认为，最好的做法是采取适度怀疑（modest skepticism）的态度。此处的“适度”体现为：不允许当事人提起含有具体数额的赔偿请求的诉讼；此处的“怀疑”体现为：拒绝使用任何简单腐败的诸如多数人规则之类的公式化规则。这种做法将会试图探究适用不同的默认规则所达至的平衡点在何处，同时试图关注当事人在默认规则之外达成的协议的不同来源。然后，审视上文标记的相关变量的完整范围，以期作出一个周全的（尽管仍然具有不确定性）裁判。

抱着适度怀疑的态度，让我们开始对默认规则的选择问题进行分析。假设我们选择 $D_1$（也就是全权使用的默认规则），那么，对于某则被信息收集者掌握的信息；若他人比信息收集者更加重视该信息的价值，那么，他人必须从信息收集者手中买回该则信息。在此种情况下，交易各方将达至什么样的平衡点？这些原先通常游离于默认规则之外（在上文提到的信息流通非常顺畅、市场交易成本为零的理想社会中，人们大多游离于默认规则之外）的交易各方是坚持遵循这种默认规则，还是依旧在默认规则之外进行额外约定？笔者相信，大多数人会坚持遵循这种默认规则。

让我们来仔细分析一下，游离于默认规则之外的人会做些什么。

首先，游离于默认规则之外的人将面临大量的调查成本，用于确定自己的什么信息正在被别人收集以及这些信息如何被使用。之所以要花费大量成本，是因为在当今社会中，大部分人在自己的个人信息如何在网络空间生成的问题上是缺乏线索、束手无策的，而且在他们的个人信息如何被收集和使用的问题上，信息的交易各方和交易促成

---

① Ian Ayres & Robert Gertner, Strategic Contractual Inefficiency and the Optimal Choice of LegalRules, 101 YALE L. J. 729, 733 (1992).

件。在该封电邮中，McVeigh 只透露了个人签名“Tim”，而未透露任何其他个人信息。一位玩具慈善捐赠活动的工作人员通过美国在线服务公司（AOL）网站中的会员信息记录，查询到“boysrch”是一名 AOL 注册会员的化名，该会员真名为 Tim，目前居住在夏威夷，曾经在军队工作，并且 McVeigh 还在个人信息的婚姻状态一栏中明确表示自己是“同性恋”。不久，该信息就被通报给了 McVeigh 当时的舰长，紧接着，军舰上的法律顾问开始对此事进行调查，怀疑“Tim”就是该艘军舰上的士兵 McVeigh。在与被告 McVeigh 会见前，军舰的法律顾问在未获授权的情况下，让其律师助理联系 AOL 网站，以获取该案的更多信息。该律师助理拨通了 AOL 的免费客服电话，在未声明其海军法律服务人员身份的情况下，谎称他已经收到了一份 AOL 客户的身份信息传真文件，想再次确认一下该身份文件的所有人。而 AOL 客服代表经过简单的搜索，很快告知他该身份文件的所有人就是被告 McVeigh。AOL 公司全然不顾禁止将私人信息外泄的规定，稀里糊涂地将客户信息透露给了他人。

总而言之，数据库隐私权问题的根源在于，各类机构在使用个人信息的过程中，全然不顾隐私保护政策，疏忽大意且不负责任地使用个人信息的行为，将对个人尊严的保护忘得一干二净。我们所走向的并不是一个充满 Big Brother 或是 Little Brother 的社会，而是一个官僚冷漠、专制武断、错漏百出、灭绝人性的更加愚蠢大意的社会，与 Kafka 在《审判》中所描述的社会越来越接近。

用 Kafka 的隐喻取代 Big Brother 的隐喻对数据库进行分析，能够为法律概念的确定与政策的制定带来种新的路径。举例而言，Amazon. com，一家互联网书籍零售巨头公司，会将与客户购书偏好有关的信息搜集起来（该信息从书籍销售行为中分析而来），然后根据该信息，为客户量身推荐书籍。如果对商家滥用个人信息的行为进行严格规制，那么，Amazon. com 这种搜集客户信息并使用的做法很明显会受到严格的限制。但是这种严格的限制，无疑会对当今社会中商业运营过程中必不可少的，并且对用户有益的信息搜集行为造成极大的损害。包括笔者自己在内的许多 Amazon. com 的客户都认为，该公司的书籍推荐功能十分有用。相反，如果按照本文的思路对数据库问题进行分析，那么，数据库问题的关键就不在于 Amazon 公司的信息搜

病的，他询问 Press 医生，SEPTA 的记录审查办公人员是否可以看到各个处方对应的姓名。Press 医生给出了否定的答案，Doe 才在该计划下按照处方配置了药品。不幸的是，虽然 SEPTA 从未查询与处方有关的姓名信息，但是 Rite-Aid 公司在其递交给 SEPTA 的报告中包含了处方对应的他人姓名。SEPTA 的工作人员 Pierce 在审查记录时，对 Doe 的药物使用情况颇感兴趣，并且着手对其进行调查。她向 Van de Beek 医生询问了该药物的情况，医生告诉她这类药物的用途，但是拒绝回答任何与药物使用者有关的任何问题。Pierce 还向 Press 医生进行了询问，Press 医生后来将 Pierce 的举动告知了 Doe。

这一信息对 Doe 而言犹如晴天霹雳。Doe 开始担心单位的其他人也会发现他的病情。他逐渐察觉人们对待他的态度有所转变。尽管如此，他并没有被解雇，并且事实上他还得到了升职。法院判决，由于该案中并没有任何保密信息遭到披露，因此被告并没有侵犯原告的宪法性的信息性隐私权。Doe 没有提供证据证明任何人得知了其病情，因而法院认为其受到的隐私侵犯仅仅是最低限度的。

然而，法院的判决未能抓住 Doe 的隐私权主张的实质。无论同事对待他的态度是否是他臆测的，他的的确确饱受了真实的、可感知的恐惧。他的真正损害在于他感到的无力感，他无法获知究竟有哪些人知道他患了艾滋病、雇主如何看待他或者会不会有人利用这一信息对其不利。正是这种不安感，使其对工作环境中的一切事物的看法都发生了转变。该案中的隐私权问题不仅仅在于 Pierce 披露了他的秘密或是 Doe 失去了对其自身信息的控制，而是信息已经完全失控，不受任何人的控制。Doe 的处境与 Joseph K. 的处境极其相似，他们都陷入了对最终裁决的无尽的等待。他被告知其信息已经被收集，他知道他的雇主正在对其进行调查，但他却无法感知、掌握与上述过程有关的任何信息。在某种程度上来看，Doe 也经历着与 Joseph K. 相同的绝望无助，他们明知道其他人掌握着有关他们的信息，并且其他人实际上正在利用这些信息，但是他们却被置之度外。

通过 Kafka 的隐喻理解数据库问题，我们可以发现，数据库问题关乎的不仅仅是保密，还关乎信息的使用。通常而言，个人信息不是保密的，它们存在于许许多多的人的脑海中，被分散地保存于全国各种各样的文件与计算机档案中。这些信息关乎人们阅读的材料、食用

“如果有三个人知道一个秘密，那么，只有当其中的两个人都死了，这个秘密才能被称为秘密。”① 这种方法确实可以保守一个秘密，但是在现实生活中，我们必须找到一种更缓和的方法。有一些能够起到加强隐私权保护的技术，如加密技术，在一定程度上保护了他人的数据和通信内容免受非法刺探。

在当今社会，要想一个秘密不被其他人知道几乎是不可能的，除非你独自去丛林生活。只要我们生活在正常的社会中，我们在领驾照的时候就一定会被要求去照相和填写个人资料，我们在找工作的时候就一定会被要求出示身份证。我们的住宅常常遭到窥探，我们的医疗数据和财政数据也常常遭到泄露，我们的通信内容很容易被拦截，我们的生活就像一本打开的书，任何人都可以查看到我们生活的细节。从政府的角度看，个人私人生活变得越来越透明。那些臭名昭著的电话窃听事件发生在不同人的身上，例如，英国王子 Charles、众议院议长 Newt Gingrich 以及白宫实习生 Monica Lewinsky 等丑闻都是因为电话窃听而被爆出来的。技术的革新、经济和社会的发展创造了摧毁隐私权的技术，这也是社会发展趋势使然。当隐居生活变得不再可能后，个人数据是否被公开就已经不是数据主体所能控制的了。因此，我们要讨论的是该怎样用法律条文来规制数据的收集和使用行为。

随着侵犯隐私权的技术越来越先进，我们有必要考虑如下问题：目前对他人信息性隐私权的保护是在我们能够容忍的范围吗？我们已经进入了一个零隐私权的时代了吗？针对上述问题，笔者将在本文一一解答。

文章第二部分介绍收集个人私人信息的技术。信息收集技术的快速发展给信息性隐私权带来的伤害是前所未有的，监控技术会侵犯他人的隐私权，这已经不是什么新闻了，但是监控技术渗入现代生活的程度以及数据库中被处理的个人信息量却还是让我们大吃一惊。虽然我们还只是处在数据挖掘、消费者信息处理以及 DNA 数据库的早期时代，但是这些技术进步已经改变了所有工业化国家的面貌。如果我们不采取一些措施来对抗技术的发展，隐私权将荡然无存。

---

① Benjamin Franklin, Poor Richard's Almanac (1735), reprinted in The Oxforddictionary of Quotations 211 (2d ed. 1959).

虽然该决议不具有强制性，但是该决议始终是对欧洲执法区监管日程的公告。根据该决议，欧洲的互联网服务提供商和电话公司要为执法机构提供全天候并实时地访问互联网网络通讯的便利。此外，无线通信服务提供商还要提供用户地理位置信息。如果服务商提供的是加密业务，那么，服务商就要保证该加密业务可以被解密。

根据美国于1994年颁布的《通信协助执法法》（the Communications Assistance for Law Enforcement Act），所有新的通信网络都应该被设计成可以受到合法监听的形式。该法没有解决加密这个问题，也没有指明通信网络应该支持多少同时发生的电话监听，这些都由实施条例予以规定。在对运营商能力是否达到要求的最初评估中，美国联邦调查局认为，运营商最大的监控力度应该达到能够同时监控同一时间内所有通话的百分之一。这项提议引起了很大的争议，美国联邦调查局不得不撤回了该提议并提出了另一项替代提议。虽然替代提议的内容有些模糊不清，但是该提议放宽了准入标准。根据民主和技术中心（Center for Democracy and Technology）的估计，如果按照美国联邦调查局的标准，如果在洛杉矶，该系统必须能够支持对136000通电话进行同时监听。

在美国，在没有法院命令的情况下对他人住宅进行监听是违法的，而申请监听命令的主体仅限于执法机构和反情报机构。[①] 在1998年，美国联邦法院和各州法院批准了1329个电话监听案件。而在1年前，美国联邦法院和各州法院只批准了738起，这10年增长了近80%。[②] 这些数据在一定程度上来说具有误导性，因为一个允许监听的法院命令可以监听的电话达到几百台，可以监听的通话甚至可以达到100000起。该数据也和美国联邦调查局统计的数据不一致，根据美国联邦调查局的统计，在高峰时期，洛杉矶每天受到监听的电话就多达1000起。法院颁发的允许电话监听的案件变多了，受到监听的人群也变多了，但是和电话通讯使用人数相比，这个比例还算是比较

① see, a. g. United States v. Rene Martin Verdugo-Urquidez, 494 U. S. 259 (1990).

② See Administrative Office of The U. S. Courts, 1998 Wiretap Report 5 (1999) <http://www.uscourts.gov/wiretap98/contents.html> Associated Press, State Authorities' Wiretapping Up, May 5, 1999 <http://jya.comwiretap98.htm>.

出台该加密政策的原因。加密技术是一项重要的 PET，如果加密技术运用得当，那么，保护他人隐私权的目标就容易实现。和其他技术不同，加密技术相对来说不贵而且任何一个有电脑或者其他加密设备的人都可以使用这种技术。不过，加密技术并不是解决隐私问题的万灵药。它很难实施得当，即便是最好的加密技术，它对于底层操作系统以及软件程序的任何一个安全漏洞都没有防御力。加密技术只能解决通信和记录中发生的隐私权难题，而这些领域发生的隐私权难题只是我们生活中面临的隐私权问题的一小部分。

法律禁止 PETs 的实施要么就是其他政策的副产品，要么就是长期以来对互联网进行限制的后果。例如，禁止反向工程软件（reverse engineering software）的开发从经济学角度来看就可能不是最有效的，反向工程软件是一种能够发现其他软件如何运作的软件。但是这种禁止性措施几乎使得那些技术成熟的用户几乎不相信自己所用的程序是安全的，因此，如果该程序的作者没有公开改程序的源代码以供查看，他们也无法让我们放心。

从公民隐私权在公共场所受到限制的角度看，我们有必要重新审查那些禁止低技术的隐私权保护工具的规则。将佩戴面具作为一种潮流或许是应对无处不在的摄像机的一种可能方式，然而，美国有许多州颁布了反面具法，该法通常作为控制三 K 党的一种方式。有些法律已经实施了 100 多年了，根据这些法律的规定，在公共场所佩戴面具是一种犯罪行为。[①] 禁止公民在公共场所佩戴面具的行为是否违反了《美国联邦宪法第一修正案》？关于这个问题，法官主要有两种观点，有人赞成，有人反对。抛开宪法问题不谈，不可否认的是，反面具法都是在人们无法想象到所有的公共场所都布满摄像机的时期颁布的。面具曾经被视为三 K 党恐吓的标志，到了现在这个社会应赋予其新的含义。即便我们假设反面具法符合 McIntyre v. Ohio Elections Commission 一案[②]确立的匿名发表言论的宪法性权利，如果我们要赋予面具新的含义，我们也要对反面具法进行重新思考。

---

① See Wayne R. Allen, Klan, Cloth and Constitution: Anti-Mask Laws and the FirstAmendmnent, 25 GA. L. REV. 819, 821 n. 17 (1991).

② 514 U. S. 334 (1995).

### 2. 法律途径

技术会侵犯他人的隐私权，这一点已经毫无疑问。学者、政府隐私特派员和技术员提出了一些法律改革的建议，他们建议将现有法律中的有关数据收集的默示规则移除出现有法律。根据现有法律，交易双方对交易中产生的个人私人数据都享有所有权，有学者建议，他人对交易中的个人私人数据应该享有传统的产权利益或者知识产权利益，商人或者其他观察者在没有和他人交涉的情况下是不能将这些数据拿走的。还有人提议，应该将公共场所的数据收集行为定性为隐私侵权行为或者犯罪行为。这些提议有很多值得学习的地方，但是也有一些缺点。

（1）以事务性数据为目的的解决方式。为了保护个人私人数据，学者根据传统的财产法或者知识产权法提出了许多立法改革提案，他们建议赋予个人对自身数据的唯一使用权。虽然法律改革的提议很多，但是这些改革提议的目的都是为了改变现有法律中的这种默示规则，赋予他人对自身个人数据的唯一使用权，即便商人共享他人的个人数据，或者他人的个人数据在公共场所是可以看见的，也要赋予他人对自身私人数据享有财产性权利。不过，这些提议无论从理论上还是实践上来看都有不少缺点。

有一个问题是，我们必须保证这些规则不会违反《美国联邦宪法第一修正案》。任何限制他人表达自己看到的或者知道的事情的规则都可能威胁他人的言论自由权。[①] 当前的理论大多数主张对《有线通信法》和《录像隐私权保护法》进行修改，但是，这并不意味着这种立法改革是一件容易的事。Kang 教授提醒我们："想象一下如果 Bill Clinton 对自身信息有着绝对的控制权，那么，《纽约时报》在没有得到 Bill Clinton 同意的情况下就不能撰写任何有关他的文章。没有人建议给予个人对个人自身数据那么大的控制权，更不用说是公众人物了。而那些主张赋予他人产权或者知识产权的提议通常关注事务

① See, e. g., Rochelle Cooper Dreyfuss, Finding (More) Privacy Protection in Intellectual Property Lore, 1999 STAN. TECH. L. REv. VS 8 <http://llstlr.stanford.edu/STLR/Symposia/Privacy/index.htm>; Viktor Mayer, Generational Development of Data Protection in Europe, in Technology & Privacy, supra note 178, at 219, 232.

制这些行为，加利福尼亚州的《反狗仔队法》就是一个典型的例子。根据该法的内容，私人要对其采用增强敏感性的技术收集他人信息的行为承担责任。这部法律扩大了他人在自己住宅中的隐私空间，将他人的数据视为不可侵犯的财产，但是该法并没有将狗仔队在公共街道的行为纳入其中。还有一些法律旨在规制拦截监控设备的购买和使用行为。例如，《美国法典》第18卷第2512条就禁止生产、销售、持有有线的、口头的或者电子的通讯拦截设备以及为那些设备打广告。[①] 或许，现在是号召规制窃听设备的时候了。

这两种方式或许都是可行的，但是这两种方式实际操作中或许会受到限制，因为这些方式可能和《美国联邦宪法第一修正案》相冲突。许多侵犯隐私权的技术的使用可能是合法的，例如，电视摄像机、摄像头在银行就广泛使用。绝对禁止使用这些技术是不可能的，这需要花费的代价也很大。允许某些场合使用这些技术，而其他场合又不允许使用这些技术，这会很难监管。当技术还比较新并且运用范围不广的时候，采用技术控制的方法效果最好。但是在这种情况下，人们对这种技术的了解也还比较少，还不了解这些技术的危害，对这些技术进行规制的法律也就少了。加利福尼亚州的《反狗仔队法》只适用于增强感官的数据收集行为，该法并没有规制执法中的数据收集行为，也没有规定数据库。因此，这部法律并不适用于公共空间。

（3）经典的数据保护法。行业自我规制的失败、以市场为基础方式面临着困境，使得欧盟以及美国着手制定数据保护法。欧盟法以该法对数据收集、再利用和转售行为的规制而出名，欧盟法以及欧盟国家的法律还对数据的种类进行了限制。欧盟规定，欧盟成员国不得将数据出口到那些缺乏数据保护规则的国家，当然，这个比较的对象是欧盟标准；但它并不要求外国的数据保护法要满足欧盟的标准，这使得像美国这样的国家可以自我决定对消费者采取哪些保护措施。到目前为止，美国制定的数据保护法少之又少，加利福尼亚州的《反狗仔队法》已经是这方面的典型了。不过，这种情况将会发生改变。对于未获得父母同意而收集未满13岁儿童信息的行为，美国联邦贸易委员会公布了具体的规制措施，这一措施将于2000年正式生效。

---

① 18 U. S. C. § 2512 (1) (a), (b) (2000).

信息，而且书店可能已经提供了这些信息。①

为什么我们能够期待自己与之交易的商家、银行和保险公司都会尊重并保护我们的隐私呢？毋庸置疑，一部分原因在于前数据采集时代所遗留下来的风俗，另一部分原因在于不论是商人、银行，还是保险公司、经纪公司，都对此表示支持，因为这对于他们而言是有利可图的。如果这种信任不能存在，那么，我们将不愿主动提供我们的信用卡号，当我们购买一些令人尴尬的商品或是观看一些按次收费的电影之前总会思量再三。通奸者将会用现金支付幽会的费用，会用投币式电话联系对方而不会使用自己的手机。

对顾客交易信息的滥用、出卖与汇总都明显违背了顾客的信赖。最初的信息接收者塑造了这种信赖的情感并受益于此。消费者能否以这种违反信赖义务的行为为由而提起诉讼？依据现在的法律，答案似乎是不能。

医生按照惯例都对其病人负有保密义务，如果医生未经病人的同意而披露病人的信息，那么，病人就可以以此提起侵权诉讼。② 此前已经有会计师和银行因为披露顾客信息而承担法律责任。③ 当雇员从雇主的工资表中收集并滥用相关信息，被认为是盗用商业机密的行为。然而，法院坚持认为，保守信息的义务与责任来源于信息主体与信息接收者之间的特殊关系。不论有多少商家、银行、保险公司、经纪公司、有线电视运营商、通讯公司或互联网正在收集顾客的信息，但我们难以振振有词地说他们与其顾客的关系有多特殊。

消费者对诸多商家追踪其个人信息的行为往往非常不满，如果说违反了保密义务就是这种不满的本质，那么，在消费者与那些商家的关系之中一定有些什么能够解释消费者对这种违反义务行为的不满情

---

① See Doreen Carvajal, Book Industry Vows to Fight 2 Subpoenas Issued by Starr, N. Y. TIMES, Apr. 2, 1998, at A20.

② See, e. g., Home v. Patton, 287 So. 2d 824 (Ala. 1973); Cannell v. Med. & Surgical Clinic, 315 N. E. 2d 278 (IlL. App. Ct. 1974) (same); Doe v. Roe, 400 N. Y. S. 2d 668 (N. Y. App. Div. 1977) (same); McCormick v. England, 494 S. E. 2d 431 (S. C. Ct. App. 1997) (same).

③ See, e. g., Rubenstein v. South Denver Bank, 762 P. 2d 755 Edward L. Raymond, Jr., Annotation, Bank's Liability, Under State Lmv, for Disclosing Financial Information Concerning Depositor or Customer, 81 A. L. R. 4th 377 (1990).

人数据最终都会成为商品并参与交易。这一现状也许会使人体芯片和wOzNet的制造者适时调整他们的商业模式，该模式曾被称为“付钱就走”的形式，其目的在于允许数据交易。在现有的“付钱就走”的形式下，人体芯片和wOzNet都是以一个统一的价格卖给消费者。这种以统一价格标价所有产品的完全之策是如何产生的？是在允许他人通过付款从而限制个人信息被行为人传播的过程中产生的，或者相反而言，是在商家以商品折扣换取顾客个人信息使用权中产生的。虽然人体芯片和wOzNet，目前都没有从它们本身所收集的个人信息中获得太多的商业利益，但个人数据的交易依然在其他领域日渐繁荣。一份计算机杂志曾这样评论那些文件共享服务中的广告：“从某种程度上说，你是在付费，但这种费用不是金钱，而是隐私。”

**2. 隐私**

本文所提到的那些技术产品无疑都会对他人的隐私造成威胁。尤其是个人数据的商品化会促使数据交易的急剧增多。当Derek带着自己的植入式人体芯片或是可佩戴的wOzNet芯片来到一家商店时，他便会触发该商店的中央计算机，于是，这台计算机就会根据Derek此前的购物记录和其他相关商场的营销清单塑造出Derek的形象，并将这些信息告诉给这家商店之中的所有售货员。商店的中央计算机也能够通过查看Derek在店内的行踪，从而判断他更喜欢哪类产品。如果他在展示数码相机的柜台前驻足观看，那么，店员一定会从计算机上发现这一点。如果计算机将Derek总结为一个电子产品爱好者或是某家公司的“粉丝”，那么，店员就可以直接向他推荐相关产品。总之，店员会将更多的注意力投给Derek，而不是其他那些他们一无所知的顾客。①

即使Derek并没有购买任何商品，但他对该店铺的光顾和他对数码相机的兴趣都会被记录到他的“市场形象”信息档案之中，其他商家也能分享这些新信息并将其用于不同目的。根据这个不断更新并扩充的个人信息数据库，Derek会收到许多为他量身定制的产品广告。作为另外一种反乌托邦的戏剧形象，我们也可以想象Derek可能

① See Don Peppers & Martha Rogers, The One to One Future: Building Relationships One Customer At A Time (1993).

其二，一些酒吧和餐馆会对驾驶员执照上的条形码和磁条进行电子扫描。[①] 驾驶执照上包括一个人的姓名、住址、年龄、体重，在某些州中，也包括社保号码。掌握了这些信息，酒吧和餐馆就能知道这名顾客多久来光顾一次，他会待多久，甚至于知道他本人属于哪个团体。如果酒吧和餐馆允许顾客用信用卡消费，那么，通过这些信息也能获知顾客的其他消费记录。由此生成的数据库存在着巨大的市场潜能。这个例子提醒我们，我们应该在多大程度上允许私营部门使用那些收集信息的基础设备，政府建立这些基础设备本来是用于其他目的的。

信息性隐私权具有个人和社会的双重价值。因此，我想以这样一个警示来结束本文：我们必须要对那些针对个人数据的管理措施进行不断审查，因为隐私市场的失灵会同时损害人们的个人自决权与民主审议权。

① Kim Zetter, Great Taste, Less Privacy, WIRED NEWS (Feb. 6, 2004), at http://www.wired.com/news/privacy, 1848, 62, 82, html.