重新思考Internet的设计：端到端争论与勇敢的新世界

麻省理工学院计算机科学实验室的David D.Clark，ddc@lcs.mit.edu

Marjory S. Blumenthal，计算机科学与电信学系，mblument @ nas.edu

TPRC提交的版本，2000年8月10日

抽象

本文着眼于Internet以及对Internet不断变化的要求集。随着它变得更加商业化，更面向消费者，并用于用途广泛。我们讨论了指导互联网设计的一系列原则，称为*端到端的论证*，我们得出的结论是，现在出现的要求可能会损害互联网的原始功能设计原则。如果发生这种情况，互联网可能会失去一些关键功能，特别是它支持新的和意外应用程序的能力。我们联系这可能趋势的结局：互联网，尤其是互联网中新的利益相关者的增加服务供应商; 新的政府利益；不断增长的用户群不断变化的动机；以及对可信赖的整体运营的需求与无法信任之间的紧张关系个人用户的行为。

介绍

端到端参数是一组（除其他事项外）表征的设计原则互联网的设计方式。这些原则最早是在1980年代初期提出的，在近20年的无数设计辩论中，它们一直是建筑模型。端到端争论涉及系统中应如何满足应用程序要求。构建通用系统（例如，网络或操作系统）时，以及然后使用此系统构建特定的应用程序（例如，电子邮件或World Wide Internet上的Web），这些特定应用程序及其所需的方式存在疑问应该设计支持服务。端到端的论点表明具体应用程序级功能通常不能（最好不应该）内置到较低层中系统的各个级别-网络的核心。其原因如下原始纸：

> *只有使用以下命令才能完全正确地实现所讨论的功能站在通信系统端点的应用程序知识和帮助。因此，提供该有问题的功能作为通信系统本身的功能是不可能。*

在原始论文中，有关应用的端到端推理的主要示例功能是确保在网络上准确，可靠地传输信息。即使有任何一个较低级别的子系统（例如网络）也尽力确保可靠性，离开该子系统后可能会丢失或损坏。最终检查正确执行

必须在应用程序级别，在传输的端点。有很多例子
这种观察在实践中。

1个

第2页

即使部分应用程序级功能可以潜在地实现在
在网络中，端到端的论点指出，如果可能的话，应该抵制这种方法。那里
将特定于应用程序的功能移出核心的许多优势
网络，并在那里仅提供通用系统服务。

- =降低了核心网络的复杂性，从而降低了成本并促进了未来
  升级到网络。
- =网络中的通用性增加了可以添加新应用程序的机会
  无需更改网络核心。
- =应用程序不必依赖于成功实施和运行
  网络中特定于应用程序的服务，这可能会提高其可靠性。

当然，端到端参数不是绝对的。有一些功能
只能在网络的核心中实现，效率和性能问题
可能会激发核心定位功能。但是，从
边缘节点的核心和“出站”已很好地充当了Internet中心设计原则。

由于端到端的争论，互联网已经发展为具有一定的
特征。通过转发路由器在Internet中实现的功能
数据包-仍然相当简单和通用。实现的大部分功能
特定的应用程序（例如电子邮件，万维网，多人游戏等）具有
已通过连接到网络“边缘”的计算机上的软件实现。边缘-
Internet上的应用程序定位和相对简单性共同
促进了新应用程序的创建，它们是创新环境中的一部分
互联网。

从头到尾移动

在最初的20年中，互联网的大部分设计都是端到端的指导
岁 论点。在很大程度上，网络的核心提供了非常通用的数据传输
服务，运行在该服务上的所有不同应用程序都将使用该服务。个人
应用程序的设计方式不同，但大多数情况下对
端到端设计方法的优点。但是，在过去几年中，
互联网及其应用出现了新的要求。对于某些利益相关者，
这些不同的新要求可能最好通过在
网络的核心。反过来，这种观点引起了那些希望
保留原始Internet设计的好处。

以下是当今互联网新兴需求的一些（相互关联的）示例：

不可信赖的世界中的运营：端到端原始文件中的示例
假设端点愿意合作以实现其目标。今天少了
很少有理由相信我们可以相信其他端点的行为符合预期。的
网络上不可信任的端点的后果包括对整个网络的攻击，
对单个端点的攻击，不期望的交互形式，例如垃圾邮件，以及
诸如网页之类的烦恼由于端节点畸变而消失。[3] 情况是
关联人口的急剧增长及其可预见的后果
多元化，以使人们拥有更多使用互联网的动机，
使用某些被视为滥用或滥用的内容。使网络更加可信，同时

端点不能被信任，似乎暗示着网络中心的更多机制
实施“良好”行为。

第3页

考虑垃圾邮件-出于广告或其他目的而发送的垃圾邮件。垃圾邮件不是
不受欢迎的终端节点行为的最有害示例-它通常使人烦恼而不是
破坏。但是，它提供了一个很好的例子，说明了如何采用不同的控制方法
端到端争论的宗旨的不同方式。是接收垃圾邮件的人，而不是
电子邮件软件，希望避免收到它。保持在端到端框架内，但
在最终端点（使用系统的人员）应用论点意味着
发送方发送垃圾邮件，接收方的软件接收垃圾邮件，然后人工接收方
删除它。基础协议，包括TCP层和更高的SMTP邮件
传输层，只是支持机制。但是，由于用户不喜欢时间（两者
个人和互联网连接时间），有时还花费了一些钱来收集和删除
不需要的邮件，有些已经在网络中其他地方提议了应用程序级功能，而不是
仅在收件人的计算机上，以防止垃圾邮件到达边缘。[4]

要求更高的应用程序：互联网的简单服务模型（称为“尽力而为”
交付”）不保证任何特定应用程序将实现的吞吐量
任何时候。诸如文件传输，Web访问或电子邮件之类的应用程序可以容忍
速率波动-虽然用户可能会因投放速度慢而感到沮丧，但应用程序仍然
“作品。”如今，出现了一系列新的应用程序，以流音频和视频，
似乎需要更复杂的Internet服务，以确保每个数据流
指定的吞吐量，这是尽力而为服务无法提供的保证。不同
从（重新）设计应用程序开始仅使用
当前的尽力而为服务，可能是通过动态调整传输的保真度
随着网络吞吐量的变化而变化的信息。至少一些应用程序设计师拒绝了这一点
他们可以设计的限制。另一种方法是添加新的数据传输
网络核心中的服务，它们提供可预测的吞吐量和有限的延迟，并且
这些建议已经提出。[5] 但是，Internet服务提供商（请参阅
下方）到目前为止还不愿意提供这些新服务。结果，申请
建筑商采用了安装中间存储站点的策略，以定位
流内容靠近接收者，以增加成功交付的机会。从而，
与简单的端到端结构不同，这些新应用程序的设计取决于两个阶段
通过这些中间服务器进行交付。

ISP服务差异化：部署增强的流传输服务
媒体和其他类型的高级Internet应用程序受当前业务模型的影响
较大的Internet服务提供商。他们（至少目前）似乎在查看增强型数据
运输服务，作为在ISP范围内提供的一种竞争产品
区分因素，有时与特定的应用程序相关，例如Internet上的电话服务，
而不是跨多个提供商网络端到端支持的功能。如果
无法端到端提供增强的服务，因此无法设计应用程序
需要使用端点实现来提供这些服务。因此，如上所述，
加速基于中间服务器的应用程序的部署
位于每个ISP内；内容交付给增强型岛内的ISP客户
服务。这种方法具有额外的效果，引起了消费者的关注
维权人士：由各方产生的有能力促进和发展的应用程序的区别
利用那些可能依赖于ISP的中间服务器，
性能，端到端运输。[6] 然而，这里的问题是封闭投资
增强服务的孤岛，加上对每个孤岛内内容服务器的投资，
降低了选择开放式端到端服务的投资动机。一旦
从一条投资道路开始，另一种选择可能很难实现。

第4页

第三方参与的兴起：越来越明显的问题是第三方的需求
各方将自己置于交流端点之间，而不考虑
结束。 [7] 第三方可以包括组织的官员（例如，公司网络或ISP
实施组织政策或其他监督的管理员）或
政府，其利益范围可能从税收到执法到公共安全。
法院下达的窃听记录说明政府作为第三方介入，而强制性
阻止某些内容可能涉及政府或组织干预。

不太熟练的用户：互联网是由技术人员设计和最初使用的。如
随着用户群的扩大，动机变得越来越容易使网络易于使用。通过暗示
端节点上存在大量软件，端到端参数是
用户的复杂性：必须安装，配置，升级和维护软件。它
对于某些人来说，利用服务器上安装的软件更具吸引力
网络上的其他地方。 [8] 易用性的重要性只会随着
消费者计算性质的变化。当今的计算机世界不仅包括PC。它
具有嵌入式处理器，便携式用户界面设备（例如计算设备）或
个人数字助理（PDA，例如Palm设备），支持网络的电视和高级
机顶盒，新型手机等。如果要求消费者设置和
分别配置他拥有的每个联网设备，至少有一个这样的机会
将配置不正确？通过配置委派，该风险会更低，
保护和控制到一个共同点，可以充当设备池的代理。 [9]
这个共同点将成为应用程序执行上下文的一部分。有了这个
这样，应用程序将不再有单个不可分割的端点。

尽管这些趋势中没有一个能够强大到足以将互联网从一种
端到端网络到具有集中功能的网络，事实上它们都可能激发
向同一方向移动可能预示着网状结构的重大总体变化。这样
变化将改变互联网的经济和社会影响。这种认可是背后的
这些变化的政治以及各方支持和反对各种方向的言论
开发和部署机制。端到端争论最近
在政治辩论中被明确引用，反映了赌注的增长和
辩论愈演愈烈。 [10] 争论的焦点是对“互联网
理念”：行动自由，用户授权，最终用户行动责任
采取的措施，并且缺乏“限制”网络用户行为的控制措施。结束于
最终论点促进了这种哲学，因为它们使创新，安装的自由得以实现。
随意添加新软件，并运行用户选择的应用程序。

端到端参数在某种程度上预设了某些类型的关系：
在两端进行沟通，在各方之间及其提供者之间
网络/互联网服务，以及最终用户或具有一系列第三方的ISP，这些第三方可能
对前两种关系中的任一种感兴趣（因此对
通讯）。如果各方利益之间存在紧张关系，
考虑目标（以及我们可能或可能会考虑的技术机制的优点）
而不是添加到网络中）在很大程度上取决于我们对案件具体情况的价值观。
如果通信方被描述为“持不同政见者”，则第三方试图窃听
或阻止对话是一个“压制性”政府，大多数人是在自由的背景下提出的
演讲将使他们的兴趣与最终当事人保持一致。将“持不同政见者”一词替换为
“恐怖分子”，而且许多人的处境变得不太清楚。同样，ISP的动作是什么时候
对设施和服务的负责任管理，以及何时操纵

第5页

通过其访问的内容和应用程序的性质和有效定价的控制
设施和服务？

也许最具争议性的问题围绕着越来越多的第三方参与
合作用户之间的通信。交流端点时要
进行沟通，但某些第三方要求将自己插入到路径中，而无需他们
协议，端到端的论点并没有提供一个明显的框架来对此进行推理
情况。我们必须放弃端到端的争论，拒绝第三方的要求，因为
它没有“适合”我们的技术设计原则，也没有找到可以保留的其他设计方法
端到端争论的力量越强。

保留端到端的论点意味着如果在给定的管辖范围内
要实现的政治或管理目标，应通过技术和手段来支持实现这些目标
基于网络技术的系统的更高级别的策略，而不是通过“内部”机制
网络。互联网的新环境意味着关于放置位置的决定
机制将更加政治化，更多的人可能需要更令人信服的
端到端决策的优点比Internet早期要好。现在是时候进行系统的
检验坚持或偏离互联网端到端争论的含义
进化。

本文的其余部分安排如下。我们首先对一些新要求进行分类
用于当今通信中的控制和保护。我们记录了对
Internet解决了这些新要求。然后，我们确定了一系列可能的解决方案，
可能会用来满足这些要求。我们研究技术选择，但我们强调
非技术方法（法律，社会，经济）很重要，有效且通常更可取。我们
然后研究对各方权利和责任的影响，
包括互联网-消费者（用户），商业ISP，机构网络
提供者，政府等。我们描述新兴参与者的范围，以强调
新世界中利益相关者空间的复杂性。我们通过提供一些结论
关于什么是最根本的变化以及什么是最大变化的观察和推测
重要的是要保存过去。

当今交流中的需求示例

如上一节所述，当今沟通的许多复杂性反映了
不同参与者之间互动的方式更加多样化。本节中列出了一些
需求，以说明问题的广度并提出解决方案的范围，
将被要求。

用户交流但彼此不完全信任

当两个（或更多）终端节点想要进行交互时，发生一种重要的交互作用
彼此交流但彼此不完全信任。有很多这样的例子
情况：

- ∞ =双方要谈判具有约束力的合同：他们可能需要对称证明
  签署，保护合同免遭拒绝，等等。[11]
- ∞ =一方需要外部确认通讯中的另一方是谁。
- ∞ =在另一个极端，两个当事方希望彼此通信，但至少有一个
  各方希望保留其匿名性。这个话题非常重要，我们
  请在下面详细考虑。

6页

用户交流但希望匿名

在许多情况下，可能会出于以下原因而产生对匿名的渴望：匿名的政治演讲和吹口哨，以保留个人隐私，同时看着网站。至少在美国，可以看到匿名公开政治演讲的特权作为受保护的权利。在这种情况下，演讲者将寻求保证其匿名性不能在当时或之后被渗透。这种关注不仅针对第三方-可能想发现发言人的人，但是政府本身可能想要压抑某些表情。另一个例子是在线投票。个人选民需要一些外部保证他们的选票是匿名的。投票系统需要确保只有注册选民可以投票，每个选票最多只能投票一次。市民集体寻求保证投票不会因拒绝服务攻击而中断，投票计数准确，并且没有投票欺诈的机会。第三个例子是呼吁匿名电子在Internet上现金付款，以便可以匿名完成在线购买。[12]

对匿名的渴望就是这样一种情况的例子：各方可能未达成一致。一端可能希望隐藏其身份，而另一端可能需要身份或至少确认某些属性（例如，成人身份或公民身份）以授权采取行动。

可以通过多种方式在网络上跟踪一个人的身份。例如，低水平诸如电子邮件地址或用户计算机的IP地址之类的标识可用于关联后续动作并建立用户个人资料，该用户个人资料又可以链接到更高级别用户在特定情况下提供的标识。[13] 动态互动控制（例如尝试识别）及其避免行为表明互联网仍在灵活，规则仍在发展，最终形式还不清楚。[14]

最终方不信任自己的软件和硬件

人们日益认识到消费者可以使用的硬件和软件今天的行为就像一种双重代理，将有关消费者的信息发布给其他各方支持诸如建立个人消费者档案等营销目标。例如，当今的网络浏览器存储“ Cookie”（从网络通过网络发送的一小部分信息）Web服务器），然后将该数据发送回相同或不同的服务器，以提供链接的跟踪连续交易，从而提供用户行为的历史记录。[15] 处理器可能包含可以将一台计算机与另一台计算机区分开的唯一标识符，以及各种程序例如浏览器可以修改为在通过Internet，允许将这些消息关联起来。[16] 本地网络接口（例如，以太网）包含唯一标识符，因此担心这些标识符可能会被用作保留跟踪个人行为。[17] 这些不同的动作正在由或多或少要求用户使用的软件（在用户计算机上）（小流行的操作系统，Web浏览器等的数量）以及可选的应用。18岁

目的与中间：第三方维护其被包括在某些种类中的权利交易

另一类广泛的问题可以描述为第三方主张其获得以下方面的权利：插入到彼此完全信任并考虑的终端节点之间的通信中自己有足够的能力独立完成自己的交流。有许多这种情况的例子。

第7页

∞ =各国政府维护其窃听（在他们指定的情况下）进行窃听的权利
在其管辖范围内的某些通讯上。

∞ =政府，按照传统，如果没有明确宣布特权，则暗中监视
当事人在其管辖范围之外的通讯。

∞ =各国政府承担控制某些当事方进入的权利
某些材料。范围包括防止未成年人获得色情
防止公民散发煽动性或不受欢迎的物质的材料
由那个政府。

∞ = 各国政府维护其参加其政府采取的具体行动的权利
公民出于公共政策原因，例如执行商业税收
交易。

∞ =私人ISP维护其权利以其利益为目的调节其网络上的流量
管理负载，以及将意图不同的用户（例如
提供或仅使用某些应用程序服务），以便向它们收取不同的费用。

∞ =私有组织维护其控制谁有权访问其Intranet和访问权的权利。
他们访问Internet的网关，以及目的是什么。

∞ = 私人方宣称有权干预整个网络中的某些行动，以
保护他们在所转让材料中的权利（例如版权）。

诸如权利持有人之类的私人团体的要求可能与
政府。以简单的方式应用端到端的论点表明，愿意
发件人可以使用他选择的任何软件将资料传输到愿意的收件人。持有人
知识产权可以断言，有点像收税人，但在私人
域中，他们有权干预自己的转让，以保护自己在
物质（以及收取费用的能力），因此有可能成为网络问题。[19]

对于这些目标中的每一个，都有两种观点：第三种是机制
各方用来将自己注入到通信中，并且最终方有行动
尝试避免这种干预。通常，可以在内部找到具有两个目标的机制
网络，代表了有关各方之间动态，不断发展的力量平衡。

不同的第三方目标会触发一系列要求，以观察和处理
通过网络的流量。某些目标（例如某些形式的窃听）呼吁
用于访问通讯的全部内容。另一方面，一些目标
仅查看IP地址和其他高级标识信息即可满足
描述交流。后面这些活动（称为*流量分析*）很常见
在通信安全和执法社区中，可能会被视为
与全内容访问相比，排名第二。

在当代环境中，对通信模式的关注已超出了
政府对各种私人团体的支持，部分是因为技术使之成为可能。一种
流量分析出现在Internet的大型组织用户的环境中，其中
管理层正在监管如何使用组织资源（例如，通过监视电子邮件）
模式或访问色情网站[20]）。最后，ISP可能会在支持中使用流量分析
他们的交通工程。ISP断言对他们进行流量检查很重要
他们为了理解用户行为的变化模式而进行的活动；有了这些信息
他们可以预测不同应用程序的增长率，从而预测对新服务器的需求，更多
网络容量等等。Napster推动了大容量MP3文件交换的兴起（
个人收藏的目录）和用于点对点共享的Gnutella，说明了

第8页

ISP需要跟踪的现象。通常，他们不需要查看实际数据
消息，但仅在指示正在使用哪个应用程序的标识符处（例如，是否
消息是电子邮件或Web访问）。

某些第三方希望观察消息的内容引起了有关
端点与第三方之间的力量平衡。正如我们在下面详细介绍的那样
可能会尝试阻止对其数据的任何观察，对此第三方可能会尝试
规范端点使用此类方法的程度。可能还有其他要点
在总体隐私和信息的总体可访问性（例如*标签*）*之间*
解释或揭示特定事实的信息。信息的标签是
在下面讨论。

一方试图强迫另一方互动

当终端节点之间的期望不对称的例子达到极限时
一方根本不希望互动，而另一方希望对此进行某种参与。
这种对某人大喊大叫的网络具有多种形式，从应用程序到
不必要的材料（例如，电子邮件垃圾邮件）进行级别泛滥，从而被视为安全攻击：
恶意入侵计算机（与特洛伊木马一样，如下所述，
或公开），或拒绝服务攻击的反交互问题，这可以用来
防止任何互动或针对特定种类。[21]

即使用户与假定无害的网站进行通信，也总是存在
恶意行为的风险-经典的安全漏洞和攻击，欺骗和误导
用户，病毒和其他恶意代码以及其他陷阱的传播。[22] 经典结束
最终论点会说，每个最终节点都有责任保护自己不受攻击
其他（因此反病毒软件很受欢迎），但这可能还不够
在当今复杂的网络中进行控制。

一种典型的计算机安全攻击是所谓的特洛伊木马，其中
说服安装并使用某些软件，这些软件在表面上执行
任务，实际上是一个敌对代理，可以秘密导出私人信息或执行其他一些操作
某种秘密和不受欢迎的任务，影响接收者的系统和/或数据。不清楚
特洛伊木马程序实际成功完成严重安全漏洞的频率，但是
越来越多的人担心“信任”的浏览器可能对特洛伊木马视而不见。
通过与恶意软件设计的服务器软件进行交互而存放在最终系统上
意图。[23]

多路通讯

上面的示例全部在两方通信的框架中进行。但是很多
就像在现实世界中一样，互联网上发生的事情是多方的。任何公共或半公共
网络产品具有多向性。某些互动（例如当前的Web）使用
单独的两方通信的数量，作为实现
从服务器到多个用户的交互。其他电话会议或接收互联网-
基于广播的材料（音频或视频），也可能涉及
网络级别，通常称为多播。

使多路应用程序设计更加复杂的部分原因是，多端
点可能无法正常运行。不同的参与者可以选择在游戏中扮演不同的角色
多路交互，具有不同程度的信任，能力和可靠性。有些人想要
正确参与，但其他人可能试图破坏交流。有些可能

第9页

正确实施协议，而其他协议可能会崩溃或发生故障。这些现实必须在决定如何设计应用程序以及应将功能放在何处时应考虑在内位于。

通常，在两方交互中，如果一端似乎出现故障或恶意，则第一行辩护是终止互动并停止与该方通信。但是，在在多路通信中，一个坏掉的端点使整个过程停止是不可接受的相互作用。应用程序的设计必须使其能够区分可接受的和恶意流量并有选择地忽略后者。最终可能会这样做-节点，但在其他情况下（例如，网络被不必要的流量阻塞）阻止网络内部的某些流量是必需的。这将需要安装流量的能力网络内部的特定于源地址和应用程序类型以及多播目标地址。

总结-这些示例真正意味着什么？

这组示例旨在说明目标要素的丰富性。社会可能希望强加其基于网络的通信。存在或识别此类示例并不意味着所有这些目标都会被接受，并且反映在新的技术机制中（更不用说其优点了）。相反，它表明与使用简单示例来说明世界时相比，世界变得更加复杂阐明了端到端的论点。

这是否意味着我们必须放弃端到端的论点？不，不是的。什么是所需要的是一组相互协作的原则-有些原则是端到端的模型，以及一些关于以网络为中心的功能的新模型。在发展这套原则，重要的是要记住，从头到尾的争论围绕可以在端点正确实施的需求；如果网络内部的实现是满足要求的唯一方法，然后结束首先，end参数不合适。[24] 端到端参数不再存在通过对最终用户授权的信念来“验证”，而不是通过对用户授权的呼吁来“验证”。更复杂的高级功能目标组合。

技术回应

上一节对已要求的目标进行了分类（至少在某些情况下个季度）。这些目标有多种方式可能会遇到。在本节中，我们将研究已提出的技术对策和将它们分为大类。

端到端参数的不同形式

端到端参数适用于网络中的（至少）两个级别。一个版本适用于网络的核心，即路由器中实现的一部分互联网本身，提供基本的数据转发服务。另一个版本适用于应用程序设计。

有关网络核心的端到端论点认为，应该避免将特定于应用程序的功能“放入”网络，但应将其“向上和向外”推送到连接在网络上的设备。网络设计师之间有很强的区别两种元素-网络中的“元素”和“连接至”或“之上”的元素网络。网络中“设备”的故障可能会使网络崩溃，而不仅仅是确定

第10页

应用；它的影响更加普遍。因此，在此级别上的端到端参数指出网络中“服务”是不受欢迎的，因为它们会限制应用程序的行为并增加了核心的复杂性和风险。网络“上”并放入的服务满足应用程序需求的地方不是问题，因为它们的影响是较窄。

从核心网络的角度来看，连接到该网络的所有设备和服务网络代表端点。不管它们在哪里-在最终用户的站点，在Internet服务提供商的设施，等等。但是在设计每个应用程序时，可以使用端到端参数来确定应用程序级服务本身在哪里应该附上。一些应用程序具有非常简单的端到端结构，其中两端的计算机直接相互发送数据。其他应用程序可能会出现具有更复杂的结构，其中服务器将最终用户之间的数据流置于中间。例如，Internet中的电子邮件通常不会一步一步地从发送者流向接收者。而是，发件人将邮件存储在邮件服务器中，收件人随后将其提取。

修改终端节点

代表互联网根源最直接血统的方法是尝试结识新的通过修改端节点来实现目标。在某些情况下，将功能放置在网络可能会影响性能，但可以实现功能目标。如果垃圾邮件是在到达接收者之前或之后被删除，它同样被删除。主要的不同是资源的使用-网络容量和用户时间-以及成本的分配-交货前或交货后删除。换句话说，区别在于性能而不是动作的“正确性”。

在其他情况下，在终端节点中的实现可能不完善但可以接受解。使用互联网进行交易的税收[25]是一个可能的例子。考虑一个这种方法要求浏览器制造商修改其产品，以便他们识别并跟踪应税交易。尽管有些人可能会获得和使用经过修改的浏览器，会省略该步骤，那么在获取（或使用）此类程序时会遇到困难，尤其是散布（或使用）它是非法的。一种方法是评估实际违反税收要求的水平，判断水平损失的损失是可以接受的，并开发互补的机制（例如法律）以最大化遵守并控制损失。[26]正如我们在下面讨论的那样，认识到不同的终点在社会中扮演不同的角色（例如，公司与私人公民）可能使最终定位解决方案更加健壮和实用。

未成年人控制色情制品的访问是另一个问题的例子，这可能是根据结果是否足够可靠而在端点上解决问题。一个可以想象令人反感的材料以某种可靠的方式贴上标签，浏览器增强了检查这些标签并拒绝检索材料的能力，除非控制人员该计算机（可能是成人）已经对其进行了授权。或者，如果用户没有断言他或她是成人的凭据，连接另一端的服务器可以拒绝发送材料。[27]这样足够吗？一些未成年人可能会绕过浏览器。冒险的青少年一直绕过控制并使用不正确的方法（包括伪造或被盗的）身份证材料很长一段时间，很难保证使用给定终端系统的人就是他或她声称的那个人。这些结果代表系统泄漏，另一种情况是合规性小于100％。就是它结果可以接受，还是需要更强大的系统？

在其他情况下，依靠终端节点修改似乎没有任何结果。作为1990年代有关政府可访问的加密密钥的辩论表明，如果目标是窃听对于可疑的恐怖分子，没有办法强迫他们仅使用守法软件（端对端论点的说明，即端节点可以按照自己的意愿进行交易）。即使某些恐怖分子“明目张胆”地交流，也不能给人以太多安慰如果有一个加密的对话，特别是它想听的话，请联系执法部门上。

向网络核心添加功能

对某些新兴网络要求的审查导致了对新机制的呼声“在”网络中，在通过Internet转发数据包的路由器级别。这个结果是端到端参数的最明确的挑战，因为它将函数放入可能阻止某些应用程序实现的网络。

今天针对功能的争论之间存在重要区别网络和过去的争论。过去，网络级功能的典型建议目的是尝试帮助实现应用程序。现在，建议是可能充满敌意和乐于助人-增加了阻止事情发生的机制，阻止某些应用程序，依此类推。

这里有一些例子，今天这种方法已经被采用。其他的是考虑的。[28]

防火墙：当今，最明显的将节点插入Internet的例子是安全性防火墙，用于保护网络的某些部分（例如公司区域）免受其余部分的攻击互联网。防火墙检查正在通过的网络流量并拒绝怀疑的通信成为安全威胁。

流量过滤器：防火墙等元素可以执行除提供保护之外的任务来自外部安全攻击。它们可以双向影响流量，因此它们可以进行编程以防止使用某些应用程序（例如游戏）或访问不当内容资料（例如已知的色情网站）以及许多其他功能。流量过滤器因此可以成为控制网络使用的更通用工具。

网络地址转换元素：今天，称为网络地址转换的设备（NAT）盒正在Internet中使用，以处理Internet地址的短缺并简化地址空间管理。[29]通过修改数据包中的IP地址，它们可以有助于从其他端点保护用户身份。这些有时集成在具有防火墙功能-例如，作为其操作的一部分，它们可以限制应用程序的种类允许操作的。NAT盒通常由组织的经理安装网络和一些ISP。也有人建议在更大的范围内使用地址翻译。可能对整个国家/地区进行扩展，以控制进出该国家/地区的方式。

但是，NAT的部署需要在其他地方进行许多调整。原始设计互联网的原理是IP地址从源到端的端到端都保持不变整个网络上的目的地。通常在IP，TCP之上使用的下一层协议进行验证这个事实。随着NAT盒的引入，它可以改写进入数据包的IP地址或离开网络的某个区域，这些框还必须修改在TCP级别；否则，TCP错误检查将报告寻址错误。的更困难的问题是某些更高级别的协议（例如应用程序）也利用了IP地址；这意味着要使NAT盒保持正确的操作，它必须了解特定应用程序的设计，显然违反了端到端的论点。

最后，实践中还以其他方式使用了IP地址。例如，某些网站许可证软件使用客户端的IP地址来控制是否授予客户端访问服务器的权限。更改客户端的明显地址可能会导致这种方案出现故障。

网络核心添加机制中的设计问题

在网络“内”施加任何控制点都有两个问题。首先，数据必须通过设备进行路由，其次，设备必须具有一定的查看能力流中包含哪种信息，以便可以做出适当的处理决策。

将控制元素置于通信路径中

从源流向目的地的数据包可以在Internet上采用多种路径，因为最好的路由选项是在Internet运行时动态重新计算的。互联网上没有一个地方可以在未指定的位置插入控制点流。但是，对于已知流，具有给定源或目的地的情况，通常可以访问插入控制点的位置。对于大多数用户而言，通过单个访问Internet连接，并且控制点可以与该链接关联。公司或其他大型公司用户通常只有很少的路径将其连接到Internet的其余部分，并且这些路径提供了一种手段来获取来自该组织的流量。这是拓扑为组织提供安装防火墙的场所的功能。这条路的那一点连接到ISP同样提供了一种监控流量的方法。因此，政府可以通过指示ISP服务于用户安装控制点来实施窃听命令所涉党派与之相关的地方-曾经尝试过的方案。[30]

一旦流量进入公共互联网的内部，它将变得更加困难进行跟踪和监视。因此，为用户提供初始访问Internet的ISP将实务上，在任何强制性地将监控设备强加于用户。[31] 随着政府对通过Internet传输的内容越来越感兴趣，我们可以期望为用户提供Internet接入点的ISP将具有吸引力向政府作为实施与公众相关的某些控制措施的工具政策目标。[32]

显示或隐藏消息的内容

假设已经解决了网络路由问题，并且要监视的流量是通过控制点，另一个问题是信息的哪些方面对控制设备。有多种选择，从完全可见到完全掩盖。一种端到端参数的简单应用将指出发送方和接收方是免费的选择最适合他们需要的沟通方式。特别是，他们应该可以自由使用私有格式，加密他们的通信或使用他们的任何方式选择将它们保密。对于那些想要加密的人来说，加密可能是最强大的工具保护他们的消息不被观察或修改。正确进行强加密时实施后，控制设备只能查看源IP地址和目标IP地址，并且包头中的其他控制字段。如上所述，流量分析是唯一的在这种情况下可以进行分析。

端到端隐私的目标与任何期望的第三方的目标直接冲突根据流的内容采取一些措施。目标是否是向电子商务征税交易，收取受版权保护的音乐表演的费用或过滤出令人反感的内容物质，如果内容的本质被完全隐藏，则中间节点很少除了共同阻止通信之外，还可以做到。这种情况可能导致

要求设备能够看到和识别完整信息。要么
在特定情况下，可能需要完全保密或完全公开内容的结果，但这是
有助于发现可能的妥协。

信息标签

一种在不透露邮件内容的情况下透露一些有关邮件内容的信息的方法
内容本身就是标记消息。在网络中可见的标签代表
最终节点方传输任何内容的权利之间可能存在一种折衷
想要（可能出于隐私保护而加密）以及某些第三方观察或采取行动的权利
已发送。标签还代表一种增加消息中实际信息的方法，例如
该示例将内容类型的简单框架强加到任意应用程序数据上。对于
例如，可以使用简单的标签“广告”来描述各种各样的消息。
加利福尼亚州的法律要求，所有不请自来的广告电子邮件都必须在广告开头添加“ ADV：”
主题。[33] 标签的潜在用途具有重要的二重性：它们可以用来
识别内容和用户。例如，色情材料的转移可能是
要求标记为“对未成年人不利”，而对该材料的要求可能会
附有要求的人的标签。使用哪种方案可能取决于在哪里
信任在于，谁可以负责。[34] 几乎有必要，这样的标签方案将
被批评缺乏普遍性和表现力，并以某种方式限制了各方，
特别是对于超越事实的品质。标签给内容带来负担
生产者或另一方要贴上准确的标签，问题就变成了
要求是可执行的。[35]

实际上，标签在美国商业广告中可能会变得司空见惯
通讯，随着联邦贸易委员会采取行动扩大做法和政策
与防止传统媒体中的欺骗有关（这导致了
例如，将广告贴在互联网上）。[36] 另外，数据标签是关键
许多过滤方案的基本组成部分，它允许在内部和外部进行过滤
网络的边缘。

标记方案回避了构建可以
分析消息并找出含义。可以想象写一个看起来像的程序
在邮件正文中得出结论，这是批量广告，或者在查看图片时得出结论，
他们令人反感，或查看网络传输并得出结论，这是在线购买。
尽管正在推行此类计划的概念，但它们却提出了许多麻烦的问题，
从此类控制的可靠性到在决策中进行决策的可接受性
首先是程序的形式

有一些关于将标签用作内容范围中间点的建议
能见度，尽管今天在实践中很少使用。较明显的标签方案之一
当今的Internet是内容的Internet内容选择平台（PICS）标准
标签，[37] 由万维网联盟开发的一种方法
识别可能令人反感的材料。PICS标准是一种强大的方法
内容标记，因为它允许第三方以及内容标记内容
生产者。这种通用性允许具有不同目标和价值观的内容的不同用户
订阅符合其需求的标签服务。标签未按原样粘贴到页面上
跨网络传输，但基于页面从标签服务中检索
正在获取。可以在终端节点（端到端解决方案）中或在
应用程序级中继，特别是Web代理服务器（网络内解决方案）。[38] 当PICS
具有许多有趣和有用的功能，也引起了批评，尤其是在声音上

对PICS标签的“自愿”性质在实践中可能成为强制性的担忧在政府压力下。因此，PICS可能最终会成为政府审查的工具。[39] 这个这种担忧似乎适用于在网络中可以观察到的任何标签方案。标签方案不应被视为解决所有内容问题的灵丹妙药，但它们只是中间点在缺乏对所携带物品的任何可见性与明确审查之间的范围内内容的规定。

如今，内容标签的另一个示例是在网页上找到的元数据标签。[40] 这些被用来帮助指导搜索引擎进行页面分类。元数据标签可以包括实际上没有出现在页面可见部分的关键字；此功能可以要么用于解决特定的编目问题，要么将页面提升到列表的顶部搜索结果。截至今天，这些标签已不再用于网络内部的控制，而仅用于查找，它们说明了使用标签的一些问题。[41]

当今的Internet在大多数通信中都提供了最小的标签，即所谓的“端口数字”，它标识了消息打算在端点使用哪个应用程序-Web，电子邮件，文件传输等。这些数字可用于粗略地对数据包进行分类，并且如今，已以多种方式使用此功能。ISP和机构网络经理观察端口号以建立用户行为模型以预测需求变化。在某些情况下，他们还根据服务合同拒绝往来于某些端口号的流量与用户。一些应用程序开发人员已通过远离可预测的方式做出回应端口号。

应用程序设计-更高级别的端到端参数

前面的讨论涉及使用新的网络扩展来增强网络核心功能，在当前世界中，与控制和过滤相比，它更关注的是增强应用程序。现在我们来看一下应用程序本身的设计。那里有两个今天可以确定的趋势。一个是不同政党的愿望，要么是用户或网络运营商，以将某种服务器插入应用程序的数据路径中，最初不是使用这种结构设计的。这种愿望可能源于各种各样的目标隐私和性能增强。另一个趋势是应用程序要求变得越来越复杂，有时会导致从简单的端到端设计和使用附加组件作为应用程序的一部分。

以下是一些当今正在采用的应用程序级服务的示例增强或修改应用程序行为。

匿名消息转发器：用户实现匿名并实现匿名的一种策略保护他们的通讯不受第三方观察是使用第三方服务，并且通过它路由流量，以便可以删除消息中可能的标识。服务使得Web浏览匿名化的流行今天，[42] 和服务的特定目标可以进行流量分析。[43] 非一致的邮件中继包括简单的邮件转发器和更复杂的系统，例如nym服务器。[44] 要使用这些设备，端节点构造通过其中一个（或通常多个）以实现所需功能的路线。至关重要的是用户构造路线，因为保留匿名性取决于路径后的数据在只有用户知道的盒子中；例如，ISP或任何其他第三方应无法直接确定路径。在这些情况下，请谨慎使用加密计划隐藏路线和身份以防止不必要的观察。[45]

有用的内容过滤：原则上，当今使用的邮件服务器可用于执行邮件过滤和相关处理。由于邮件还是通过这些设备路由的，

第15章

服务器过滤提供了一个选项，可以在垃圾邮件或其他有害材料之前将其删除

甚至转移到接收主机。[46] 可以通过多种方式来进行过滤上面讨论的内容访问范围：查看邮件上的标签，匹配发件人针对可接受的通讯录的列表，或处理邮件的内容（例如，检测病毒）。

内容缓存：万维网，也许是最常见的Internet应用程序今天，最初设计时具有简单的两方端到端结构。但是，如果大量用户获取相同的流行网页，原始设计暗示该网页将一遍又一遍地从服务器中获取，并在网络。这种观察结果提出了这样的建议：当页面从服务器发送到用户，将复制并“缓存”在用户附近的某个位置，以便如果附近的用户请求第二次翻页时，可以使用缓存的副本满足此后续请求。这样做可能会提供一些显着的性能优势，但它确实打破了端到端的本质网络；例如，服务器不再能够告知其页面已被检索多少次，服务器也不能执行用户特定的操作，例如广告放置。[47]

使用受信任的第三方进行更复杂的应用程序设计

如今，应用程序设计中的许多问题都以某种方式源于应用程序之间的不信任。参与该应用程序的用户。一种基本方法是使用相互信任的第三方一方位于网络上某个地方以创建上下文，在该上下文中，两方交易可以成功进行。[48] 换句话说，本来可以是简单的两方以直接方式符合端到端参数的事务成为三方或更多方之间的互动顺序。每次交互都名义上结束终端（这些第三方不必“在”网络中），但其健壮性取决于更大的上下文由整个序列组成。

受信任的第三方可能会做的一些简单示例包括签名和日期戳消息的数量（即使消息是加密的，独立的签名也可以提供保护某种形式的抵赖）或确保将消息同时发布到多个派对。[49] 另一类受信任的第三方将实际检查消息的内容，并验证交易形式是否正确。这个角色有点类似于公证人的角色上市。[50]

第三方的另一个作用是提供凭据，以便为交易中的每一方提供对另一方的身份，角色或可信度有更多的保证。例子包括选民登记，多数票证明（例如，允许访问被认为是对未成年人有害）等等。第三方的作用与内容的标签和用户。可能是第三方是用于对材料进行分类的标签的来源，例如上面在PICS中讨论的内容。除了凭证以外，还有其他形式的令牌描述可以事先获得的用户和内容。例如匿名电子来自受信任的第三方（类似于银行）的现金提供了一个上下文，其中两方可以进行匿名买卖。

公钥证书

当用户使用公钥密码术时，对第三方的重要作用就会发生身份验证和受保护的通信。用户可以创建一个公钥并将其提供给其他人，以便以受保护的方式与该用户通信。基于良好的交易-已知的公钥可以是非常简单的两方交互，非常适合端到端范例。但是，第三方有一个关键角色，即发布公共密钥

第16页

证明书并管理此类证明书的库存；这样的各方称为证书当局。该证书是（可能值得信赖的）第三方的断言，即

指示的公共密钥实际上与特定用户一起使用。这些证书是主要的基本上是所有公钥方案的组成部分，但规模太小以至于用户可以以一种特殊的方式，将他们的公钥彼此一对一地通信互信。

获取证书的步骤可以提前完成。在大多数方案中，交易后必须执行的步骤；这一步在实践中是棘手的。用户可能会发生由于疏忽而丢失了他的私钥（与给定公钥对应的值）或盗窃; 替代地，用户可能以某种与之相关的目的变得不值得证书已颁发。在这种情况下，证书颁发机构（第三方）想要撤销证书。如何得知？显而易见（且成本高昂）方法是让遇到公共密钥证书的任何一方联系第三方发布它来询问它是否仍然有效。尽管这种互动通常在电子信用卡授权，更多使用证书和更多用户的潜力给认证机构带来巨大的性能负担的风险，因为这会最终每次名义上使用两方证书时都会收到查询交易，以及导致撤销的事件序列存在固有的滞后。结果，复杂度可能远远超过与无效相关的复杂度今天的信用卡授权。已经提出了改善性能的建议撤销过程的含义，其细节无关紧要。但总的来说出现：要么是公钥证书的接收者都在“实时”检查过程中，与与该密钥关联的一方进行交易的过程，或者完成交易然后稍后验证相关方的身份，并确保交易已经完成是不合适的。[51]

通常，在涉及多方的复杂交易中，存在一个与各方采取各种行动的时机。选民登记在以下时间不发生投票，但要提前。但是，除非进行定期检查，否则您会发现已故的选民仍在投票，以及刚刚离开城镇并登记的选民别处。页面的PICS评分必须事先完成。即使PICS等级为检索页面时进行实时检查，评分本身可能已过时，因为页面内容已更改。通常似乎适用的概括是，与第三方之间的初步或后续互动之间的时间差交易本身，第三方扮演的角色可靠性降低的风险就越大。

更大的背景

重要的是要考虑存在这些技术机制的更大范围。那背景包括经济的法律和社会结构，增长动力可信赖度，以及技术，法律，社会规范和市场共同实现的事实各方之间的力量平衡。

非技术解决方案：法律在网络空间中的作用

仅仅因为在诸如Internet之类的技术系统的上下文中出现问题，并不是解决方案只能是技术性的。[52] 实际上，使用法律和其他非技术性可以认为这些机制与最高级别的端到端争论相一致，功能不仅从网络核心而且从应用程序“移出”以及位于网络外部的所有层。

第17页

例如，控制不必要的材料向传真机的传送（传真中的垃圾邮件世界上有一些法律禁止某些未经请求的传真传输，并要求发送传真机附上其电话号码，以便可以识别发件人。[53] 同样，

基于计算机的犯罪的增长已导致将某些互联网行为定为犯罪：1987年《计算机安全法》的重点是“联邦利益”计算机，在此感谢部分原因是Internet的广泛使用以及相关的计算机趋势通过网络，在整个1990年代，越来越多的执法机构关注，立法，与私人和公共部门滥用计算机有关。[54]

标签计划的泛滥表明技术和法律之间的相互作用方法。网络可以检查标签，但可以强制执行标签正确的操作属于法律领域。[55] 当然，在各种保护消费者的情况下，公共安全情况；例如，联邦贸易委员会对广告进行监管-包括声明和认可-以通常会影响内容和格式的方式进行，并且开始研究有关在线隐私保护的法规的必要性，而证券交易委员会负责监管财务索赔，而食品药品政府管理与食品，药品和医疗设备有关的索赔。美国联邦贸易委员会其他人则认为标签是一种不完善的机制，因为人们可能会忽略它们，它们可能不适用于外国资源，并且受美国法律约束声明为强制性发言，但标签对市场的干扰要小于例如彻底禁止引起政策关注的产品。

迄今为止，在互联网上，执法还不太正式。情况也一样行业自愿采取的行动可能会导致标签内容的“自我监管”，旨在避免或阻止政府监管；电影，电视节目的内容分级（现在与V芯片相关联[56]），而计算机游戏提供了吸引了公众和政府审查；更多的创业例子包括质量标签更好的商业局网站的兴起以及为这个目的。在其他情况下，可能会引起更普遍的警惕：因为每日新闻在对公司滥用个人信息（例如，Amazon.com，RealNetworks或DoubleClick），[57] 公众审查和关注本身可以具有影响。[58] 总体而言，网络之外的机制，例如法律，法规或社会压力，限制原来是不可信任的第三方，最后是用来保护自己的第三方的系统身份不如承诺的好，等等。非技术人员的满意度如何机制可能取决于人们对政府角色的期望（例如，如何家长式的），行业的角色（例如，如何剥削或如何负责）以及能力和个人愿意了解情况并采取自己的防御行动的意愿（在这种情况下，隐私和安全方面的问题）或负责任地（在税收等方面）。[59]

在技术和法律方法之间存在着哲学上的区别在这里讨论。技术机制的特征是其行为是可预测*的先验的*。可以检查一下机制，说服自己做什么，然后再依靠它按照说明工作。另一方面，法律机制常常在事实发生后起作用。一种当事人可以诉诸法院（一种第三方），并且由于法院命令或禁令而达到更改; 当然，法律机制的存在通常与期望有关威慑力。

例如，上面引用的nym服务器通过以下方式解决了电子邮件匿名性问题技术手段。通过创造性地使用加密，通过通信谨慎地路由数据应用程序，并且没有日志记录，因此事后确定几乎是不可能的发送消息的人。[60] 结果（在设计师看来是有益的）是，人们可以使用nym服务器充满信心，以后无论是“好人”还是“坏人”都无法进入

第18页

并强行揭示身份。缺点是“坏蛋”可能会使用匿名者做的事情真的很糟糕，足以使观点平衡趋向于应对和不惜一切代价保护匿名。在这种情况下，社会是否希望采取补救措施？

在哲学层面上，辩论本身代表着寻找正确权利的重要部分
平衡。但是目前，互联网是一个系统，其中技术而不是法律是
强迫最直接的塑造行为，直到法律环境成熟，
在网络空间采取行动后，采取补救措施的可能性要比在现实空间中要少。[61]

有人认为，法律在影响基于互联网的行为方面的价值有限，因为
互联网是跨境的，来源和目的地可能在不可预测的管辖范围内，和/或
来源和目的地可以位于具有不同法律体系的司法管辖区中。这个论点
鼓励那些需要技术控制的人（他们只是按照他们的工作方式工作，
独立于司法管辖区，因此对特定司法管辖区的满意度不同
当局），以及主张私人，基于群体的自我监管的用户，其中用户群体
通过选择同意一种方法（例如，使用PICS）以创建共享上下文，
可以起作用。由于私有的，基于群体的监管的局限性，各种
监管机构正在研究与经营活动有关的各种条件。
互联网和干预措施的权重选择，进而激发人们进行自我干预的新尝试
可能会或可能不会生效或接受的法规。同时，法律解决方案正在
积极探索。[62]

评估我们今天的位置

如导言所述，当今有许多力量在推动改变互联网：
呼叫（来自各种声音）以确保稳定可靠的运行，即使我们对信任的信任度降低
网络的个人用户；新愿景驱动的新型复杂应用程序
以消费者为导向的经验；互联网服务提供商发展成包含
增强服务以获得竞争优势；范围广泛的第三方扩散
对用户实际所做的事情感兴趣；不太熟练的用户的扩散
谁的“创新”是喜忧参半；以及新形式的计算和通信
需要新的软件结构。所有这些力量都有增加后果
复杂性，互联网设计中结构的增加以及互联网失去控制
用户。是否选择将这些趋势视为互联网成长的自然组成部分
或西方的栅栏，它们正在发生。无法将时钟调回原点
早期互联网的情况：真正的变化强调了有关
互联网的持久性设计原则和假设。

新玩家的崛起

当今互联网的许多不同之处都可以追溯到
在过去的十年中进入了游戏。互联网的商业阶段确实少于
十岁了-NSFnet，由政府资助的骨干网络，早在
1980年代，直到1995年才关闭。当时，商业ISP开始
数量激增，玩家数量非常少，而且他们的角色相当简单。

自那时以来，世界变得更加复杂。一种趋势是显而易见的：
政府在互联网中角色的转变。推动者的历史性角色正在消亡。
相对而言，政府对互联网设计和运营的贡献
缩水了。[63] 同时，随着越来越多的公民开始使用互联网和
依靠它，政府对互联网业务的性质和消费者问题的关注已经
长大的。即使有些人遗憾地看到了这一趋势，也很容易预测到。实际上，

18岁

第19话

政府的行为与其他部门的政府活动以及
常规电信的历史，包括电话和广播媒体：
反托拉斯警戒，试图控制消费者欺诈行为，商业法规的定义，税收，
等等。政府几乎没有做任何代表新角色的事情。在里面

联邦通信委员会（Federal Communications Commission），处理自然垄断和
驻扎在政府内部的专门的法律和专门机构
通过将法律转化为法规并参与法规执行来解决频谱稀缺问题。在
在美国，政府在很大程度上避免将这些工具用于
互联网，但这样做的潜力已得到广泛认可（尤其是由于对互联网的审查
并购对互联网的发展有影响）
球员的行为。

通配符一直是ISP的发展。它的作用不太明确，预定义也不太清楚
而不是政府，它已经发展并变得更加复杂。政府
在1990年代初认识到私营部门将建立国家（最终是全球）
信息基础架构，以及因骨干网商业化而产生的淘金热
使ISP业务与许多其他业务相似，而ISP则寻求最有利可图的手段来
定义并开展业务。ISP为增强其作用而采取的任何措施
除了基本的数据包转发外，它不太可能与端到端思维兼容，因为
ISP无法控制端点。ISP实现了网络的核心，并且
终端软件通常来自其他提供商。[64] 因此，ISP最有可能
通过修改其控制的网络部分来添加服务和约束。例如，
一些居民用户发现自己无法在他们的网站上运行Web或游戏服务器
家。[65]岁这些服务仅限于支付较高费用的商业客户
互联网。从一个角度看，这种服务分层是自然而然的：
私有企业的性质，将用户分成具有不同利益和价格的不同层次
他们相应地。在周六晚上陪同此人时以全价乘飞机的人
停留一小部分费用就能了解基于价值的定价。还有一些
互联网观察者从道德上考虑了将这些限制应用于互联网服务时
错误。从这个角度来看，互联网应该是用户应该使用的一种工具。
能够做任何他想做的事情，端到端。作为一个社会，在整个社会中
世界上，我们尚未开始解决这种紧张局势。

在不受限制的商业世界中，对Internet服务最终形式的担忧是
行业整合加剧了这种情况，这引起了人们对当地充分竞争的担忧
访问（以ATT对TCI和MediaOne的收购为标志）以及之间的合并
互联网访问提供商和互联网内容提供商（以AOL拟议的收购为标志）
时代华纳，包括其所有有线设施）。[66] 一个相关的问题是“开放获取”辩论，
这关系到是否应迫使ISP共享其设施。不用担心
只是ISP中的选择，但是如果对替代ISP的访问受到限制或阻止，则
用户将根本无法访问某些内容。因此，有一个
假定在无法访问Internet和失去开放性
互联网的终结性质。[67]

随着越来越多的消费者加入互联网，他们已经非常重视
不同的经历。在充满竞争的拨号上网世界中，公司
占据美国消费者主要份额的是美国在线（AOL）。一个人可以推测
通过查看AOL提供的内容，了解消费者喜欢的各种体验。的
AOL的重点在于减少对任何活动和目的地的开放和平等访问（最终目的是什么）
结束争论将需要），以及有关打包内容的更多信息（由预期的内容加强）
（与时代华纳合并），可预测的编辑以及对不良影响的控制。其

第20话

订户数量的增长证明了消费者对其提供的服务以及
他们提供的相对易用性。那些要求一种或另一种互联网作为
集体社会目标至少会很好地从消费者的声音中吸取教训
到目前为止听到的。

关于ISP的法律待遇出现了新的问题。ISP的兴起和

历史悠久的电话公司，广播公司以及最近的转型
有线电视提供商在放松经济的广泛目标之间造成了新的紧张关系。
监管—目的在于促进竞争以及随之而来的消费者利益，例如
较低的价格和产品创新-以及对产品不断演变的结构和行为的担忧
新兴的通信服务领导者-影响价格的实际经验的因素
和创新。尽管美国联邦电信监管机构已回避
正在讨论的“互联网监管”主题包括共同的法律概念
适用于电话服务提供商的运输应适用于ISP。[68] 今天的立法
和监管查询提出了ISP业务是否应继续发展的问题
靠互联网本身—将互联网转变为公共基础设施是否需要一些
一种干预。[69]

互联网服务的机构提供商-公司，学校和非营利组织
运营部分Internet的组织-还发展了一套更为复杂的
角色。员工因不当使用公司附件而被解雇
互联网，有时雇主比ISP的限制要严格得多。
他们削减的服务以及为可接受的使用而制定的规则。当今的互联网用户
不一定能按照他的意愿去做：他可以在不同的地方做不同的事情
互联网，也许是一天中的不同时间。

最后，绝对不能忽视互联网的国际性。作为互联网
在其他国家迅速兴起和发展，文化差异
在不同地方将是影响互联网整体状况的主要因素。在一些
国家/地区，ISP可能与政府是同一件事，或者政府可能会强加
ISP上的操作规则与我们在美国所期望的完全不同

信任的侵蚀

本文中的许多示例说明了不完全信任彼此的用户
其他仍然渴望交流。在改变互联网的所有变化中，
年 信任可能是最根本的。ISP提供的服务的确切详细信息可能会更改
随着时间的流逝，消费者的压力或法律可能会逆转它们。但是简单的模型
早期的Internet（连接到透明网络的一组相互信任的用户）已经消失了
永远。要了解互联网的变化方式，我们必须拥有更完善的
考虑信任及其与其他因素（如隐私，开放性和实用性）的关系。

互联网在越来越多的经济和社会活动领域中的传播
建议在信任方和非信任方之间使用它的情况都有所增加。结果正在增长
个人对自我保护的兴趣，这可能涉及主动或被动地第三
派对。在这种背景下，一些特定的第三方开始关注自己的问题
目标，例如资产保护，收入来源或某种形式的公共安全。那是，
可信度既可以自我保护（可能是端到端），也可以激发第三方的积极性
干预（似乎挑战了端到端原则）。

随着信任的侵蚀，端点和第三方都可能希望插入中间元素
进行沟通以实现他们的验证和控制目标。中级
元素实时地插入在通信双方之间，

第21话

设备需要检查（至少部分）数据流以及用户的增长趋势
及其软件对通信流进行加密以确保数据完整性和控制
不必要的披露。如果流已加密，则无法对其进行检查；如果已签名，则不能
改变了。从历史上看，用于完整性保护的加密更容易被以下方面接受：
有关加密的当局比考虑加密的机密性高，但这可能也太过分了
glib在普遍加密的世界中的一个假设，其中个人可能会遇到

加密不是信任的替代品，例如，表现谨慎
的个人开会
在公共场所，或与其他各方一起听，等等。进行加密对话
和一个陌生人在一起可能就像在黑暗的小巷里遇到那个人。无论发生什么，都没有
目击者。明确的通信可以允许插入的网络元素来处理
流，这对于交互的安全性至关重要。这个例子
个人可能选择权衡隐私权以换取其他价值的情况说明了
主张在隐私，安全性和其他因素之间进行选择和权衡
变得更加复杂。

同时，有很多事务可以将端点集合视为
私人，即使他们之间没有完全信任。在在线购买中，诸如
价格或信用卡号可能应受到外部观察的保护，但事实是
购买可能是记录问题，如果另一方提供了追索的依据
行为不端。这种情况可能会导致选择使用加密，而不是总加密
IP级别上的数据流（如IPsec提议中），但有选择地应用，例如
由浏览器发送到消息的不同部分。IPsec的使用最自然地适用于
信任度最高的各方之间的通信，因为此方案可以保护
来自观察的最大信息量。

在网络中使用受信任的第三方增加了如何知道的困难
第三方实际上是值得信赖的，或者端点正在与第三方对话
认为他们是。如果恶意的“模仿”第三方设法将自己插入
受信任的代理商的位置？如今，网站尝试使用类似于
受人尊敬的。互联网用户如何才能确信站点在物理上
远程，只有通过他们的网络行为才能看到，实际上是他们声称的，实际上是
值得信任吗？ [70]

权利与责任

法律活动的兴起反映了围绕相对权力（或
相对权利或相对责任）作为个人最终用户和
网络作为公共物品的代理（例如，状态，给定服务的用户组
网络）。其中一些辩论源于一个国家或州的法律，有些则源于价值体系
和意识形态。美国宪法第一修正案对
言论自由；其他国家有不同的规范和法律传统。同样，社会
它们在定义问责制以及如何在匿名之间取得平衡方面将有所不同
和问责制。根据不同的国家背景，不同的地理区域
可以管理网络以实现不同的功率平衡， [71] 乌斯季不同
组织对网络用户施加不同的策略。本地控制可能是
并不完美，但是塑造本地体验并不一定是完美的。但是如果互联网要
作为互联网工作，不同地区之间的差异有一定的局限性。

Internet的端到端设计为用户提供了确定什么功能的强大功能。
他选择使用的应用程序。这种力量增加了用户之间进行军备竞赛的可能性

第22话

和那些希望控制它们的人。这个潜力应该是一个发人深省的想法，因为它
会有相当破坏性的副作用。密码政策辩论认为，如果
例如，控件被放置在网络中，试图拦截和读取私有
各方之间的通信，用户的响应很容易就是加密他们的
私人通讯。对此的回应要么是禁止使用加密，要么
推广政府可访问的密钥，或阻止传输任何不能通过
识别，这又可能导致隐藏在其他消息（隐写术）中的消息。

如果实际上控制通话越来越难在试图规范隐私通讯严重损失，受影响个人的特权。[72] 这些控件还可以阻止部署任何新应用程序，并扼杀创新和创造力。考虑一下如果必须获得部署新应用程序的许可证，Internet可能看起来像今天。这样的升级是不可取的。

权利和责任之间最关键的紧张关系可能是信任的侵蚀-匿名与问责制之间的平衡。端到端论点的性质表明，端点可以根据需要进行交流，而无需来自网络的约束。一方面，这意味着对问责制的一定需求，这些无节制的活动竟然造成了伤害。任何系统，无论是技术或社会，要求采取保护措施以免发生不负责任和有害的行为。端到端的论点不要暗示护栏以保持使用者在路上。另一方面，有人呼吁匿名行动的权利，以及某些匿名行动（例如美国）是受保护的权利。当然，即使不是绝对匿名，隐私也非常重要-在许多社会都尊重目标。那么对隐私和匿名的渴望又如何呢？考虑到端到端的行动自由，平衡了对问责制的需求论点暗示？这将是未来十年的关键问题。

前进中的一个实际问题是政策的可执行性。一些在实施方面，沟通以及某些类型的各方更容易处理控制（或在关注的人的眼中避免需要控制的行为）。对于例如，经常会出现一个区别：私人与公共之间的分离通讯。如今，Internet对两个同意的终端节点在通过网络通信。他们可以发送加密的消息，设计全新的应用程序等。这与端到端的简单表达是一致的论点。这种交流是*私人的*。相比之下，*公共*传播或*向公众*传播，具有不同的技术和社会特征。

- =为了吸引公众，必须做广告。
- =为了获得公众的认可，必须使用众所周知的协议和标准。公众有空。
- =为了使公众了解，必须公开自己的内容。没有这样的事情公共秘密。
- =为了达到公众地位，必须接受一个人可能会受到公众的监督。当局。

这些因素使公共传播比私人传播更容易控制交流，特别是在公共交流是商业演讲的地方（程度有限，至少在美国，比非商业性适用更多的规则言语）。如果标签上的信息已经过加密，则当局可能不会能够验证每个标签是否正确。但是当局可以检查发件人是否

第23话

通过成为服务的订户来计算适当的标签，看看发送的信息是否是正确标记。[73]

支持执法的另一种沟通方式是在个人与公认的机构。在许多情况下，转移的一端或另一端可能更容易握住负责任的，要么是因为它在特定的管辖范围内，要么是因为它属于另一类机构。例如，可能更容易识别公司并向其施加要求和其他业务相比，个人而言。因此，在客户与客户之间的交易中银行，可能比客户更容易对银行实施强制性监管。银行是

经久不衰的机构，已经受到大量的监管和审计，而个人
客户的约束较少。这可能会导致银行成为银行的一部分的情况。
执法方案。同样，内容提供商，如果他们打算提供该内容
对公众而言，在市场上必须比个人客户更容易识别，并且
这样一来，执法机构及其所需的客户就可以看到它们。即使
从内容提供商处进行的每次转移都无法检查其正确行为，
当局可以通过成为客户来进行抽查。如果处罚为非
符合性很强，可能无需验证每次转帐的准确性
达到合理的合规性。[74] 认识并利用这些不同的角色
机构和个人可以提高最终定位应用程序和最终应用程序的可行性
通常结束方法。

结论

端到端参数的最重要好处是它们保留了灵活性，
互联网的普遍性和开放性。它们允许引入新的应用程序；他们
从而促进创新，并带来随之而来的社会和经济利益。运动更多
网络内部的功能危及通用性和灵活性以及历史模式
创新。一个显而易见的新原理是，实现以下功能的元素
通常，对端到端应用程序不可见或有害的应用程序必须位于网络中，因为
不能期望应用程序自愿包含该中间元素。

多种力量似乎促进了互联网内部的变化，这可能与
端到端的论点。尽管有些人对此表示关注。
政府越来越多的参与，ISP可能会给政府带来更大的挑战。
互联网的传统结构。ISP实施网络的核心，以及任何
ISP实施的增强或限制措施可能会作为新机制出现在
网络的核心。作为通往客户的门户，它们是其他人固有的焦点
也对客户的行为感兴趣。

用户基础的不断变化正在将互联网推向新的方向，为
ISP和政府的努力。问题在于拥有的端点软件的数量以及
如果不了解，则由消费者操作，因此，Internet系统在
大继续支持端到端的哲学。最初的互联网用户是
技术上的，并且受益于端到端方法的灵活性和授权，
当今的消费者像其他消费电子产品一样接触互联网和系统，
服务。低廉的价格和易用性比以往任何时候都变得越来越重要，这表明它正在增长
捆绑式和托管式产品对自己动手技术的吸引力。减少工作
消费者可能暗示他们对互联网上可以做什么以及谁可以观察到的内容的控制较少
他们做什么; 然而，关于在线隐私的初期争议表明，
限制了许多消费者出于各种原因将放弃的权利。

第24话

在改变互联网的所有变化中，信任的丧失可能是最严重的
基本的。早期Internet的简单模型-一组相互信任的用户
到透明的网络-永远消失了。明天的座右铭很可能是“全球
与当地信任的交流。” 信任问题出现在多个层次：Internet访问范围内
（例如浏览器）和应用程序软件（其中一些可能会触发Internet访问）
在以下通信中访问远程站点上的内容或进行交易的活动
在ISP运营的接入网络范围内，与陌生人有各种各样的联系，
雇主等-经营者寻求在许可的情况下遵守自己的目标
其他人使用他们的网络。对信任的日益关注给传统互联网带来压力

来自网络限制到端的论点就其本质而言表明可以根据需要进行交流文化的匿名性在许多情况下都得到重视。社会使用的增长和对社会的依赖但是，互联网引发了对问责制的呼吁（本身含义各异），带来了压力限制端点可能发生的事情或跟踪行为（可能来自内部）网络。在某些情况下可以支持信任的步骤是对内容。正如正在进行的实验所表明的那样，标记可能有助于保护隐私，在保留端到端的同时避免令人反感的材料和匿名性交流，但它们仍然构成重大的技术和法律挑战。

更复杂的应用程序要求导致依赖于应用程序的设计在受信任的第三方之间进行调解，以最终用户之间进行调解，端到端通信分为一系列组件端到端通信。虽然这种方法可以帮助不完全信任彼此的用户进行值得信赖的交互，它会添加自己的交互信任问题：如何知道第三方本身确实值得信任，或者端点正在与他们以为是第三方进行对话？这些并不需要太多意识到解决Internet信任问题将涉及的不仅仅是技术，而且政府的查询和计划行动的泛滥，加上各种法律这些行为相结合会冲击互联网及其用户。

如果开放和透明，很可能会扼杀某些类型的创新互联网的性质正在受到侵蚀。如今，没有证据表明创新已被抑制总体。新的互联网公司的投资水平和新产品的范围消费者，从电子商务到在线音乐，都证明了不断发展的健康互联网。但是创新的性质可能已经改变。它不再是单个广告素材车库里的人，但有千万美元支持的创业公司正在做革新。端到端的论点可能偏爱小型创新者，而内容服务器和ISP控制哪些服务可以和不能以什么方式使用，这是对小型创新者的障碍，但对于资金雄厚的企业而言，作为启动新服务的一部分可以解决所有这些问题的创新者。所以趋势明天可能不是缓慢创新的简单原因之一，而是更为微妙的创新之一由更大的玩家提供更多的资金支持。

端到端争论进而对灵活性的最阴险的威胁是，商业投资将转移到其他地方，以支持由不是端到端而是基于“内部”特定于应用程序的服务器和服务的解决方案网络。内容镜像，可将内容副本定位在用户附近，以实现快速，高性能交付，便于交付特定物料，但只有物料被镜像。对内容复制的依赖性越来越大，可能会减少对目的升级到Internet容量。我们可能会看到，而不是突然的变化互联网的精神，但形式和功能僵化了。及时一些新的网络可能会作为Internet上的覆盖层出现，试图重新引入上下文

24

第25话

不受约束的创新。互联网就像之前的电话系统一样，可以成为后续系统的基础架构。

我们对技术对未来施加的限制作了两幅画互联网。一是技术解决方案既固定又僵化。他们实施了一些给定的功能，并且完全独立于本地需求和要求。他们制造出黑色选择替代方案的结果。存在匿名服务，或者确实存在不。另一方面，我们观察到在实践中谁会施加控制，谁会逃避控制。两者之间有争斗垃圾邮件发送者和控制者，需要知道谁买家和使用无法追踪的电子邮件地址的买家，以及希望

限制访问某些内容以及尝试访问这些内容的人。这种模式表明平衡
玩家之间的力量并不是赢家通吃的结果，而是不断发展的平衡。它
这表明结果不是由特定的技术替代方法决定的，而是结果的相互作用。
这个非常复杂的系统的许多功能和特性。这表明它为时过早
预测最终形式。我们现在所能做的就是以倾向于某些结果的方式推动。
我们认为，网络的开放性，普遍性是源于端到端争论的结果，
是鼓励创新的宝贵特征，应保留这种灵活性。

1克拉克的研究得到了国防高级研究计划局的支持，合同号为N6601-98-8903，并且
由MIT Internet Telecomms Convergence Consortium的工业合作伙伴提供。Blumenthal是该综合大楼的员工
摘自美国国家科学院，1998年撰写本文时也是麻省理工学院的一名员工。的
本文包含的观点和结论是作者的观点和结论，不应解释为必然代表
DARPA，美国政府或美国国家科学院的官方政策或明示或暗示的认可。

2参见J. Saltzer，D。Reed和DD Clark。1984年。“系统设计中的端到端参数”。*进行ACM交易
计算机系统*卷 2，第4号，11月，第277-288页。

3请参阅计算机科学和电信委员会。1999。*信任网络空间*，国家科学院出版社。

4有关垃圾邮件及其控制的一种观点，请参阅D. Dorn，1998年，“垃圾电子邮件应缴的邮资—垃圾邮件使Internet损失数百万美元。
每月”， *互联网周刊*，1998年5月4日；在http://www.techweb.com/se/directlink.cgi?INW19980504S0003。总结
有关控制垃圾邮件的立法方法的信息，请参见蒂姆·欧埃尔特。1999年。“技术快速研究：垃圾邮件”。 *计算机世界*，
4月5日，第70页。邮件滥用防护系统（MAPS.LLC）为第三方（ISP）提供了过滤和控制垃圾邮件的工具。
他们的章程指出，他们控制垃圾邮件的方法是“教育和鼓励ISP严格执行条款，
禁止他们的客户从事滥用电子邮件行为的条件。” 请参阅http://www.mail-abuse.org/。

5在过去的十年中，为定义所谓的“服务质量”机制进行了大量工作。
互联网。参见Braden，R，D.Clark和S.Shenker。1994。Internet *体系结构中的集成服务：概述*。RFC
IETF和Carlson，M.等，第1633页。1998. *差异化服务的体系结构*。RFC 2475，IETF。这项工作的进展
在http://www.ietf.org/html.charters/intserv-charter.html和http://www.ietf.org/html.charters/diffserv-charter.html上进行了报告。

6见拉尔森，加里和杰弗里·切斯特。1999. *开放之路之歌：为21世纪建设宽带网络
世纪*。媒体教育中心第四节，第6页。请访问http://www.cme.org/broadband/openroad.pdf。

7我们还讨论了其他类型的第三方，它们的服务可以通过沟通的端点或
他们的行为原本是可以容忍的。两种第三方都有增长的潜力，但本节重点介绍
施加不受欢迎的第三方。

8作为趋势的一部分，应用程序服务提供商（ASP）的兴起标志着这一趋势。

9构造“免配置”或“即插即用”或“即装即用”设备的常用方法是：
假设其他元素承担了控制设置和配置的角色。当然，集中化带来了其他
问题，例如漏洞的共同点，以及集中管理和分发之间的适当平衡尚不明确
消费者网络的安全功能。

10例如，请参阅：Saltzer，Jerome H. 1999年，*“开放获取”只是冰山一角*，10月22日，可在*以下网址*获得：
http://web.mit.edu/Saltzer/www/publications/openaccess.html。以及Lemley，Mark A.和Lawrence Lessig。1999.之前申报
联邦通信委员会，（在同意许可控制权转让的申请中

26页

MediaOne Group，Inc.归AT＆T Corp. CS备案号：99-251）。可从http://cyber.law.harvard.edu/works/lessig/MB.html获得。
可在http://cyber.law.harvard.edu的概述中查看Lessig的工作。对于一个可以直接说到结束的轻量级示例
最后，请参见：Lessig，Lawrence。1999年。“这是建筑，董事长先生。”

11《全球和国家商业电子签名法》表明了对
需要工具来支持网络媒介的交易，尽管观察家注意到它提出了有关如何做的自己的问题
因此-解决技术和政策问题将需要更多工作。

12 Chaum，大卫。1992年。“实现电子隐私”。*科学美国人*。八月。第96-101页。

13似乎这种对身份保护的关注，特别是在诸如
地址，被夸大了。电话系统说明了如何增加对身份的关注
沟通的复杂性。在电话系统的大部分历史中，被叫电话（因此该人
接听电话）不知道呼叫者的电话号码是多少。然后发明了“来电显示”功能，以显示
呼叫者到被叫方的号码。这很快导致了对一种方法的要求，以防止这些信息被传递

通过电话网络。添加此功能后，在电话号码级别重新建立了呼叫者匿名功能，导致
转向要求接收者可以拒绝拒绝透露其电话号码的人的呼叫的功能。
支付“未列出”号码的人使用的电话号码的处理方式还出现了其他问题，
电话服务提供商和州监管机构的决定似乎有所不同。鉴于这种相当复杂的平衡的出现
在传统电话技术中，没有理由认为互联网用户最终会需求更少。即使
没有显示单个用户的身份，此低级别信息可用于构建聚合配置文件
行为，例如Amazon在1999年夏季发布的有关基于e-
邮件地址。请参阅Amazon.com。1999年。“ Amazon.com推出了具有成千上万个畅销书的'Purchase Circles（TM）'
列出家乡，工作场所，大学等。” 8月20日，西雅图，新闻稿，网址：www.amazon.com；
Declan的McCullagh。1999年。“老大哥，亚马逊的大“乐趣”。” *有线*，8月25日，可在
www.wired.com/news/news/business/story/21417.html; 路透社 1999年。“亚马逊修改了购买数据政策。” *Zdnet*，八月
27，可在www.zdnet.com/filters/printerfriendly/0,6061,2322310-2,00.html上找到；和Amazon.com。1999年“ Amazon.com
修改“ Purchase Circles [TM]”功能。” 新闻发布会，西雅图，8月26日，可访问www.amazon.com。

14这种赠与的例子是来自诸如Hotmail之类的提供商的电子邮件帐户的普及，
要求用户证明他的真实身份（在建立财务帐户时会被要求）。这允许用户
发送具有相对匿名性的消息。因此，某些在线商家将不接受使用以下内容的用户的订单
Hotmail帐户。

15 Cookies可能是更大型的监视软件的一部分。参见，例如，O'Harrow，Jr.，Robert。1999年。
“担心“网络错误”的困扰：看不见的事实收集代码引起了隐私方面的关注。” *华盛顿邮报*，11月13日
E1，E8。

16参见O'Harrow，R和E. Corcoran。1999年。“英特尔放弃ID号计划”，*《华盛顿邮报》*，1月26日。
http://www.washingtonpost.com/wp-srv/washtech/daily/jan99/intel26.htm。英特尔放弃使用ID作为标识符
在电子商务交易中受到消费者压力。请参阅http://www.bigbrotherinside.com/。

17 Microsoft实施了一种方案，以使用从Office 97派生的唯一ID标记使用Office 97生成的所有文档。
机器的网络地址。为了回应公众的批评，他们使禁用此功能成为可能。他们也
在Windows 98的联机注册过程中，不再报告每台计算机的硬件唯一ID。请参阅
http://www.microsoft.com/presspass/features/1999/03-08custletter2.htm。

18见Cha，Ariana Eunjung。2000。“您的PC正在监视：将发送个人数据的程序变成例行程序。” *的
华盛顿邮报*，7月14日，A1，A12-13。

19参见计算机科学和电信委员会。2000年。*数字困境：
信息时代*，国家科学院出版社。

20 D'Antoni，H.2000。“网络冲浪者要当心：有人在看着。” *InformationWeek Online*，2月7日，
http://www.informationweek.com/bizint/biz772/72bzweb.htm。当前可用软件的示例包括SurfWatch，网址为
http://www1.surfwatch.com/products/swwork.html和Internet资源管理器，网址为http://www.sequeltech.com/。

21 2000年初对主要网站进行的拒绝服务攻击激增，说明了此问题的严重性。

22莫斯，迈克尔。1999年。“在电子邮件劫持游戏中”。*《华尔街日报》*，11月9日，B1，B4。
“已经有大量的网站在Internet上进行欺骗，诱使人们通过使用与互联网地址稍有不同的地址进行点击。
被模仿的网站：这里是多余的字母，那里是连字符。现在，几乎是保密的，其中一些相似的Web
网站也在抓电子邮件。”

23一系列影响微软Internet Explorer的公开问题以及相关软件的产生
Microsoft安全站点上记录了这些修复程序：http：//www.microsoft.com/windows/ie/security/default.asp。类似的清单
可以在http://home.netscape.com/security/notes/中找到有关Netscape Navigator的问题。

24 Jerome Saltzer，1998年。个人通讯，11月11日。

第27话

25与使用互联网本身征税相反，例如电话服务征税。此讨论不
处理税收的好处；它源自对实现它的（多种）努力的认可。

26例如，独立于技术，通过审计的实践和风险来促进所得税合规性。

27实际上，当今许多色情网站都结合使用了拥有信用卡和自我确认的方式
年龄是成年人可以接受的保证-尽管一些未成年人拥有信用卡。表示成年有不同
如Lessig所指出的，表示少数派的后果；这里的目的是对比内容和用户的标识。

28还有其他目的可以在网络中强加一个控制点，以实现据说更强大的功能。
端点实施所不能提供的解决方案。这些措施包括促进窃听/窃听，收税和
与使用网络进行交易相关的费用，等等。Internet工程中正在讨论一个问题
工作队（IETF）是如何修改互联网协议以支持法律通讯援助的方式
1995年执行法（CALEA）窃听法规。参见耶利克劳斯。1999年。“ Internet工程师拒绝窃听
提案。” *纽约时报*，B10年11月11日。设计界当前的观点是这不是
IETF的适当目标。但是，设备供应商似乎对遵循CALEA感兴趣，

由于他们的客户表达了兴趣，因此讨论的结果仍然不清楚。

29可能会引入新的Internet地址空间，作为下一代Internet协议的一部分称为IPv6的IPv6具有更大的地址集，将减轻对NAT设备的需求。当前有很多关于NAT设备是Internet的临时修订，还是现在的永久部分。

30当本文完成时，有关FBI的“食肉动物”系统（称为“互联网”）的新闻爆出。部署在ISP场所的“窃听系统”。参见金，尼尔和泰德·布里迪斯。2000。“ FBI的窃听扫描电子邮件火花关注。” *《华尔街日报》*，7月11日，A3，A6。另外，请注意，用户到处移动并拨号输入不同的电话号码不会使用相同的物理链接进行连续访问，但是由于它们必须进行身份验证他们自己到ISP来完成连接，ISP知道谁在拨号，并且可以相应地建立日志记录。

31同样，如果一个组织对控制其用户的行为有任何要求，它将由从出口角度可以最好地实施控制。

32 当然，这种控制并不完美。创意用户可以购买多个ISP帐户，以一种无法预测的方式从一个移动到另一个。这就是当今垃圾邮件发送者与那些垃圾邮件发送者之间的斗争中正在发生的事情谁来控制它们，这是控制和回避之间动态争斗的另一个例子。

33 1998年制定的1676年《加利福尼亚州议会法案》。

34有关内容和用户标签的详细讨论，请参见Lessig，Lawrence和Paul Resnick（1999）。“分区互联网上的讲话：法律和技术模型。”*《密歇根州法律评论》* 98（2）：395-431。

35这对于行业自我监管的可行性至关重要。鉴于政府迫在眉睫的前景，该主题监管，是许多争论的主题。例如，主要的行业参与者和学者参加了1999年国际贝塔斯曼基金会（Bertelsmann Foundation）组织的会议，将标签方法赋予用户授权并敦促政府支持基于标签的私有过滤。参见贝塔斯曼基金会。1999年。*互联网内容的自我监管*。9月，德国，古特斯洛，网址：http：//www.stiftung.bertelsmann.de/internetcontent/english/content/c2340.htm。

36参见，例如：美国联邦贸易委员会。1998年。*互联网广告与行销：路*。华盛顿特区，八月，请访问：www.ftc.gov。

37由万维网联盟维护的PICS网站是http://www.w3.org/pics。

38有许多实现PICS筛选的Web代理服务器。看到http://www.n2h2.com/pics/proxy_servers.html。

39有关PICS引起的关注的讨论，请参见http://rene.efa.org.au/liberty/label.html。对于这样的回应PICS开发人员和支持者之一的担忧，请参阅Resnick，Paul编。1999年。“ PICS，审查制度和知识自由常问问题。” 可从www.w3.org/PIC/PICS-FAQ-980126.HTML获得。

40万维网联盟维护的Metatdata网站是http://www.w3.org/Metadata/。

41例如，有些诉讼试图阻止在网页的元数据字段中使用商标，而不是与商标持有人相关联。有关与元数据中的商标有关的一些诉讼的摘要，请参见：http://www.searchenginewatch.com/resources/metasuits.html。

42可以在http：//www.anonymizer.com、http：//www.idzap.net/找到对浏览器服务进行匿名处理的示例，http://www.rewebber.com/、http://www.keepitsecret.com/、http://www.confidentialonline.com/home.html和http://www.websperts.net/About_Us/Privacy/clandestination.shtml。这些中的最后一个提供匿名匿名服务中间体位于国外，以避免美国法律制度的影响。其中一些服务的质量是在Oakes克里斯（Chris，1999）中受到质疑，“匿名网络冲浪？嗯，”*《 有线新闻》*，4月13日http://www.wired.com/news/technology/0,1282,19091,00.html。

第28话

43有关试图提供流量分析保护的系统的示例，请参阅Goldschlag，David M.，Michael G. Reed和Paul F. Syverson。1999。“匿名和专用Internet连接的洋葱路由”。*通讯ACM*卷 42，编号 2月2日。有关完整的参考书目和讨论，请参见http://onion-router.nrl.navy.mil/。

44Mazières，David和M.Frans Kaashoek。1998年。“电子邮件笔名的设计，实现和操作服务器。” *第五届ACM计算机和通信安全性会议论文集*（CCS-5）。旧金山，加利福尼亚，11月，第27-36页。

45传出消息的开头是一系列地址，每个地址都指定一个中继点。每个地址是使用前一跳的公钥加密，以便中继点（只有中继点）可以解密消息应使用其匹配的私钥进行下一跳。每个中继点将消息延迟不可预测的时间，因此很难将传入消息和传出消息相关联。如果使用了足够的跃点，则几乎不可能跟踪从目标到源的路径。

46有关当前可用来过滤邮件服务器中垃圾邮件的工具的概述，请参见http://spam.abuse.net/tools/mailblock.html。

47用于内容的受控登台的更复杂的复制/托管方案提供了弥补这些问题的功能限制，作为回报，内容提供商通常必须向服务付费。

48这是一个在不同情况下进行更多分析的主题。有关法律评估，请参见，例如
Froomkin，A。Michael。1996年，“受信任的第三方在电子商务中的基本作用”，《*俄勒冈法律评论*》75:29，
可在www.law.miami.edu/~froomkin/articles/trustedno.htm上找到。

49例如，请参见Dieter Gollmann的Zhou Jianying Zhou的共同承诺协议。1996“公平的不可否认性
协议。” 5月6日至8日，奥克兰，*1996年安全和隐私研讨会的论文集*。

50公证人是“ [a]由州政府任命的负责人，负责见证重要文件和文件的签署。
宣誓。” 参见国家公证人协会。1997年。“什么是公证人？” 加利福尼亚州查茨沃思，地址：
http://www.nationalnotary.org/actionprograms/WhatisNotaryPublic.pdf。对这一作用的认识导致对
“网络公证人”作为互联网中的有用代理人这一直是美国律师协会的研究主题，但是
目前看来并没有引起人们的兴趣。

51与支票付款有些类比，在这种情况下，通常不会验证银行余额
采购。但是，支票的签收人可能会要求其他形式的身份证明，这可以帮助您收取不良费用。
校验。如果证书已失效，则接收者甚至无法指望交易中的另一方
其实是。因此，以后求助的选项可能会更少。

52我们强调机制的广泛选择，是因为技术人员通常更喜欢技术
解决方案。本文早期承认的互联网哲学主张技术优于其他类型的互联网。
机制。参见，例如，戈德堡，伊恩，戴维·瓦格纳和埃里克·布鲁尔。1997年。“针对个人的隐私增强技术
互联网”，网址为www.cs.berkeley.edu/~daw/privacy-compcon97-222/privacy-html.html。这些作者注意到“
cyberpunks信条可以粗略地解释为“通过技术而不是通过立法获得的隐私”。如果我们可以保证
通过数学法则而不是官僚主义的法律来保护隐私，那么我们将拥有
为社会做出了重要贡献。正是这种愿景指导并激发了我们的互联网隐私保护方法。”

53没有技术验证该号码确实已发送（传真就像互联网一样，是端到端的。
设计），但前提是可以使用该法律将垃圾传真的数量保持在可接受的水平。另请注意
该法律的目的是控制不必要材料的接收，与电话相反，该法禁止“匿名传真”
呼叫，可以防止呼叫者的电话号码传递给被叫方。

54. 1999年年中，根据行政命令建立了一个与
互联网上的非法行为。总统关于互联网非法行为的工作组。2000年 。*电子前沿：
非法行为对互联网使用的挑战*。游行。可在：
http://www.usdoj.gov/criminal/cybercrime/unlawful.htm。

55作者意识到，今天在互联网上，各种标签都与自愿性的内容分级计划相关，
等等。; 目前，法律或法规的互补性插图来自其他领域。但是请注意，
上面引用的贝塔斯曼基金会会议摘要专门将执法作为自愿性的补充
标签。它观察到：“执法是任何国家在预防，侦查，调查和预防犯罪中使用的基本机制。
起诉互联网上的非法和有害内容。由于各种原因，这种状态反应是必不可少的：它保证状态
垄断权力和公共秩序，它在民主上合法化并可以直接执行，并确保正义，公平和
法律确定性。但是，仅凭法律实施的法律法规体系将是无效的，因为
互联网的技术，日新月异和全球性。在协调的方法中，必须建立自我调节机制
结合执法作为必要的备份。”（第45页）。

56美国联邦通信委员会，“ V-Chip主页”，可访问http://www.fcc.gov/vchip/。

57上面引用了Amazon.Com上的信息。在RealNetworks上，请参阅：Clark，Don。1999年。“ RealNetworks将发行
软件补丁程序可以阻止程序监视用户。”《*华尔街日报*》，B8年11月2日。那篇文章解释了，
“用户不知道的[Real-Jukebox]软件会定期通过Internet将信息传输给公司，

第29话

包括用户播放的CD以及磁盘驱动器上加载了几首歌曲。” DoubleClick展示了更广泛的
隐私挑战，因为它跟踪消费者在站点和产品之间的移动；引起广泛争议的争议
反应，包括因向联邦贸易委员会投诉而进行的政府调查。参见：Tedeschi，Bob。
2000年。“评论家对跟踪Web用户的新闻报道。” *纽约时报*，2月7日，C1，C10。

58 Simpson，Glenn R.，2000年。“电子商务公司开始重新考虑对隐私法规的反对，如滥用，愤怒。
上升。”《*华尔街日报*》，A24年1月6日。

59个人可以做什么以及行业可以做什么，当然取决于激励措施，而激励措施是激励措施的一部分。
非技术机制图。围绕UCITA开发的最新争议说明了不同
对谁承担哪些成本和收益的期望和解释。这些不断发展的框架的问题是现实
尤其是消费者和企业通常希望避免诉讼费用。

60服务器的操作员很乐意根据任何法院命令提供他们所拥有的信息，但是
系统经过精心设计，以使这些信息无用。

61技术，法律和其他对行为的影响之间的紧张关系是人们广泛讨论的
劳伦斯·莱西格（Lawrence Lessig）谈“代码”的作用（宽松地讲，技术）。参见他在1999年出版的《*网络空间的法典和其他法律*》（基本）
书籍，纽约。对《*守则》的*重要回应……请注意，技术具有延展性，而不是恒定不变，这是前提

纸，政府和行业的利益和动机也是如此。参见，例如，Mann，Charles C.，1999。
未被认可的数字世界立法者。*《Atlantic Unbound》*，12月15日，可在以下*网址*获得：
www.theatlantic.com/unbound/digicult/dc991215.htm。

62所谓的“法律冲突”提供了一套原则和模型来解决跨越
至少两个司法管辖区。在现实空间中解决此类问题非常困难，网络空间也带来了更多挑战，
但是在法律冲突下的进展专栏阐明了一些方法，其中包括以法律为准的私人协议
在这种情况下，国际协调（困难而缓慢，但已经在进行）和间接监管，
它针对域外活动的局部影响（例如人员和设备的行为）。有关概述，请参见
戈德史密斯，杰克L.，1998年。“反对网络无政府状态”。 *芝加哥大学法律评论*，65：4，秋季，第1199-1250页。其中
戈德史密斯解释说：“网络空间提出了两个相关的法律选择问题。首先是问题
复杂。这就是如何为具有多个管辖权的网络空间活动选择单一的管辖法律的问题
联系人。第二个问题与情景有关。这是当活动场所如何选择适用法律的问题
不能轻易地在地理空间中找到目标。”（第1234页）判例法表明，这些问题正在解决中（或至少
从事）。参见例如：Fusco，Patricia。1999年。“法官裁定ISP，服务器位置可能决定管辖权。” ISP-
《星球》，6月11日，请访问：www.isp-planet.com/politics/061199jurisdiction.html；和Kaplan，Carl S.，1999年。
赌博案涉及管辖权的棘手问题。” *纽约时报*，8月13日，第B10页。后者解决了
州法律与联邦法律之间的相互作用，该法案通过《电汇法》（18 USC 1084）和《旅行法》（18 USC）禁止赌博
1952年）和州际运输赌博用具法（18 USC 1953年）。其中一些问题已遭到攻击
美国律师协会的互联网管辖权项目；请参阅http://www.kentlaw.edu/cyberlaw/。

63请参阅计算机科学和电信委员会。1994. *实现信息未来：互联网和
除此以外*，美国国家科学院出版社和计算机科学与电信委员会。1999. *资助革命：
政府对计算机研究的支持*，国家科学院出版社。

64个大型ISP（例如AOL）试图通过分发自己的浏览器来控制最终节点，
他们鼓励或要求用户雇用。事实证明这种方法是成功的。将来，我们可以期待
看到ISP有兴趣将其对端点的控制扩展到可能的扩展，例如通过添加功能
互联网机顶盒和它们安装在家庭中的其他设备。

65例如，请参见http://www.home.com/aup/上的Excite @ Home适当使用政策，
禁止通过其住宅Internet服务运行服务器。

66有关可能结果的评估，请参见Jerome Saltzer。1999。“开放访问”只是冰山一角，”
为马萨诸塞州牛顿市电缆委员会准备的论文，10月22日，在http://mit.edu/Saltzer/www/publications/openaccess.html上。
在简短评论他认为不理想的许多可能结果后，Saltzer指出最可怕的是
当今的开放存取之争的可能结果，如果没有开放存取以及窒息的竞争和创新，
随着客户和电缆竞争对手都开始更好地理解互联网为何如此运作，这种可能性越来越小了
以及一些新兴实践的含义。”

67参见上文尾注10中引用的材料。还要注意在“对等”的标题下提出的担忧。例如，参见
卡鲁索，丹妮丝。2000年。“数字商务：互联网依赖于网络之间相互传递数据。但是如果
其中一个拒绝？” *纽约时报*，2月14日，p.C4。

68共同运输意味着某些权利和某些责任，例如提供者有义务为所有人提供服务。
如果这些订户将网络用于不可接受的目的，则可以保护他们免受责任。事实
Internet的设计使得（通过端到端的争论）ISP无法轻松地控制通过其网络发送的内容
ISP似乎可以为所有参与者提供服务这一事实使一些人建议将ISP视为普通运营商。的
有人认为ISP比其名义业务具有更大的控制内容的能力，
技术会建议。

第30话

69 1990年代后期，人们对“关键基础设施”的关注加剧了人们的关注和关注。
越来越依赖互联网，政府和一些行业领袖对新计划和
监视互联网使用或“滥用”并增强其针对恶意或意外事件的鲁棒性的机制
破坏。参见Blumenthal，Marjory S.，1999年。1999年。“可靠和值得信赖：网络基础设施的挑战
《千年边缘的保护》，*《iMP杂志》*，9月，
http://www.cisp.org/imp/september_99/09_99blumenthal.htm。

70受欢迎的虚构人物哈利·波特（Harry Potter）收到了一些建议，这些建议可能同样适用于他的世界和
互联网：“如果您看不到大脑的大脑，那么就不要相信任何能够自己思考的事物。” 罗琳，JK，1998年。*哈利
波特与密室*。布卢姆斯伯里出版公司，伦敦，第43页。242。

71庞弗雷特，约翰。2000年。共产党人寻求信息遏制，*《华盛顿邮报》*，
一月27。

72参见计算机科学和电信委员会。1996年。 *密码学在保护信息安全中的作用
社会*。国家科学院出版社。

73如今，监管机构（例如联邦贸易委员会）正在对实际网站进行抽查。

74这种方法有点类似于世界上某些地方的做法，即不总是检查乘客
公共交通工具有适当的门票。相反，有巡回检查员进行抽查。如果罚款失败

拥有正确的机票是足够高的，此计划可以实现合理的合规性。