DOI: 10.3724/SP.J.1224.2013.00223

“信息化背景下的经济转型与社会管理：挑战与对策”专刊

信息化时代的若干政治哲学问题

吴 彤[1]，张春峰[1]，丁大尉[2]

（1. 清华大学科学技术与社会研究所，北京 100084；
2. 烟台大学人文学院，山东烟台 264005）

摘 要: 资本与权力的联合，正在改变互联网的架构，推动网络监控功能的发展。关于监视的理论可归为四类：极权主义监视理论、全视主义监视理论、监视集合理论、律法主义监视理论。按照劳伦斯•莱斯格的观点，用于搜索某种文件的计算机蠕虫病毒无论出于什么目的，都干预了人权与自由。安德鲁•查德威克认为“窥探”与“搜查”必须在律法主义的框架内得到授权才可以进行。在中国，技术和工程领域缺乏关于网络监视与自由、民主之深刻思考。不加制约的互联网监视系统，扩大了干预与监视的权力范围。这个问题的根基涉及国家与社会的关系这一根本性的政治哲学问题。应在自由主义的立场上，补充律法主义的监督视角，形成适度自由主义的互联网发展的政治哲学。

关键词: 信息化；互联网；技术；权力；资本；监督；政治哲学

中图分类号: N031 **文献标识码:** A **文章编号:** 1674-4969(2013)02-0223-08

引言

1999 年以前，互联网不受规制的观点曾是主流观点。这些观点主张：“现实空间的种种规制不应延伸到网络空间。政府不能干涉人们的网络生活。”近年来，上述主流观点已逐渐退出历史舞台。[1]前言，3“9·11”之后，即便是奉行自由主义的美国，也在加强互联网的监控。这种趋势与互联网建立之初的意愿，以及按照这种自由主义建立起来的互联网架构，无疑是存在矛盾的。资本对于互联网的利用，与政府对于互联网的监控相互结合，推动了对于互联网监控的加强趋势。持自由主义理念的人们则对此非常担忧。

互联网上信息海量且复杂，一方面，互联网的发展推动了电子商务、电子政务的发展；另一方面，利用互联网犯罪，互联网上色情泛滥，也造成了诸多问题。恐怖主义组织也在利用互联网。如果互联网不可监控，那么互联网就会成为藏污纳垢的场所。但是如果互联网可以任意监控，又有可能极大地介入人的隐私空间。这就提出了一系列问题：互联网是否应该监控？如果可以进行监控，如何进行监控，监控在何种意义上才是合理和合法的？而这些问题又呼吁关于互联网的政治哲学的发展。

按照杜俊飞在安德鲁•查德威克（Andrew Chadwick）《互联网政治学：国家、公民与新闻传播技术》的代译序里所说的[2]序 007，互联网的政治哲学内容包括两个部分：

1）互联网本身：互联网产生与发展过程中的

收稿日期: 2012–12–04; 修回日期: 2013–01–10
基金项目: 973 课题子课题“新一代互联网技术和社会关系研究”（2009CB320501）
作者简介: 吴彤（1954–），男，教授，研究方向为科学技术哲学、科学技术与社会。E-mail: wutong@tsinghua.edu.cn
张春峰（1983–），男，博士生，研究方向为科学技术哲学。E-mail: zhangcf05@mails.thu.edu.cn
丁大尉（1977–），男，讲师，研究方向为科学社会学与科技政策。E-mail: dingdw08@mails.tsinghua.edu.cn

政治因素，以及互联网生长过程中形成的内部政治，如互联网技术演进与融合中的技术格式争论、关键技术的政治推动、技术应用程序的最后敲定、现有技术的霸权地位的确定、互联网的全球管理、互联网全球管理中的权力争夺等。

2）互联网应用：互联网这种技术形态诞生以来的政治化使用，以及由此带来的对现实政治的影响，如电子民主、电子动员、电子竞选、电子政务、互联网监视、互联网监管与控制、“数字鸿沟”引发的政治落差、互联网的地缘政治等。

本文将按照这两个部分所划定的内容，仅讨论互联网技术监督的科学政治哲学问题。

1 互联网技术架构及其演变的政治影响

互联网技术架构本身是否具有网络监控的功能？按照标准观点，一个网络监控系统应该具有的功能包括：网络数据采集、对应用层数据的还原、对应用层数据的分析、对网络通讯的控制。互联网最初的架构里并没有网络监控的功能，至少没有全部功能。然而，互联网在其发展过程中，政府和商业组织推动了网络监控功能的出现和发展。

1.1 TCP/IP 协议与网络监视

1974 年，两个定义不同计算机网络之间可以传输报文的协议 TCP/IP 问世，其核心技术免费向全世界开放，导致了 Internet 的大发展。

TCP/IP 实际上是一组不同层次上的多个协议的组合。通常认为它是四层协议系统：

第一层，链路层，主要是物理层，包括操作系统中的设备驱动程序和计算机对应的网络接口卡。在物理层实现监控的困难很大。

第二层，网络层，包括 IP（网际协议）、ICMP（控制报文协议），以及 IGMP（Internet 组管理协议）。

第三层，运输层，主要为两台主机上的应用程序提供端到端的通信，包括 TCP（传输控制协议）和 UDP（用户数据报协议）。

第四层，应用层，包括 HTTP（用于传输 Web 内容）、FTP（用于传输文件）、SMTP（用于发送和转发电子邮件）、POP3（用于收取邮件）。

原来互联网架构中的 TCP/IP 并不包括审查 TCP/IP 数据包内容的技术。但 TCP/IP 也没有阻止其他应用程序来审查 TCP/IP 数据包，并披露数据包的内容。推动这些程序出现的机制是政府对于网络监控的需求，以及商业组织出于经济利益考量对于身份认证的要求（如电子银行的需求）。一般而言，各国政府都力图确保其搜查能力和权力不被日新月异的技术所削弱。例如，美国政府曾经力图通过给一种加密芯片技术 Clipper 芯片的开发与推广进行补贴的办法，控制加密标准，从而控制加密技术的使用。后来这一做法失败了。美国政府又开始试图直接规制加密代码的作者——要求他们必须在代码中留有一扇政府能够进入的后门[1]74-75。商业方面，微软就在推动数字身份验证技术的发展。不仅如此，现如今，政府与商业组织的合作对于规制互联网和监控更是推波助澜。那些曾作为抵制规制堡垒的公司，摇身一变，成为制造规制“武器”的“兵工厂”。这些“兵工厂”大量生产与监控有关的软件。

比如：有一个软件被称为内容控制软件，叫“iProtectYou”。它可以审查网络上的数据包，该软件能够“过滤有害网站和新闻组，按照预定的时间表制定上网时间，限制发送和接受的数据流量，屏蔽电子邮件、网络聊天、即时消息及 P2P 连接中的不雅词汇，记录网上活动的详细日志”。这是一种置于互联网顶端并实施监控的应用程序。[1]63

还有大量控制网络的应用程序被设计出来。其中，最常用的是 Nmap。Nmap 被用于网络探测和安全扫描，可以迅速扫描大型网络。Nmap 利用原始 IP 数据包，采取全新的技术来确定：网络上哪些服务器可以访问、它们提供什么服务（程序

名称和版本）、它们运行哪个操作系统（操作系统的版本）、它们使用哪一种过滤程序或防火墙，以及其他一些信息。这个软件是自由软件。[1]63

另外，还有各种“数据包过滤”技术。它们也属于监控技术，可以监控到数据包携带的是什么，以确定是否允许其通过。这就是代码层对TCP/IP 作的补充。它赋予管理员审查网络数据包内容的权限，这一权限大大加强了网络的可规制性。

1.2　后门与窗口

通过技术为监控留下日后可以审查或搜查的后门与窗口，不仅是一种事后监控办法，也是一种把相应的制度建设与技术架构结合起来的技术加规制的方法。劳伦斯·莱斯格（Lawrence Lessig）提供了两个公司的例子：

第一个是 Network Associates，是全球最大的网络信息安全和管理的提供商之一，沿用 PGP（Pretty Good Privacy）密码技术，即采用公开密匙加密与传统密匙加密相结合的方法。起初，它是规制的劲敌；而今，它所提供的软件却在密码技术控制和密匙系统的还原方面，为公司创造了便利。密匙系统的还原为公司开了一个后门，在大多数情形下，这个后门远比政府需要的后门要宽松得多[1]80。

第二个是思科公司。1998 年思科公司发布了一款路由器，这种路由器使提供商能够在链路层之间加密网关之间的通信数据。同时，这种路由器还设有一个开关，通过控制这个开关，可以打开或关闭路由器数据的加密，并且能够协助采集未经加密的通信数据。政府可以操纵这个开关，换句话说，只有在政府允许的情况下，通信数据才可以被加密[1]80。

这两个例子表明，技术架构正在通过商业组织发生变化（这里当然有政府施加的政治影响），互联网已经从个人英雄主义的时代变为商业和政府主控的时代。

正如劳伦斯·莱斯格所指出的，政府并不能改变 TCP/IP 自身的规制架构，但是政府可以通过修改网络空间中任何一层的代码来改变互联网架构的实际约束力[1]70，如美国政府就一直努力通过法律手段来规制互联网。美国国会 1994 年通过的《法律执行通信协助法》（*The Communications Assistance for Law Enforcement Act*，简称 CALEA）要求：网络必须被设计成保护执法能力的模式，以便实施电子监听。这一要求曾经在一系列的“安全港”协议下协商，最终规定标准网络必须符合法律的这一要求[1]71。CALEA 的通过只是一个信号，4 年后，美国联邦调查局请求联邦通信委员会进一步加强政府对互联网的规制权。美国联邦调查局提出的修正案中有一条规定，要求通信公司报告信号传送经过的信号塔，以此来追踪移动电话用户的位置。这间接地要求通信公司修改代码以将其信息披露给美国联邦调查局[1]73。2005 年 8 月，美国联邦通信委员会规定，VOIP（Voice-Over-IP）服务“必须设计成便于政府监听的模式”[1]72。

1.3　从 IPv4 到 IPv6 的安全与监控

IPv6 把互联网地址从 IPv4 中的 32 位扩展到 128 位，使得互联网地址空间海量增长。而以往的 IPv4 地址的设计原理与路由寻址理论不能适应 IPv6 下的新一代互联网。IPv6 需要在 IPv4 基础上进行扩展，因此其中的安全可扩展性如何，是一个重大的理论与实践问题。现有互联网产生的大量安全问题，确实是由于互联网对用户源地址不加验证而带来的。新一代互联网如何解决用户真实地址访问的问题，成为下一代互联网发展的重要问题。

肖恩·赫尔姆斯（Shawn Helms）针对下一代互联网协议 IPv6，指出它会“为每一个数据包配上一把密匙，他人不可篡改或伪造这把密匙，因此，用户对于数据包的安全性大可放心。同时，这项验证功能也可以在整个互联网上识别信息的

发送方和接收方，因此，几乎完全抹杀了用户匿名的可能性”[3]。

新一代互联网的中国研究者根据“真实 IPv6 源地址访问”这一可多维扩展新一代互联网体系结构的基本要素，提出了可信任的新一代互联网体系结构的层次模型。该模型分为可信任的网络基础设施层、可信任的安全服务层、可信任的互联网应用层等三个层次。其中，可信任的网络基础设施层，主要研究新一代互联网的真实 IP 地址访问；可信任的网络安全服务层，主要研究面向新一代互联网全局网络身份标识系统、基于真实地址和身份的全局访问控制系统、新一代互联网公钥基础设施建设、认证中心系统、密钥管理协议和密钥管理系统等；可信任的新一代互联网应用层，主要研究建立在真实 IP 地址访问、可信任安全服务基础上的可信任安全应用模型，并着重研究大规模点到点的综合通信平台、可信任的电子邮件服务和可信任的 BBS 服务模型[4]。相信新一代互联网更加安全，同时也实现实名，自然监控也变得更加容易。然而，网络实名制是否与互联网的自由主义冲突？作者曾经在博客上做过一个调查，结果显示，大多数人还是支持网络匿名（表 1）。

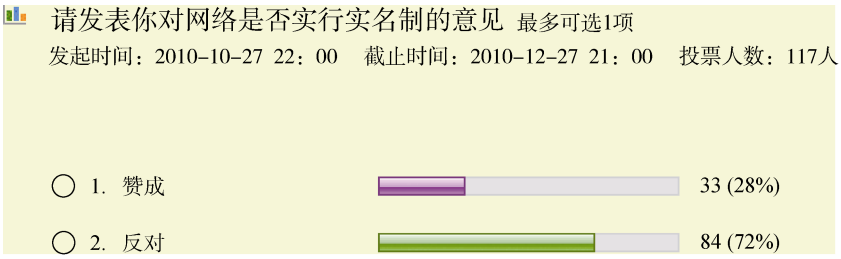

表 1　关于网络实名制的网络调查

表格来源：wutong54 的新浪博客。

在法理方面，提供安全和可信任的网络无疑是对的，但是在此种架构下，如何协调网络上的表达自由这一基本人权与网络监控之间的关系，也存在诸多不同认识[5]，确实需要认真论证。现在的监控技术对于政府和商业组织是有利的，而网络监控本该是对所有人公平的。如何实现对于上述两类组织及其中个体的监督？存在有利于民众监督政府或商业组织的技术吗？

2　互联网监督的几种理论视角

目前关于网络监视有多种理论或观点，安德鲁·查德威克把它们归为四类[2]348-355：极权主义监视理论、全视主义监视理论、监视集合理论、律法主义监视理论，并讨论了它们在应用到互联网监控的解释上的利弊。

2.1　极权主义（Totalitarianism）监视理论

这类理论以乔治·奥威尔（George Orwell）的反乌托邦小说《1984》为基本模型，反映了 20 世纪 30—40 年代的德国纳粹主义和冷战期间的斯大林式的社会监视思想。

极权主义意味社会秩序完全由政治权力或国家权力达成，私人空间被压缩到几乎不存在的状态，自由被减至最低限度。正如汉娜·阿伦特（Hannah Arendt）所言，它意味着私人及公共生活的一切方面都被包摄在一个囊括一切的统治过程之内。总之，极权主义政体的主要特征就是政治权力的渗透性和扩散性；它的极端类型就是政治权力渗透到人类的一切领域，社会秩序完全由政治权力来达成，个人不再有任何私人空间或自由。

在监视的方式上，极权主义监视采取的是，以权力集中的方式隐蔽地拦截个人通信，其对社会的态度的基点是采取恐惧与不信任。

然而，极权主义监视理论对于互联网来说，其解释有很大局限。它特别关注民族国家，而互

联网本身具有高度去中心化的特征。此外，跨国公司在互联网中的作用，也是极权主义监视理论无法解释的。但是极权主义监视理论也有它的用处，民族国家正在学会如何利用集权的方式管理本国的互联网，使分散与集中很好地统一起来。

2.2 全视主义（Panopticism）监视理论

全视主义，即全景监视主义。该理论以法国哲学家米歇尔·福柯（Michel Foucault）的“全景监狱”作为基本模型，来理解现代社会的互联网监视和相关问题。而这种“所有的地方都能够被看到”的“全景监狱”来源于政治哲学家杰里米·边沁（Jeremy Bentham）1791 年的监狱设计。米歇尔·福柯认为现代监狱不再采取暴力原则对付囚犯，而是通过经验观察来进行科学测度与控制。米歇尔·福柯还认为，“圆形监狱式”的原则已经渗透到了许多机构，如学校、工厂、军队及国家官僚机构。

安德鲁·查德威克认为，全视主义的电子监视有五个特征：自动化的高效率、非人性化、无所不在、优先占有、社会规则[2]352。

电子形式的全景监视，会涉及有关个人和群体的信息收集、处理和共享，这些信息被用来协作与控制他们对现代经济生活的商品与服务的使用；也会产生某种社会歧视效果，如社区的电子眼监督，会把一些非该社区人群列为值得特殊对待的群体。电子全景监视，也把每一个人变成为“超级全景监视监狱”的参与主体—— 既被监视，也监视着他人。

当然，全视主义在运用到互联网的监视上也同样有其缺陷，即它没有把握互联网监视的去中心化和网络化特征。

2.3 监视集合（Surveillant assemblage）理论

监视集合理论来源于凯文·哈格蒂（Kevin D. Hagerty）和理查德·埃里克森（Richard V. Ericson），他们认为监视是一种信息流的集合。通俗地说，监视很少像“全景监狱”那样处处时时每一个点都会监视到，监视虽然是全视的，但是监视常常着重的是“点”，即只在关键点上窃听信息流[2]352。这种观点有其合理性。凯文·哈格蒂和理查德·埃里克森借用隐喻，把监视与块茎植物生长（地下水平扩展其结构）联系起来：块茎极具活力，在其生长的过程中不断长出新的根茎；互联网监视类似于“块茎监视”，通过类似块茎的生长方式，“跨越多种技术和实践的多重联系”，把个人支离破碎的信息通过某种组织或技术重新聚合起来[2]352-353。

监视集合理论在解释互联网监视时的优点：让我们注意到网络技术悄无声息的扩张；把具体零碎的数据链接起来的功能；监视不依赖于等级体系—— 网络形成了多数人监视少数人的情形，网络的全视监视因此有了民主的意蕴—— 草根也可以监督精英。全视监视与重点监视在监视集合理论的视角下是统一的。

当然，如果我们相信监视集合理论，我们就无法想象我们是否还有自己的隐私。

2.4 律法主义（Legalism）监视理论

安德鲁·查德威克认为，西方资本主义国家的主流政治话语比较倾向于保护隐私的理论路向。他把这一路向称为“律法主义”。按照他的说法，律法主义监视理论认为，在反抗毫无根据的监视时，可以做出有意义的选择，即可以诉诸法律和宪法来保护个人的私人领域免受侵害[2]354。律法主义监视理论注意到，要在国家安全、公司利益、个人隐私权三者之间求得平衡，须通过合理合法的协商手段。律法主义在西方国家的理论根基是自由主义，不过在作者看来，这种自由主义已经是一种很受限制的弱自由主义。

律法主义监视理论提倡通过三种途径来处理国家安全、公司利益、个人隐私权三者的关系：第一，通过提供宪法保障来保护公民免受政府和企业的任意侵害；第二，通过法律途径来处理监视、安全与隐私的问题。在遇到互联网新技术发

展引发的侵权问题时，可以通过重新解释现有法律或呼吁制定新的法律和政策，牢牢把握技术变革所带来的影响。

3　可怕的监督

劳伦斯·莱斯格在其著作中以一个假设案例说明政府在互联网监督中可能的权力及其限制的问题：设想一个被设计用来做好事的蠕虫病毒，其代码的作者是美国联邦调查局。该局正在寻找属于美国国家安全局的某份文件。这份文件已被进行了密级分类，非经正当手续而持有该文档即属非法。将该蠕虫病毒在网上散布，一旦储存到某一台计算机的硬盘上，它就会将硬盘数据如实报告给美国联邦调查局。如果在该硬盘中没有发现目标文件，它会随即销毁自己。它执行所有这些工作的同时没有干扰机器的正常运行。没有人知道它所在硬盘的位置，除了在硬盘上发现目标文件，它不会报告有关该硬盘的任何事。[1]24-25

使用蠕虫病毒进行网络搜查违宪吗？劳伦斯·莱斯格指出，乍一想，会很容易得到一个答案，但实际上这是一个困难的问题。在该假设案例中，蠕虫病毒在执行一个政府发动的对公民硬盘的搜查任务。我们并没有（如法律通常要求的）合理的理由去怀疑某个公民的硬盘上非法存有政府正在搜寻的文件。这属于政府对私人空间的普遍的无嫌疑的搜查[1]24-25。劳伦斯·莱斯格认为，从美国宪法（尤其是美国宪法第四修正案）的出发点看，没有比这更为糟糕的事了。美国宪法第四修正案正是用来阻止这种滥用职权的情形。英国国王乔治二世和乔治三世曾发给官员“普遍搜查令”，授权他们可以有针对性地在私人家里搜查犯罪证据[6]。美国宪法第四修正案的主旨是这种搜查至少需要有嫌疑[1]25 的证据支持。从表 2 可以看出“蠕虫”假设案例与英国国王“普遍搜查令”的异同。

表 2　“蠕虫”假设案例与英国国王“普遍搜查令”的比较

“蠕虫”假设案例	英国国王的“普遍搜查令”
行事方式静默，计算机用户无从知道其硬盘被“蠕虫”病毒搜查过； 不造成无关的破坏，完成任务后自我销毁，不读取、复制私人信息； 普遍性搜查，但不侵扰日常生活，只针对违禁目标。	警察闯入私人房中搜查，给被搜查者带来麻烦、增加负担。

资料来源：文献[7]101。

更深入地思考：设想蠕虫病毒不是简单地搜查它所遇到的每一台机器，而只是在有司法授权的前提下才渗入某台机器。这样，无嫌疑搜查的问题就没有了。若如此，政府的政治要求需要网络技术的支持才能实现，即网络需为每一台联网的终端设备实名预留一个带有“门牌号”的后门，以便司法授权下的蠕虫病毒能够即时侵入搜查的嫌疑目标。技术上应该实现这种网络架构吗？这正是第三代互联网技术发展中应该关心的问题，也是涉及技术的政治哲学问题。[7]100-101

“蠕虫”假设案例所反映的问题，在当代社会并不只局限于政府行为。现代生活的显著特征就是技术的日新月异，不断更新的技术使数据搜集和处理的效率越来越高。即便原有的互联网技术架构中没有监督、追踪和搜查的技术设定，互联网公司在经济利益驱动下，也会设计、利用这些技术，搜集网民的网络痕迹，通过分析其网络行为特征，可以很容易地发现其偏好、习惯，从而为商业机会找到突破口。如约翰·巴特尔（John Battle）所说，像大多数物质文明产物一样，点击流正在成为一种资产[8]。例如，对拥有 Gmail 账号或其他 Google 账号的人，Google 在 2007 年悄悄将其缺省配置定为个性化搜索。Google 公司的科学家开发了一种“音频指纹采集”系统，它可以用你电脑中的麦克风监听你周围的背景声音，并将其用于个性化目的。如果你开着电视机，这个系统就可以记录音频信号样本，并与其“音频数据库”进行比较，从而确定你在看什么电视节目。然后

Google 公司就可以把与你喜欢的节目有关的报道或广告提供给你[9]124-125。这不正是监视技术吗？

在中国，一些网络技术研究者和开发人员，甚至根本意识不到这其中的问题。他们认为进行网络监控是理所应当的，而且理所应当为这种需求服务。[7]101-102 例如，四川大学计算机应用专业某硕士研究生的学位论文为《基于应用层的网络监控系统的研究、实现与应用》，该研究开发了一种网络监控系统，其中一种为并联方式的网络监控函数库 NetInfo，另一种是串联方式的网络监控函数库 NetInfoTb。该系统可以进行实用的网络监控和立场判断，包括：审查应用层传输的文本信息（包括可以转换成文本信息的其他信息）的立场，检查它是否违反有关方针政策和规定，如果违反了，可以根据用户的策略配置，采取保存、警告、显示、审计、阻断、替换等动作，使违法信息无处藏身。此外，该系统还可以根据 URL、发信人、收信人等应用层信息，TCP 连接的源 IP 地址、源端口、目的 IP 地址、目的端口等运输层信息对网络通信进行监控[10]2。在该系统的 NetInfoTb 中，一个处于普通模式的 TCP 连接对象能在用户（监控者）的指示下，转变到拦截模式，处于拦截模式的 TCP 连接对象将伪装成接受方，接受被拦截方发送的所有数据，且能任意修改被拦截的数据，而不被通信双方所知；并能在用户的指示下，停止拦截模式，TCP 连接对象会将篡改后的等长数据封装在多个 TCP 数据包中发送给接收方，直至发送完毕并接收到相应的应答数据包。通过这种方式，NetInfoTb 用户能够任意地篡改通信双方发送的数据而不为双方所知[10]57。

重要的是，该论文对该技术方式的制度约束只字未提。如果没有政治和法律制约，这种技术的滥用将是多么可怕，所有人的信息都将有被监控、篡改或窃取的可能。这样的（软硬件）系统比之劳伦斯·莱斯格假想的“蠕虫”病毒更甚，它的全视主义监视功能极有可能把互联网变成米歇尔·福柯所述意义上的“监狱”。中国古代社会官方对拥有技术技能的术士的管控，正说明滥用技术对社会秩序的破坏作用需要得到遏制[11]。

4 适度监督的合理性基础

赞成对网络施加监视的人士的理由是，网络出现了越来越多的问题，这些问题包括网络犯罪、网络恐怖主义和侵犯他人利益的行为与言论；不赞成对网络进行监视的人士则担心监视会损害人们在互联网上的自由与权利，会侵犯人们的隐私空间。

事实上，这个问题的根基涉及国家与社会的关系这一根本性的政治哲学问题。国家是凌驾于社会之上，还是社会中的一个受限制的组成部分？国家拥有统治的工具，所以在自由主义的政治哲学看来，国家的权力必须受到制约。因此，一个理性社会，应该在自由主义的理性观点下，遵从律法主义的制度设计，尊重人的基本权利，来进行适度的监视。这种适度的监视要在律法主义的实际立场上，取得合法的审查许可。对网络不加区分地全程监视和对所有公民进行全程监控，实际上已经不自觉地侵入了公民的隐私空间，侵犯了公民的自由。监控不能侵犯法律范围内允许的表达自由，否则就侵犯了自由主义的法理根基。

如今在发达国家，各种互联网监控软件和系统的发展、互联网监控高涨的呼声，导致了自由主义的退却，政府对于网络的监控越来越细密和严格、无孔不入。然而，中国是一个还在发展现代民主制度、进行现代民主制度建设的国家，适度自由主义是与科学发展观、建设和谐社会的诉求一致的，应得到宽容和保护。今天，我们已经有了这样的政治共识：人生而自由，人有表达的自由，这是人生而具有的权利。一个民主、自由而和谐的社会，必然要保卫人的自由，包括互联网上的表达自由。

总之，我们赞成适度的自由主义理念，赞成互联网监控应该在实际的律法主义基础上进行，而不能采取极权主义或全视主义的立场。根据这样的理念设计互联网的技术监控与安全系统（或软件）以及相关协议，对于技术政策制定者和社

会来说都是有益的。

5 结语

互联网技术监督的问题，只是信息化时代若干政治哲学问题的一个部分。原本以自由主义为理念建立起来的互联网，由于现实社会的控制与监督的渗入，而成为一种新的监督工具。对互联网的监督进行研究有四种可以借鉴的理论视角：极权主义、全视主义、监视集合理论和律法主义。应该在互联网原本存在的自由主义的立场上，补充律法主义的监督视角，从而形成适度自由主义的互联网发展的政治哲学，给人以表达自由的空间。因此在设计互联网技术层面的各类技术时，可以留有“后门”，但是要通过严格的律法程序限定准入，不能允许随意侵入他人的私人空间。

很长时间以来，人们非常自然地把互联网看成一种使人得到解放的技术，认为它使我们有了空前的自由，可以任意地表达自己的真实或虚假的意见、观点、激情，似乎互联网是一个自由主义的天堂，是现实社会无法对之进行规制的理想场所。然而，就核心意义来说，信息技术不是使人解放的技术，而是实行控制的技术[9]148。

互联网已经发展成为与政治和经济密切结合的巨机器。在这个巨机器面前，自由主义的理想是那么的渺小，其期待的实现是那么的遥不可及。但是不论如何，我们还是要持守自由，通过法律和政治制度的建设，在互联网的技术监控中限制政府的权力，建设网络自由和民主共生的网络空间。

参考文献

[1] 劳伦斯·莱斯格. 代码 2.0: 网络空间中的法律[M]. 李旭, 沈伟伟, 译. 北京: 清华大学出版社, 2009.
[2] 安德鲁·查德威克. 互联网政治学: 国家、公民与新闻传播技术[M]. 任孟山, 译. 北京: 华夏出版社, 2010.
[3] Helms C S. Translating Privacy Values with Technology [J]. *Boston University Journal of Science and Technology Law*, 2001(7): 288-299.
[4] 徐恪, 吴建平, 徐明伟, 等. 高等计算机网络: 体系结构、协议机制、算法设计与路由器技术[M]. 第 2 版. 北京: 机械工业出版社, 2009: 208.
[5] 甄树青. 论表达自由[M]. 北京: 社会科学文献出版社, 2000: 66-80.
[6] Stuntz J W. The Substantive Origins of Criminal Procedure[J]. *Yale Law Journal*, 1995(105): 406-407.
[7] 吴彤. 蠕虫：网络监督与科学教育: 从科学实践哲学的立场看科学人文教育[J]. 科学与社会, 2011(4).
[8] 约翰·巴特尔. 搜[M]. 张岩, 魏平, 译. 北京: 中信出版社, 2010: 13.
[9] 尼古拉斯·卡尔. IT 不再重要[M]. 闫鲜宁, 译. 北京: 中信出版社, 2008.
[10] 张志国. 基于应用层的网络监控系统的研究、实现与应用[D]. 成都: 四川大学. 2003.
[11] 吴彤. 中国古代正统史观中的“科技”[J]. 内蒙古师大学报, 1990(4): 60-67.

Elementary Investigation of Some Political Philosophy Problems in Information Age

Wu Tong[1], Zhang Chunfeng[1], Ding Dawei[2]

(1. *Institute of Science*, *Technology and Society*, *Tsinghua University*, *Beijing* 100084, *China*;
2. *College of Humanities*, *Yantai University*, *Yantai*, *Shandong* 264005, *China*)

Abstract: Power and capital have promoted the emergence and development of the network monitoring function. There are many theories or opinions about monitoring which Andrew Chadwick classifies into four categories: totalitarian, All-seeing, monitoring set theory and legalism. Lawrence Lessig points out that the computer worms for searching some files still interfere with the human rights and freedom. Andrew Chadwick argues that it must be authorized before they can "spy" and "search" within the framework of legalism. In China, some scientists and engineers of technology and engineering for network monitoring lack the concept of freedom, democracy and freedom of expression without interference. The foundation of this problem involves the relationship between state and society, which is the fundamental problem of political philosophy. Based on liberalism, we should improve legalism supervision, so as to form moderate liberalism of internet development in political philosophy.

Key words: informatization; internet; technology; power; capital; supervise; political philosophy