中外法学 Peking University Law Journal
Vol. 24, No. 2(2012) pp. 379 - 394

网络安全、隐私与互联网的未来

胡 凌*

摘 要 2010年底的腾讯QQ与奇虎360的战争引发了对中国互联网企业问题的重大讨论,较为严肃的讨论主要集中在涉及的法律问题(例如隐私、恶意软件、不正当竞争、垄断)和企业的社会责任。本文试图从网络安全的角度重新解读这一事件及相关法律问题,认为是网络空间的安全问题导致了互联网企业对其产品、用户对其电脑和各种服务产生了安全防护需求;随着安全问题的日益严重,这种需求可能伴随着集体恐慌、对服务便利的期待、互联网商业模式的刺激、政府的默认和鼓励等因素而日益高涨。同时,网络安全服务企业还试图成为互联网"入口"或"平台",提供安全以外的诸多服务以扩大市场份额,甚至要垂直整合互联网不同层面的应用和服务。从整体上看,互联网巨头们试图提供排他服务的意图与对云计算的追求将会极大减少终端设备的创生性,使互联网架构变得更加封闭可控,减少互联网创新的规模,对互联网发展的控制权从边缘逐渐回到中心。

关键词 3Q大战 互联网 网络安全 隐私 创生性

2010年底的腾讯QQ与奇虎360的战争(以下简称"3Q大战")引发了对中国互联网企业问题的重大讨论,除了普通用户与网络推手在网上表达的或真或假的意见之外,较为严肃的讨论主要集中在涉及的法律问题(例如隐私、恶意软件、不正当竞争、垄断)[1]和企业的社会责任。[2] 这些讨论往往就一个单独的话题进行分析,缺乏与其他话题的联系,也没有看到引发这些话题的真正原因和实质。例如,在关于网络隐私的讨论中,主流意见认为显然应当加强法律对网民隐私的保护力度,但矛盾在于:安全和隐私是一枚硬币的两面,安全软件提供商只有

* 上海财经大学法学院讲师。感谢沈明、欧树军提出修改意见,文责自负。

〔1〕 参见王雅平:"'停战以后'——由中国互联网产业'3Q大战'所引发的法律思考",《中国电信业》2011年第01期。

〔2〕 参见蓝狮子编:《X光下看腾讯》,中信出版社2011年版。

在对用户电脑进行扫描的基础上才能查杀病毒，提供更加方便的服务，其前提是用户对提供商的信任。这一信任的极端版本是“云计算”，即用户的全部信息和文件全部存放在服务商的中心服务器，用户甚至不必拥有自己的上网设备，只要一个经过认证的密码即可随处使用各种云端服务。如果用户信任安全软件提供商，目前的安全软件侵犯用户隐私的指控就不复存在，因此问题不在于扫描行为本身，法律不能解决这样的问题。

本文试图从网络安全的角度重新解读这一事件及其相关法律问题。[3] 认为是网络空间的安全问题导致了互联网企业对其产品、用户对其电脑和各种服务产生了安全防护需求；随着安全问题的日益严重，这种需求可能伴随着集体恐慌、对服务便利的期待、互联网商业模式的刺激、政府的默认和鼓励等因素而日益高涨。同时，网络安全服务企业还试图成为互联网的“入口”或“平台”，提供安全以外的诸多服务以扩大市场份额，甚至要垂直整合互联网不同层面的应用和服务。从整体上看，互联网巨头们试图提供排他服务的意图与对云计算的追求将会极大减少终端设备的创生性，使互联网架构变得更加封闭可控，减少互联网创新的规模，对互联网发展的控制权从边缘逐渐回到中心。这一趋势随着互联网逐渐转向移动领域而变得愈发明显。3Q 大战的实质是一场争夺用户桌面和终端设备的战争，软件不兼容正是这场战争中不可或缺的标志性战役。

本文的结构如下：第一节简要讨论网络安全带来的新问题及其防护模式，其特征是由私人安全软件企业向社会提供广泛的服务，其模式经历了一个从产品到服务的转变以回应日益严重的网络安全威胁。第二节分析 3Q 大战的过程，特别强调网络安全是这一事件的导火索，并且同样是隐私安全引发了网民的集体恐慌，其后果是用户纷纷转向声称自己更加安全可靠的安全软件公司。第三节从流行的法律分析入手，探讨传统的隐私、恶意软件、不正当竞争乃至垄断如何镶嵌在这一具体事件过程中，作为解决个案纠纷的法律分析并不能阻止或有效规制 3Q 大战背后隐蔽的商业逻辑。第四节进一步展开这个商业逻辑，即互联网企业（包括安全软件企业）成为互联网入口或平台的企图，这一企图和实践在中国缺乏有效市场竞争规则和创新激励的环境下迅速膨胀，导致少数巨头做大，其后果是在内容层和应用层，它们将主导形成一个更加封闭的互联网架构，并在表面上可以消解既有的法律问题。第五节着重分析两种互联网架构的理想类型：开放与封闭，并简要讨论我们该如何在日益严重的安全威胁下保持两种状态之间的动态平衡，建构一个繁荣开放而又安全的互联网。

一、谁保护网络空间？

网络安全问题既同互联网原初架构有关，也同作为主要终端设备的个人电脑有关。首先，根据经典的“端对端”原则（end - to - end principle），互联网的设计应该尽量保持数据传输过

〔3〕 本文分析的网络安全，仅仅指计算机系统、终端设备和基础设施的安全问题，主要包括系统病毒、漏洞攻击、黑客入侵等等，并不包括信息内容安全。

程的简捷，将对数据的认证置于终端而非传输过程之中。[4] 互联网独特的 TCP/IP 协议将数据分割成若干数据包，只有在传输至终端设备时才能被重新组装，成为完整的信息，在此过程中运营商无法得知数据包的内容。其次，作为终端的个人电脑和操作系统使得用户有能力编写病毒和恶意程序，并极易迅速扩散至整个互联网。[5] 自从 1988 年世界上第一例蠕虫病毒"Morris"出现以来，世界上各种病毒、木马和网络攻击层出不穷，严重威胁到互联网的繁荣和用户数据的安全。[6] 特别是制造网络病毒逐渐成为一种有利可图的产业，网络安全就基本上成为伴随互联网扩散的常态问题，且愈演愈烈。第三，随着互联网的服务和应用程序愈加多样和复杂，市场竞争愈加激烈，很多未经安全审查的软件程序常带有某些缺陷和漏洞，从而使得病毒和恶意程序有各种机会入侵个人电脑。用户会下载使用各种软件，但缺乏足够的警惕和技术能力进行自我保护，也无法判断软件质量与安全风险。[7]

由于互联网一开始是一个超越国界的匿名开放系统，在无法根本改变其原初架构的情况下，针对其弱点，网络安全防护就有必要从信息流通的端点入手。现实中至少有如下几种选择：首先，对国家而言，为保护本国网络使用者免受来自国外的攻击，可以控制本国网络同其他国家网络连接的出口，并在出口信道设置入侵检测系统以排查可疑的数据包。但是这样做要受到本国通讯和言论法律的制约。其次，互联网骨干和接入运营商（以下统称 ISP）逐级进行安全防护，这就违反了"端对端"原则，可能受到公众质疑以及国家的监管。当然国家也可以制定法律要求它们承担安全责任。第三，同理，互联网内容和应用服务商（以下统称 ICP）为了保障交易和服务安全、保护用户信息免受攻击侵犯，也会采取安全措施，国家也可以施加法律责任。最后，由用户自主选择在电脑终端安装安全软件，防护本地个人资料。在不同的国家，以上四点措施可以综合运用，也可以偏重于某些端点。另外，无论谁来实施防护，所需的安全系统可以由国家统一提供，也可以由专门的安全软件企业提供。由于软件产品复制与分发的成本为零，软件提供者的前期研发投入与后期技术更新就成了关键的问题。

和前互联网时代的武器制造与使用相比，发动网络攻击的技术门槛大大降低，并使以国家为目标的网络战与一般的网络攻击之间的界限模糊不清，原先存在于核战争时代的战争规则与策略也不再适用。[8] 面对不确定的网络攻击，国家无法像提供传统公共品一样承担整个网

---

〔4〕 J. H. Saltzer, et al., "End - to - end Arguments in System Design", 2 *ACM Transactions on Computer Systems*, issue 4 (1984), pp. 277 - 288.

〔5〕 这被称为个人电脑的"创生能力"(generativity)，见齐特林："创生性的互联网"，《数字时代阅读报告》2010 年第 3 期。电脑病毒同生物病毒的不同之处在于，电脑病毒永远不会被清除消灭，而会一直存留在互联网上，等到时机成熟便会大规模爆发。见巴拉巴西：《链接：网络新科学》，湖南科学技术出版社 2007 年版。

〔6〕 OECD, *Computer Viruses and Other Malicious Software: A Threat to the Internet Economy* (2009); Mark Bowden, *Worm: The First Digital World War*, Atlantic Monthly Press, 2011.

〔7〕 此处涉及的另一个问题是软件产品质量责任的问题，这牵涉到软件的生产流程、行业竞争环境和法律的缺位，不加展开。

〔8〕 Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It*, New York: Ecco, 2010.

络空间的防卫，而只能聚焦于国家基础设施和政府部门信息设备的安全；同时由社会中大量的企业和个人用户负责自己的安全，安装安全软件采取私力救济。[9] 这样既可以减少国家不必要的财政支出，又可以通过市场竞争产生更好的安全软件服务。针对不同种类网络威胁提供独特产品，[10] 是有效率的资源配置方式。[11] 国家若采取传统防卫观念，认为互联网安全隶属于国家信息主权安全，那么在架构上就必然要求采取控制出口信道的做法，这样才能在第一道关口最大限度地防止病毒入侵，但成本极为高昂。[12] 这些措施都属于 Lawrence Lessig 提出的通过代码规制网络空间的行为，比单纯地立法禁止要更加有效。[13]

中国互联网自建设伊始就极为强调网络信息安全工作，早期为数不多的法规几乎全部侧重于这一方面。[14] 经过十多年的建设，国家已经建成较为完善的互联网安全防护法律和技术体系，[15] 确立了安全等级标准和应急处理程序，[16] 并向 ISP 和 ICP 逐级施加了安全责任。[17] 在架构上采取了监控互联网出口信道的做法，对国际流量进行防范检测。[18] 更重要的是，国家通过“双软认定”许可认定了一批网络安全企业，在统一技术标准的前提下向单位和个人用户提供安全服务。最近国家更有使用公共财政征集绿色软件的企图，通过向社会免费（甚至是强制）发放该安全软件，试图控制用户终端信息流通。[19] 该项计划的部分失败（至少成功在中小学电脑上推广安装）表明了网民对国家权力延伸至互联网终端的抵触，因为个人电脑被认为是私人领域，通过国家权力强制推行已经无法被欣然接受，即使是打着保护未成年人的旗号。[20] 无论如何，在相当长的一段时间里，网络安全由专门的安全软件企业向用户提供有偿服务来实现，国家缺乏提供此类公共服务的激励和能力。

---

〔9〕 和传统的国内安全保卫与军事防卫的二分法相似，网络安全防护也可以区分针对国内和国外的攻击。在中国，前者由公安部网络安全保卫局负责，后者由总参信息保障基地领衔。

〔10〕 例如，病毒、木马、网络攻击的对象和防护措施是不同的：病毒和木马通过文件或网页点击传播，前者可能造成文档感染和系统失灵，后者则为了窃取记录电脑密码，一般对文档不造成损坏；网络攻击更多地针对重要的数据库和服务器。入侵检测系统可以深入数据包查询，但无法防止被操纵的僵尸网络发起拒绝服务攻击。

〔11〕 Mark F. Grady, Francesco Parisi (ed.), *Law and Economics of Cybersecurity*, New York: Cambridge University Press, 2006.

〔12〕 当然，这道关的实际作用有限，原因包括：很多新型病毒从国内制造和传播；国外的威胁更多来自像拒绝服务（Denial of Service，DoS）一类的攻击，入侵检测系统无法阻止。

〔13〕 Lawrence Lessig, *Code: Version 2.0*, New York: Basic Books, 2006.

〔14〕 参见胡凌：“1998 年之前的中国互联网立法”，《互联网法律通讯》第 4 卷第 1 期（2008 年）。

〔15〕 《计算机病毒防治管理办法》。

〔16〕 《信息安全等级保护管理办法》，《互联网安全保护技术措施规定》，《互联网网络安全应急预案》，《木马和僵尸网络监测与处置机制》。

〔17〕 《电信条例》。

〔18〕 《国际互联网信道管理办法》。

〔19〕 参见胡凌：“内容过滤软件与互联网的治理”，《二十一世纪》2010 年 6 月号。

〔20〕 这个问题和本文主题紧密相关，虽然国家权力受到约束无法通过强硬方式渗透至终端，但商业力量可以轻易进驻网民桌面，其结果造成对终端更加软性而全面的控制，个人电脑也会转变成非私人的信息设备。

对网络安全软件企业进行认定和许可，是基于如下现实：占据中国互联网主流市场的 Windows 操作系统作为开放的操作系统允许开发者和企业编写各种新软件和应用程序，由用户自主选择安装使用。这些软件在操作系统中不能相互干涉，依靠各自的 API 接口运行于操作系统平台上。由于安全软件的重要，以至于需要单独核发许可。对软件提供商而言，安全软件同其他产品没有交叉关系，尽管他们可以开发其他应用软件，但和安全软件之间是相互独立的。安全软件可以单独下载安装，通过本地的病毒程序库认定用户是否感染了已知的病毒，如果是新型病毒则需要用户主动定期更新。[21] 安全软件需要对用户下载的文档和程序根据病毒库进行核对，并定期扫描硬盘，遇有安全风险时提醒用户采取措施。软件即服务（Software as a Service，SaaS）模式的兴起改变了人们对软件产品的认识，软件不再是一次性购买消费的应用程序，而是可以源源不断地提供更新和新功能的长期服务。[22] 对于安全软件而言，病毒库可以随时在线更新；对于新型病毒和未知程序，甚至可以不需更新病毒库直接提交到安全软件中心即时处理，这就是所谓“云查杀”。[23] 但无论如何，传统的安全软件行业始终坚持同其他信息服务相分离，靠出售软件赢利，市场份额是衡量安全企业业绩的最重要指标。

随着安全隐患威胁日益加重、安全软件企业的数量增多，市场竞争变得愈发激烈。安全软件原本只是应用程序之一种，但因为安全威胁而变得越来越重要，以至于用户对它们形成了强烈的依赖，甚至需要一个安全“总管家”来帮助管理个人电脑。但是当非安全软件企业涉足此类领域的时候，就不可避免发生抢夺用户桌面的矛盾和冲突。这就是 3Q 大战的导火索。

二、谁保护用户桌面？

在传统的病毒之外，木马程序和流氓软件逐渐兴起并形成一条完整的产业链。[24] 因为木马本身可以悄然隐藏在用户电脑中，窃取用户资料和密码，给用户造成经济损失。对主要的信息和应用服务提供商而言，如果不能确保用户的桌面安全，就无法向他们提供稳定高效的服务，可能会面临用户流失的问题。这个问题对腾讯而言极为严峻，作为中国最大的即时通讯公司，腾讯逐渐将业务扩展至娱乐、信息服务、增值服务等领域，用户可以通过一个 QQ 号码登入统一的终端，享受“一站式”服务。那么 QQ 号码的价值就不仅仅是好的号码数字（比如吉利易记的数字、或位数少的以表明自己是老用户），而是背后一整套个人数据和财产。从 2005 年

〔21〕 早期的安全软件用户在购买软件之后，需要每周到服务销售点领取最新的病毒库磁盘。见徐晓辉等：《梦想金山：一个坚持梦想的创业故事》，中信出版社 2008 年版。

〔22〕 参见胡凌：“从‘治理软件’到‘通过软件的治理’”，《北大政治与法律评论》2011 年第 2 期。

〔23〕 云查杀模式赋予安全软件公司极大权力，在缺乏约束的情况下可以决定任何软件的生死，其背后还是用户的信赖和恐惧问题。见《南方周末》对马化腾的采访，http://www.infzm.com/content/52334，最后访问日期：2012 年 2 月 27 日。

〔24〕 互联网实验室：《中国流氓软件及治理对策研究》（2006 年 12 月）。

起,窃取 QQ 账户已经慢慢发展为集团犯罪行为,有着极为详细的分工流程:制作传播木马——窃取 QQ 密码——窃取其他 QQ 财产信息——转卖账户——猜测用户其他密码(如网络银行)——进行其他犯罪活动。如果用户持续遭受这样的损失,将会有不少人放弃使用 QQ。因此保护用户的 QQ 账户安全就是保护腾讯自己的市场,其要点在于帮助用户抵御猖獗的木马侵害。

除了求助于政府,[25]依靠用户自我保护以外,腾讯决定开发安全模块保护自己的应用程序,这就是 QQ 医生。[26] 最初的 QQ 医生只针对威胁腾讯账户的木马,但如前所述,开放的操作系统平台允许用户自主安装使用未经安全测试的软件,安全风险无处不在。一旦 QQ 成为用户日常的主要应用程序,一旦腾讯提供的一站式服务成为用户主要的网络活动,其安全检测势必要扩展到整个桌面系统甚至整个电脑硬盘,因为在理论上用户的任何网络行为和电脑使用行为都将潜在地威胁 QQ 账户的安全。那么 QQ 医生更进一步成为整个电脑的大管家就势在必行,这就是后来推出的升级版 QQ 电脑管家,从名称即可看出腾讯的意图。由于电脑管家是镶嵌在 QQ 的终端软件中的,用户只需要正常登陆 QQ 即可以享受安全保护,不再需要其他安全软件。很明显,腾讯借助庞大的用户群推广自己的新服务,这对传统的安全软件商而言是重大挑战。[27]

这就和另一款市场占有率颇高的网络安全软件 360 发生了冲突,其提供商奇虎 360 公司以查杀木马病毒著称。[28] 按照奇虎公司的逻辑,自己是专业的安全软件提供商,正在扩展市场份额,不愿意放任半路杀出的腾讯占领自己的领地,特别是后者可以凭借其庞大用户迅速扩张。[29] 但通过正常的市场竞争无法一下子挽回失去的用户,在互联网服务市场不正当竞争,监管比较模糊的情况下,奇虎放手一搏,试图激发用户恐慌来放弃使用 QQ 电脑管家,于是通

---

〔25〕 深圳市公安局将保护虚拟财产作为打击网络犯罪的头等大事,主要的受益对象就是腾讯,因为腾讯作为深圳的地方大型企业,有必要进行特殊保护。深圳市公安局已经破获了几个全国性的 QQ 号码盗窃团伙。参见《深圳市公安局 2010 年度公共服务白皮书》。类似地,盛大也和上海市公安局浦东分局合作成立"盛大警务室",加强对虚拟物品的保护。因为普通用户个别的网络物品被盗往往无法确认价值,在警力资源有限的情况下,只有达到价值 1 千元的标准公安机关才会立案侦查,就有必要由互联网公司出面统一报案。需要注意的是,政府保护的基础不是保护用户的财产,而是腾讯的财产,因为按照《软件许可及服务协议》,QQ 号码所有权属于腾讯。

〔26〕 开发安全软件程序保护自己的主要应用服务的做法比较常见,例如支付宝也开发了安全控件,用户如不下载安装则无法使用。

〔27〕 腾讯以不断扩展为特征的商业模式被广泛批评为抄袭和模仿,借助庞大用户群打压专门市场中的竞争对手。见"狗日的腾讯",载《计算机世界》2010 年第 28 期。

〔28〕 奇虎董事长周鸿炜早年曾以设计一款流氓软件 3721 助手闻名,但后来转向网络安全领域,抗击病毒和木马,2008 年奇虎声称其断绝了中国境内的流氓软件产业链。见"奇虎称流氓软件产业链已基本消灭",载 http://it.people.com.cn/GB/42892/42927/115725/7709928.html。

〔29〕 参见《南方周末》对周鸿祎的采访,http://www.infzm.com/content/52335,最后访问日期:2012 年 3 月 9 日。

过开发隐私保护器广为宣传 QQ 正在扫描用户的电脑、窥探他们的隐私。[30]

对绝大多数技术盲用户而言,这一宣传引发了极大的恐慌,他们不是仔细审查奇虎提交的证据,而是先行卸载或停用 QQ,并倒向同样扫描用户电脑的 360。[31] 媒体和公共知识分子没能起到应有的作用,反而给人站队攻击对手的不良印象。[32] 腾讯(以及奇虎的竞争对手们)和奇虎双方都雇佣了大量网络水军,在各种论坛和信息平台上造势,更加剧了问题的模糊。

奇虎深知无法通过似是而非的指控动摇腾讯的主导地位,自己也尚无能力扩展至其他服务领域取而代之,只能争取牢牢控制网络安全服务市场。只要用户不再使用电脑管家,双方即可相安无事。但问题就在于电脑管家镶嵌在腾讯一站式服务的软件架构中,用户只要安装 QQ 就会自动开启使用,若要阻止用户除了恐吓,还有必要采取技术措施。这就是所谓"扣扣保镖"的目的。安装"扣扣保镖"的非会员用户会发现 QQ 安全防护的按钮已经被悄然取代,并且还有屏蔽 QQ 上嵌入的幅式广告的诱惑。此举不仅妨碍了腾讯自我防护的长远意图,更直接减少了其广告收入。于是腾讯一边向法院起诉奇虎不正当竞争,一边采取果断的技术措施,这个"艰难的决定"就是宣布两款软件互不兼容。尽管其本意是"让用户先删除 QQ 下网避开,或者等过一段时间再装回来",[33] 此举还是激怒了网民,认为是凭借市场地位对他们的要挟。

对腾讯而言,任由用户安装扣扣保镖未必会像马化腾声称的那样"再过三天,QQ 用户有可能全军覆没",[34] 毕竟用户只是更换了安全软件,还在继续使用其他 QQ 服务;也未必能大幅减少广告收入。[35] 关键在于:第一,扣扣保镖允许用户卸载腾讯的其他捆绑服务,并禁止 QQ 软件升级自救;第二,在马化腾看来,它可以诱导用户备份好友列表,从而顺利获取这些有价值的信息,为 360 最终开发即时通讯软件做准备;[36] 第三,它开了一个极具破坏力的先例:其他腾讯服务的竞争者们可以群起效仿,纷纷开发独立的插件屏蔽腾讯的诸多服务,例如网络

---

〔30〕 奇虎提供了 QQ 电脑管家运行的截图,但从未详细说明此种扫描对安全防护是否必要,是否真正威胁到用户私人信息的安全,是否回传个人信息。相反,随后奇虎扫描搜集用户信息的证据被其竞争对手金山公司披露,最后也不了了之。

〔31〕 这被认为是腾讯长期公关工作的失败,并没有提供一种深刻的价值将用户聚在一起,用户也只是从实用角度使用 QQ,没有根本的认同。参见蓝狮子编:《X 光下看腾讯》,见前注〔2〕。

〔32〕 这部分是因为懂技术的公共知识分子较少,无法就技术问题解惑,媒体也没能组织专业人士进行讨论。尽管金山公司出具了对奇虎证据的反驳意见,腾讯也发表了声明,但人们并不在意。退一步说,马化腾和周鸿祎在接受《南方周末》专访时都用较大篇幅说明安全问题是引发两者争斗主要原因,但盛行的外界评论却很少提及这一问题,造成公众认识上极大的盲点。

〔33〕 《经济观察报》对马化腾的专访,http://www.eeo.com.cn/industry/it_telecomm/2010/11/05/185013.shtml,最后访问日期:2012 年 2 月 27 日。

〔34〕 同上注。

〔35〕 腾讯放置在聊天客户端的幅式广告曝光率很高,在腾讯发展早期起到重要作用。但随着腾讯业务的扩展,客户端广告收入所占比重逐渐减少,更多的广告被放置在腾讯网和微博上。

〔36〕 《经济观察报》对马化腾的专访,见前注〔33〕。这一点在 360 首席架构师李钊看来是"被人利用了",并暗示传出的伪造证据是雷军和从奇虎离职的安全卫士总经理傅盛所为。见李昭:"傅盛离职内情:从 360 叛将到腾讯马前卒",http://blog.sina.com.cn/u/2460042820,最后访问日期:2012 年 2 月 27 日。本文则试图说明,不论具体原因如何,只要个人电脑还是网民上网的主要终端,3Q 大战就不可避免。

游戏,从而肢解统一的一站式服务,这将是对腾讯"帝国式"商业模式的沉重打击。由于竞争规则的模糊,缺乏有说服力的先例,法律启动和运行的过程极为缓慢,[37] 动员媒体号召公众也无法获得信任,采取不兼容的举措、鲜明地宣示立场似乎是马化腾仅有的杀手锏。

在工信部的协调下,最终两家公司和解,恢复兼容。尽管双方互有损失,[38] 但腾讯更大的教训是认识到其商业模式和架构在当下不良竞争环境中的脆弱性,加紧整合各种服务的步伐,并坚持开发安全产品。[39] 而奇虎则借此名声大噪,还成功在美国上市,巩固了其安全软件的市场地位。[40] 本文关心的问题是,经由 3Q 大战,中国互联网巨头通过网络安全问题整合资源,争夺用户,并形成较为明确的商业目标,造成互联网架构的集中。在详细分析这一模式之前,下一节将简要分析涉及的几种法律争议及传统解决方案。

三、主要的法律争议

(一)隐私

腾讯扫描用户电脑是否侵犯隐私,这首先取决于用户对个人电脑的法律属性的认识。比照传统观念,人们普遍认为储存在自己电脑上的一切文件和软件程序都是私有物品,如果有人翻查、扫描或记录就是侵犯了隐私,无异于未经同意就闯入房间搜查。按照这样的想法,无论是 QQ 还是 360 实际上都扫描了用户的电脑,都有能力记录用户的上网行为,都可能侵犯了隐私;而这是任何安全软件得以生效的前提,如果不能扫描,也就无从得知何处藏有病毒。问题的关键在于,在个人电脑产生的相当长的时间里,这种最高标准的隐私观念往往无视隐私与安全的妥协,当病毒和网络攻击猖獗的时候,人们不得不安装安全软件,允许它们仅仅根据病毒程序类型和特征防护安全,其基础在于对软件提供商的信任。[41] 只要安全软件不涉及用户的

---

〔37〕 在 3Q 大战之前,奇虎同百度、金山发生过诸多摩擦,相互起诉对方不正当竞争,但大多没有宣判。腾讯诉奇虎的一审直到 2011 年 4 月才宣判,法院判决奇虎因不正当竞争赔偿 40 万元,这时奇虎已经成功上市,这种赔偿既不能威慑,也不能弥补对手失去的市场份额,甚至连象征意义也不具备。二审判决更拖到了 2011 年 9 月底,距离 3Q 大战已近一年。同理,2011 年 5 月北京一中院判决奇虎诋毁及强行卸载金山网盾等行为构成不正当竞争,赔偿金山 30 万元,几乎也不起作用。

〔38〕 马化腾估计有 2000 多万台装有扣扣保镖的电脑受到强制性影响卸载 QQ,占腾讯总用户的 15%,360 安全卫士则损失了 20% 的用户——3 亿用户中的 6000 万。

〔39〕 腾讯于 2011 年推出了开放平台,将其属下的应用服务向开发者开放。另外根据马化腾在 3Q 大战终审胜诉后的一封内部邮件,"安全是所有互联网服务的基石,而我们的安全产品是肩负着用户与合作伙伴的双重责任。所以我们必然要加倍重视,把安全这个产品和服务做到极致。我们会长期关注和大力投入安全领域,不会懈怠",http://tech.ifeng.com/internet/detail_2011_09/30/9592989_0.shtml,最后访问日期:2012 年 2 月 27 日。

〔40〕 有分析认为马化腾的不兼容决定是周鸿祎没有想到的,否则奇虎将会使中国互联网市场变得更加黑暗;腾讯的反击使奇虎不得不借助外力结束这场由它自己挑起的战争。见铁军:"狩猎:我看 3Q 大战",http://hi.baidu.com/litiejun/blog/item/c58d34ce2444f129b700c86a.html,最后访问日期:2012 年 2 月 27 日。

〔41〕 腾讯诉 360 不正当竞争案的一审法院认为,QQ2010 软件监测提示的可能涉及隐私的文件,均为可执行文件,涉案的这些可执行文件并不涉及用户的隐私。二审法院也认为,根据现有法律,360 并没能充分证明腾讯的安全软件侵犯了用户的隐私。

信息内容就是可以信赖的,这有赖于一个专业的知识共同体的监督。因此,网络隐私的标准应当降低一级:安全软件的功能应当仅限于查找发现可疑的程序,并告知用户可能的风险。但是如果安全软件超出了其许可范围,扫描了其他不相关的文件,并记录用户的可识别身份信息(例如浏览记录、使用其他软件情况、密码等,且不论用于何种用途),就无疑违反了隐私的最低标准。但安全软件公司的云查杀模式已使得本地扫描变得不必要,回传相关信息可以精确定位新型病毒,这更增加了侵犯隐私的风险。

360 利用公众对隐私内涵的模糊理解和腾讯公关的失误广为宣扬,令公众对腾讯产生了深深的不信任。360 的宣传策略是说,QQ 安全防护是不专业的,不值得信赖;同样是扫描病毒文件,用户只能相信作为专业安全软件公司的 360 自己,这和它对腾讯的指控显然是矛盾的。用户因为一开始的广泛宣传形成恐慌,凭直觉他们也愿意相信自己的隐私遭到威胁,却宁愿接受 360 软件长期而稳定的监控。即便后来当人们发现扣扣保镖劫持 QQ,360 贮存用户的上网信息的时候,也会更愿意接受 360"给用户自主选择"的说法,这是一种先入为主的效应。

但实际上,最高隐私标准背后的精神在于独立和自主,这一理念产生于前互联网时期的长期实践。[42] 信息技术则将这种得到物理架构庇护的权利变成某种"信息隐私",个人数据可以被大规模挖掘搜集、聚合、处理和利用,实现政治和商业目的。[43] 特别是当个人信息被广泛搜集之后可以被用来提供个人化服务的时候,独立和自主已经慢慢遭到侵蚀,这远远比扫描硬盘的行为更为强大。下文将要说明,未来的信息服务将不会受到这种法律指控,却可令用户进一步失去自主权。[44]

(二)恶意软件和不正当竞争

按照现有的官方定义,扣扣保镖属于破坏技术保护措施的外挂程序,劫持了 QQ 自己的安全软件,并通过过滤腾讯广告的方式侵害了其利益。[45] 在互联网发展史上,很多恶意软件往往是主流应用软件的辅助软件,它们寄生于主流软件麾下,在不损害主软件服务商利益的条件下会增加该软件的价值,帮助用户更好地了解和应用,并形成产业链。但是由谁来开发辅助软件就成为涉及市场竞争的问题。主流软件开发商可能会禁止其他企业开发该种产品,而想自己提供全套服务,并防止本软件的缺陷被其他企业利用。其他企业的行为就被称为"外挂"或"恶意软件",受到法律的笼统禁止,但其提供的服务很可能是对用户有利的。360 开发扣扣保

---

〔42〕 Alan F. Westin, *Privacy and Freedom*, New York: Atheneum, 1967; W. Prosser, "Privacy," 48 *Cal. L. Rev.* 383 (1960); Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy", 4 *Harvard Law Review* 193 (1890); I. Altman, *The Environment and Social Behavior*, Brooks/Cole, 1975.

〔43〕 参见胡凌:"信息生产与隐私保护",载苏力主编:《法律和社会科学》第 5 卷(2009 年)。

〔44〕 腾讯的《软件许可及服务协议》单方面规定了隐私的界线:个人隐私指"那些能够对用户进行个人辨识或涉及个人通信的信息,包括下列信息:用户的姓名,身份证号,手机号码,IP 地址,电子邮件地址信息"。而非个人隐私指"用户对本软件的操作状态以及使用习惯等一些明确且客观反映在腾讯服务器端的基本记录信息和其他一切个人隐私信息范围外的普通信息"。因此对诸如使用习惯和偏好的分析就不会违反隐私法律,因为那更多是通过软件程序自动完成的,用户也感觉不到被侵犯。

〔45〕 《恶意软件定义细则》。详细的分析,见周汉华:"对 360 隐私保护器、扣扣保镖相关法律问题的分析",http://www.iolaw.org.cn/showArticle.asp? id=2766,最后访问日期:2012 年 2 月 27 日。

镖的理由是，它给予了非成员用户更多的选择权，让他们可以摆脱内嵌广告；而这正是腾讯收入的一个重要来源。但同时不应忽视的是，作为云查杀安全软件提供商，奇虎自己也握有极大权力来规定哪些软件属于恶意软件，之前已经和很多其他安全软件不相兼容。[46] 360 的目的很明显，就是采用强硬手段和 QQ 争夺用户桌面，阻止腾讯开发自己的安全软件。只有当主流软件升级为平台的时候，其外挂才能顺利转型为独立的产品，相互促进共同升值，而不是原来的竞争关系，外挂问题也会逐渐消失。

除此之外，两个阵营都采用了不正当竞争手段，他们动用大量网络推手攻击对方，侵害对方名誉，让用户无所适从。[47] 尽管 QQ 也采取了法律手段，但由于网络用户的非理性选择，如不采取紧急避险措施，很可能威胁腾讯的市场占有率和商业模式；它也没有采取无休止的劫持手段，而是以让用户自己决定为名义宣布互不兼容，实际上相当于逼迫用户进行两难选择。在这个过程中，很难说谁的行为更加道德或正当，当恶性竞争启动时，这一结果已经不可避免地发生了，这是它们争夺桌面的最终目标决定的。

（三）垄断

腾讯的行为已经超越了传统意义上的垄断。传统经济学和法律上的垄断需要对单边市场进行界定，并计算市场份额，判断是否有滥用支配地位的行为。[48] 但是互联网企业拥有很多种产品和服务，属于新型的多边市场，不同市场相互交叉补贴，很难判断是否属于垄断。[49] 例如，腾讯虽然占据即时通讯市场，但在网络音乐、游戏、增值服务等领域均无法和其他专门的巨头相比。[50] 也就是说，腾讯的诸多服务是交叉补贴的，有些并不盈利但可以吸引大量用户，在吸引到用户和流量时再赚取广告和增值收入。人们常常以微软垄断案为类比主张对腾讯的拆分，但论者往往忽视的是，微软主要是因为其操作系统平台捆绑了自己开放的音乐播放器和浏览器，是平台和之上的应用程序之间的关系，捆绑一定会造成排他效应。但腾讯的即时通讯同其他服务是平行的关系，尚没有严格证据表明其即时通讯的市场份额同时造成了其他单独服务市场份额的独占。[51]

上述争议如果按照传统法律分析，可以给出标准答案，但无法解决问题，因为他们没能同

---

〔46〕 和 360 产品不兼容的软件包括金山、瑞星、遨游、百度，以及最近的可牛。据傅盛单方面宣称，可牛甚至遭到了封杀，在产品还没上市之前，360 的病毒库中就已经将其列入。

〔47〕 《反不正当竞争法》。3Q 大战后，工信部出台了《互联网信息服务市场秩序监督管理暂行办法（征求意见稿）》和《互联网信息服务管理规定（征求意见稿）》，希望加强互联网信息服务市场秩序规范。中国互联网市场的不正当竞争比比皆是，不仅竞争法软弱无力，政府相关部门作为看得见的手更加肆无忌惮，例如安全软件行业就因为计算机信息系统安全专用产品检测和销售要由政府许可而出现了像“微点案”这样的冤案。

〔48〕 《反垄断法》第 18、19 条。

〔49〕 Eisenmann, T. R., G. Parker, and M. van Alstyne, “Strategies for Two - Sided Markets”, *Hapvard Business Review* 84, No. 10(October 2006)；李剑：“双边市场下的反垄断法相关市场界定”，《法商研究》2010 年第 5 期。

〔50〕 参见谢文：《为什么中国没出 facebook》，凤凰出版社 2011 年版。

〔51〕 互联网实验室《中国互联网行业垄断状况调查及对策研究报告》（2011 年）认为，腾讯、百度等企业的市场地位已经构成“多方市场垄断”，其判定“具有隐蔽性，即用免费市场上的垄断掩盖了收费市场的垄断得利”。这实际上已经超越了传统的垄断概念，相关认定也更加复杂。

新经济的商业模式联系在一起，也就无从反映现实的快速变化。如果我们换个角度思考，下一节将表明，腾讯与360行为的共同本质毋宁是努力成为互联网不同层面的“入口”，向用户提供一站式服务，最终提供排他的整个互联网服务，将不同层面（内容层、代码层、物理层）垂直整合在一起。它们不是提供开放的平台，而是要赢者通吃，减少其他互联网公司的创新。上述法律争议都可以通过架构改变而得到解决，3Q大战在这个意义上就不是单纯的法律问题，而是网络巨头们庞大的帝国野心的一个微小征兆。

四、互联网“入口”与新经济的商业模式

不难发现，尽管安全问题是3Q大战的导火索，但背后的深层次问题是安全软件服务的自我定位。如果安全问题只是对操作系统平台的防护，那么对用户而言，使用哪家产品都大同小异，只要严格禁止不正当竞争，最终的桌面市场份额还是要通过更好的服务来获得。但有战略眼光的互联网公司早已不满足提供某一类单一市场的产品，即使其产品能够迅速在线更新。它们关注的毋宁是创造一个一站式入口，并排他地提供互联网使用的大多数服务。即使这些服务在严格意义上并没有达到市场支配地位，但服务之间的交叉补贴为扩展市场提供了较大的空间。我们已经看到腾讯、百度、奇虎360等公司已经显露出这样的姿态，一方面它们凭借既有的优势产品服务（即时通讯、搜索、安全软件）稳定市场份额，并积极扩展业务，所有这些业务都镶嵌在一个（或一揽子）一站式的入口程序中，例如浏览器和聊天客户端。这些业务主要由自己的研究团队开发，但它们也开始开放部分平台，允许众多程序开发者在其上开发大量应用程序，这大致对应着谷歌（以html5为特征的浏览器云计算平台）和苹果（iOS操作系统）模式，它们都在逐渐架空和取代现有的Windows操作系统，甚至有取代个人电脑之势。[52]

这样的模式是如何形成和演变的呢？让我们先回到互联网经济的基本模式。互联网在九十年代中期向商业力量开放，并一直由商业力量和伦理主导其架构变化。中国引入互联网的主要目的之一也是加强信息技术和信息产业，这样我们就可以对比中西方互联网的商业模式。概括说来，新经济的特征是“免费”。[53] 企业通过提供免费的内容（新闻、音乐、影视、游戏）换取用户的时间、注意力和粘度，再通过收取广告收入实现赢利。增值收入是另一种方式，通过向用户收取少量服务费用实现。比较好的模式是向用户提供个人化的定制服务，精确地定位用户的偏好和个人信息，从而预测和推荐。这就需要广泛地搜集用户信息，这些信息可以被转卖给其他商家，加快网络个人档案的整合。因此提供多方面的服务就可以产生规模效应，对用户的信息掌握得越多，就越可以向用户投放有针对性的广告，并提供更完善的服务。在一个复杂的商业创新生态环境中，不同的产品尽管分属不同的市场，却可以交叉补贴：某些服务向用

〔52〕 未来的互联网趋势究竟是以Web为主还是以Internet的交互性为主，仍有很大争议。参见Kevin Kelly：“Web已死，Internet永生”，http://www.techweb.com.cn/news/2010-08-19/664571.shtml，最后访问日期：2012年2月27日。

〔53〕 参见安德森：《免费：商业的未来》，中信出版社2009年版。

户免费(例如视频),同时在另一些服务收取增值收入(例如会员资格)。因此互联网企业不再是传统的单边市场上单一产品的供应商,它们提供着两个或两个以上市场中的产品,这些产品的市场占有率要分别计算,很难估算一个整体性的市场支配地位。

这个意图的最终目标是成为互联网"入口",只要占据了入口,任何用户使用互联网都必须经过自己的领地,就可以永远立足。[54] 互联网可以大致分为内容层、应用层、代码层和物理层。[55] 在每一个层面我们都可以发现互联网巨头努力成为该层入口的努力,例如,在内容层,门户网站提供海量的信息,为了将用户尽可能地留在本站;与之对应的则是搜索引擎,为了让用户迅速离开本站(但以个人搜索信息为交换)。在应用层,可以开发自己的浏览器、即时通讯客户端、安全防护客户端,将很多服务以按钮的形式镶嵌在上面,用户即可通过这些软件完成全部互联网工作。在代码层,可以开发独占的操作系统,其源代码有封闭与开放之分。在物理层,少数电信运营商垄断电信服务和移动互联网服务,这实际上是将上述几个层面的垂直整合。另外,随着云计算技术的成熟和移动终端的兴盛,用户的数据完全可以存贮在服务商的终端服务器中,服务商可以在后台运行安全扫描,用户不能知晓和控制,任凭服务商对其文档和信息进行扫描分析,根本不需要回传信息这样的引起争议的行为。这样网络安全服务完全和其他在线服务融合在一起,它们各自获取的用户信息可以相互补充,为用户提供更加个人化的服务。

腾讯是中国最早探索这一模式的互联网企业之一,因为免费的即时通讯服务本身无法带来利润(甚至是广告收入,比如聊天软件上面空间有限),必须扩展至其他领域进行互补,这是典型的多边市场中的交叉补贴行为,也摸索出一条实用的赢利之路。百度和腾讯没有发生过正面冲突,因为百度主要是基于浏览器网页服务,与腾讯的软件客户端并没有直接关联,因此也在利用其搜索引擎的绝对优势开发应用平台。[56] 安全防护软件的地位非常微妙,如果没有疯狂的盗号行为,很难预测腾讯会向安全领域进军,但其应用整合的意图已经逐渐明晰。[57] 对于像奇虎 360 这样的安全软件公司,为了巩固安全软件市场地位(同时也是路径依赖),不仅要和传统安全公司如金山和瑞星竞争,更要同腾讯这样的非传统安全公司展开争夺,其举措也是先采用免费策略占领市场和用户,再

---

〔54〕 业界长期有口号云:做流量不如做联盟,做联盟不如做导航,做导航不如做搜索,做搜索不如做客户端。实际上流量、联盟、导航和搜索都是收集个人信息的模式,但唯有客户端可以保持长久稳定的收入来源。

〔55〕 参见莱斯格:《思想的未来》,中信出版社 2004 年版。

〔56〕 类似的例子还有庞升东的 51.com,这是腾讯热忱的模仿者,但由于它主要基于浏览器,和腾讯没有利益冲突,因此腾讯能够接受这样的互补者。但当以彩虹 QQ(也为庞升东开发)和珊瑚虫 QQ 为代表的直接竞争模仿者出现时,腾讯毫不犹豫地进行了封杀回击。参见林军、张宇宙:《马化腾的腾讯帝国》,中信出版社 2009 年版;薛芳:《企鹅凶猛:马化腾的中国功夫》,华文出版社 2009 年版。

〔57〕 腾讯目前的模块化"蜂鸟"平台架构更像是曹操的巨型战舰,通过铁锁将不同种类的服务连接起来,表面上不怕风浪,但并不处于一个统一的平台上面,被逐个击破的风险较大。其技术、内部组织和资源调配机制决定了腾讯向开放平台转变的艰巨性。但腾讯另辟蹊径,进军手机终端,推出了采用云计算架构的手机 QQ 浏览器。值得注意的是,该架构也采用马化腾批评过的云查杀,更说明该项技术已经不可避免地被广泛采用。参见"腾讯刘成敏详解手机 QQ 浏览器云战略:将建开放平台",http://www.donews.com/original/201108/587531.shtm,最后访问日期:2012 年 2 月 27 日。

试图通过安全软件客户端或浏览器增加功能从而取代操作系统。[58] 尽管这三家公司都在高调强调平台建设和开放，但能否做到像英特尔、微软和苹果那样的“平台领导”还有待观察。[59]

五、互联网的两种未来

至此，我们可以在一个规范的意义上辨识互联网巨头所带来的互联网架构的转变。本文设想的第一种未来“理想类型”就是经由互联网入口模式而带来的一站式互联网，这可能最终由几家大型互联网公司提供，形成一个长尾式的产业链，但其创新要受到高度审查。[60] 其要点在于，少数互联网公司作为基础性平台向用户提供全部网络服务，以至于他们并不需要访问其他网站，全部只需要用一个实名认证的账户登录（未来可以是虹膜、静脉一类的生物信息）。为向用户提供更方便快捷的服务，网站掌握用户基本资料和偏好，并动态地预测用户的需求，提供完全个人化的信息服务。为确保绝对安全，用户的全部信息将存放在“云端”，一切网络活动都将在服务商的终端服务器中进行，现有的个人电脑将被取代，成为随处可用的信息设备。这就意味着现有的创生性的操作系统将不再能生产病毒，但同时也将丧失其创新能力，越来越多的用户变成纯粹的消费者，他们只是消费，鲜有创造（或者仅仅是通过某些特定服务软件“创造”，例如绘画和制图）。由此带来的结果必然是一个集中封闭的互联网架构，网络提供商甚至可能垂直整合物理层和应用层（请设想一下中国电信同腾讯的合并，并生产智能终端设备），集中资源和力量对服务器进行防护。广大用户将实际上不享有终端可以控制的隐私和个人自主（从而目前的电脑隐私问题被消解）。按照第三部分的论述，隐私在根本意义上意味着自主选择，但集中化的智能分析使得用户的个人信息可以得到精确预测，用户将变得更加依赖个人化服务，从而互联网公司对终端用户的控制变成软控制，用户乐在其中丝毫不感到压迫。[61]

目前的国家能力无法做到这一点，因为这一过程的转变涉及大量分散的市场信息、交易和

---

〔58〕 360 的免费策略在一开始遭到其他传统安全公司的打压，因为这无疑会极大减少它们的市场份额。但随着多边市场模式的明显和竞争压力增加，像金山、瑞星这样的收费杀毒企业也纷纷宣布其安全软件永久免费使用，而通过其他渠道补贴，整个安全软件行业的商业模式被彻底改变。其他领域像盛大那样的网络游戏企业也很早就意识到免费策略，参见刘琦琳：《免费经济》，商务印书馆 2011 年版。

〔59〕 安娜贝拉·加威尔：《平台领导：英特尔微软和思科如何推动行业创新》，广东经济出版社 2007 年版；姜奇平：“谁最有可能成为中国的互联网 OS?”《互联网周刊》2012 年第 4 期。

〔60〕 例如苹果公司拥有一整套开发规范，约束应用开发者，并对他们的产品进行严格审查，更禁止普通用户随意编写软件发布。苹果的 iOS 系统因此可以说是高度安全，和 Windows 截然相反，同时也减少了相当程度的创新。

〔61〕 在这个意义上说，本文的观点和流行的意见并不矛盾。这些意见认为互联网加强了人们的自由度，使他们得以从事之前做不到的事情、享受之前无法得到的服务和信息、并赋权给大众。这样的观念容易忽视硬币的另一面：新世界中崛起的信息巨头，以及我们作为交换而（永远）失去的东西。

私人成本，只有私人企业通过激烈而精细的市场运作和技术开发，才能最终实现。[62] 首先，促成这一未来的首要动力就是市场竞争，使得原来开放的操作系统和终端设备也逐渐转向垂直模式（例如微软和谷歌），特别是当互联网快速向移动终端发展的情况下。[63] 从长远来看，3Q 大战远未结束，巨头们的下一个目标便是生产操作系统（或替代品），控制手机生产市场，加强同电信运营商的合作，从而做到真正的垂直整合。[64] 原先的竞争只是发生在内容层或应用层，但未来的竞争将是三个层面整体上的割据与合纵连横。其次，网民的集体选择在封闭架构的形成过程中起到相当的作用。由于网络服务样式繁多，用户希望减少复杂的密码认证，最好由几家企业提供统一便捷的认证登陆，这已经成为普遍的趋势；[65] 由于安全软件不兼容带来的不便使用户也希望仅仅使用一种软件；[66] 另外，就像 3Q 大战暴露出来的，当集体恐慌超过理性思考的时候，他们就会拥抱暂时的安全而舍弃长远的自由。但问题在于，互联网架构一旦改变就很难恢复，以至于像 3Q 大战这样的冲突将把我们带进一个愈加封闭的网络世界。最后，国家的网络控制目前仍然属于某种硬控制，一旦国家默许这种转变，甚至将政治治理的逻辑慢慢转向商业运作的逻辑，学习、利用商业模式和组织，那么粗糙的硬控制将会转变为精细的软控制，表面上看来分散的权力实际上回归中心，使国家能力进一步增强。[67] 因此，商业模式的动力、国家的默许支持、用户的集体选择都无可避免地将我们卷入这样的未来，它们是这一转变的最大动力。

另一个较为温和的未来则需要在目前的状况基础上加以改进。我们被保证得以拥有具有较多创生性的开放式的网络架构，这个架构允许终端用户享有较大自主权和匿名性，但也需要承担保护自己的安全责任；个人电脑可以进行诸多创新，但也可能带来安全隐患。为使这个构架仍然保持着不同层面的相互独立和演进，从而允许每一层的最大限度的创新。个人的信息不会被系统地搜集，个人需要作出努力才能使用互联网服务，找到适合自己的信息，并针对安

---

〔62〕 类似的经验还包括实名制和安全软件，政府强制推行网络实名制和安装绿坝都无法达到商业网站和服务商通过市场扩展类似服务的效果。

〔63〕 Brian X. Chen, *Always On: How the Iphone Unlocked the Anything - Anytime - Anywhere Future——and Locked Us in*, Cambridge, MA: Da Capo Press, 2011。开放的智能手机操作系统仍饱受病毒的侵袭，这也许会成为其走向封闭的关键因素。

〔64〕 腾讯推出了定制手机，尽数整合全部 QQ 服务；另一个开拓方向则是 Q + 平台，力图取代现有的操作系统。其专属硬件和软件的整合尚需时日。

〔65〕 例如一些大型网站合作，允许各自的用户可以相互用自己的账号登陆而不用申请新账户，其背后是网站们分享用户个人信息的协议。

〔66〕 根据一项最新研究，国内安全软件之间广泛存在不兼容现象，可以极大消耗用户电脑资源，甚至造成功能缺失，迫使用户只能选择一种。参见上海交通大学“反恶意软件研究小组”：《安全软件兼容性问题白皮书》（2011 年）。

〔67〕 就在这次 3Q 大战过程中，有人提出政府“应建立实时高效整合化的网上公众服务与监管体系”，“在市场主要的互联网桌面客户端软件中，强制设置‘超级管理权限’，并内嵌‘网上 110’模块、‘网上 315’模块”，夺取“软件的最高管理权”。这种思路和争夺桌面的商业模式如出一辙。参见“律师称客户端软件已成第六大媒体，建议强化监管”，http://tech.sina.com.cn/i/2010 - 11 - 18/01264877449.shtml，最后访问日期：2012 年 3 月 29 日。

全威胁采取适度的自我防御。[68]

个人选择无助于阻止集体的自然选择。要想阻止第一种利维坦式的未来，同样必须依靠集体的力量。[69] 人脑无法体会到的长期价值（例如作为个人自主的隐私）就必须成为一种意识形态，甚至公民宗教，以至于要提醒人们像本能一样快速反应才可以，这就需要广泛的权利团体和媒体的呼吁，靠外在的理性声音来对抗人脑几百万年演化形成的直觉系统和恐惧本能，并需要社会的放大效应加以辅助补充。[70] 例如，需要不断提醒人们理性思考如下问题：封闭互联网架构可能对个人自主的侵蚀，以及集中化的云计算未必能确保绝对安全。[71]

目前的隐私法和反垄断法都无法阻止正在发生的互联网架构大转型，因为其中涉及的隐私和垄断观念并不能直接反映新经济的要求。同时，立法者既没有看到用户隐私和个人信息与新经济的商业模式之间内在的隐秘联系，也没能预见作为硬币另一面的安全问题会促使网络服务商们采取极端措施、铤而走险。3Q 大战折射出的、更重要的用户自主、创新繁荣与开放架构的复杂关系更不可能逐一反映在法律中。法律在新世界似乎无能为力，但至少这次事件为监管者提供了管窥全豹的些许机会，我们需要重构财产、隐私、垄断等法律观念和制度。[72]

在中国，保持目前的互联网开放架构还面临着两大竞争对手，它们恰好是第一种未来的热烈拥护者：广电系统和电信系统。广电系统正在利用三网融合的机遇整合零散的地方广电网，尽管困难重重，但要紧的是其意图：将网络电视做成全国范围内最主要的信息设备终端，这样互联网将成为一个完全封闭运行的内联网。三家电信巨头虽然相比之下要更加开放，但始终控制着 3G 智能手机的开发主导权，并着眼于垂直控制终端操作系统（例如基于 Android 开发自己的操作系统，以及定制专门的终端，利用运营商地位拉拢更多用户），其一贯的风格也是凭借其平台地位打压排挤有利可图的应用服务商。[73] 未来两大终端设备的演进将决定互联网的演进方向。由于新经济的诸特征，架构的变化似乎不可避免，目前的技术状态也许不过是人类信息技术发展史上的短暂过渡阶段。[74] 未来虽然未知，但我们的自由和自主笃定要受到

---

〔68〕 有学者提出可以尝试两个不同的操作系统之间相互切换，一个用于试验创新，另一个则安放有用的数据。但他没有涉及云端储存的问题。见齐特林："创生性的互联网"，见前注〔5〕。

〔69〕 霍布斯在《利维坦》中的逻辑就是自然状态下的人们因恐惧、骄傲等激情而订立社会契约，由强有力的国家掌管其自由和生死。见霍布斯：《利维坦》，商务印书馆 1997 年版。

〔70〕 有关恐惧和风险的关系，参见加德纳：《黑天鹅效应》，中信出版社 2009 年版。

〔71〕 互联网的分布式架构本身就是为了应对核打击而设计的，大量复杂系统的研究也表明，当网络资源向少数中心节点集中时，整个网络将极为脆弱。我们已经看到互联网服务正在经历像水、电、天然气一样由分散到集中化服务的模式。参见 Nicholas Carr, *The Big Switch: Rewiring the World, From Edison to Google*, New York: W. W. Norton & Co., 2008。

〔72〕 一些初步讨论，见胡凌：重构隐私和隐私权？"载《互联网法律通讯》（2011 年即出）；"认知资本主义如何重新定义财产"，http://www.ideobook.com/1181/how-cognitive-capitalism-redefine-property/，最后访问日期：2012 年 3 月 29 日。

〔73〕 Henry Hu, "The Political Economy of Governing ISPs in China," *the China Quarterly*, September 2011.

〔74〕 互联网架构或生态系统是不断演化的，从科学角度看并不能说明偶然出现的后者一定优于或劣于前者。参见滨野智史：《架构的生态系》，大鸿艺术 2011 年版。

新商业模式的影响。

六、结 语

西方学界一直关注的问题是:互联网是什么?〔75〕既然有多种多样的信息网络设计方案,为什么要保持互联网的原初架构?〔76〕如何在其终端创新性和安全隐患之间保持平衡?〔77〕如何在个人自由和架构控制之间保持平衡?

通过本文的叙述可以看到,市场的无序竞争不会导致开放的互联网;相反,正是网络经济的商业模式决定了互联网架构的封闭性。政府有必要摆脱控制的思维,对这一趋势进行监管,不仅是为了经济效率,更是为了限制架构整合和人的异化。即使是在有序竞争放松管制的国家如美国,消费者也会通过市场选择和集体行动选择一个更加封闭的互联网,其引爆点正是安全问题。〔78〕从西方历史上看,总是会出现大资本集团试图控制信息流通的架构、技术和效果,尽管每次技术发明都可能给人类带来自由幸福,但最终的结果往往是由少数商业力量进行控制。〔79〕自由的技术如何能摆脱利益集团的操控已经远远超出了本文的范围,本文仅从微观的角度提供了一个中国语境下技术如何被商业力量主导演变的诠释。

信息网络技术无疑有助于我们进一步思考"自由与枷锁"的关系。〔80〕如果互联网架构能够通过商业力量决定性地影响我们的生活的时候,用户同互联网企业签订的服务契约是否能够使用户保持自主和独立?我们是否能够超越资本的力量掌握架构变化的轨迹?如何通过一种网络空间中的社会契约来设计机制?人们能否理性地实现这一设计?这将是未来需要进一步讨论的问题。

(责任编辑:薛 军 章永乐)

---

〔75〕 Lawrence Lessig, Code: Version 2.0,见前注〔11〕。

〔76〕 Barbara van Schewick, *Internet Architecture and Innovation*, Cambridge, Mass.: MIT Press, 2010; Yochai Benkler, The Wealth of Networks: *How Social Production Transforms Markets and Freedom*, New Heaven: Yale University Press, 2006.

〔77〕 齐特林:"创生性的互联网",见前注〔5〕;John Palfrey and Jonathan Zittrain, "Better Data for a Better Internet", *Science*, Vol. 334, No. 6060. (02 December 2011), pp. 1210 - 1211。

〔78〕 齐特林:《互联网的未来》,东方出版社 2011 年版。

〔79〕 Ithiel de Sola Pool, *Technologies of Freedom*, Cambridge, Mass.: Belknap Press, 1983; Tim Wu, *The Master Switch: The Rise and Fall of Information Empires*, New York: Alfred A. Knopf, 2010.

〔80〕 "人生而自由,却无往不在枷锁之中",卢梭:《社会契约论》,商务印书馆 1980 年版。