中国网络监控报告之二

政府如何监控我们的电子网络通讯？

作者：于声雷（维权网协助）

目录：

导言

一、现代电讯工具在中国的开发及其对传统信息垄断的挑战

二、中国官方对现代电讯工具的管制、审查、和监控

1.对手机短信的监控

1.1.手机短信监控流程

1.2.手机短信监控措施

2.对电子邮件的监控

2.1.服务商自律安装过滤

2.2.“国家防火墙”

2.3.监控涉外电邮机制剖析

3.对QQ的监控

3.1.腾讯公司自律，QQ设有后门检测程序

3.2. QQ如何监视用户的聊天记录

4.对SKYPE、MSN的监控

4.1.对skype的监控

4.2.对MSN的监控

三、关于安全使用电讯工具的建议

1.一般性安全措施

2.电邮安全措施

3. QQ安全措施

4. SKYPE安全措施

5. MSN安全措施

四、保障公民言论自由和通信自由

附件一：中国网监目前使用的关键字基本过滤词表[相关部分]

附件二：QQ是如何监视你的聊天记录？

导言

手机、电子邮件、QQ、MSN、SKYPE等现代电讯通讯工具对中国公民行使言论自由权发挥着特殊的作用。要理解这种作用，首先需要了解一些特定背景。

言论自由的基本内容是表达和传输信息的自由。一个政治体制是否有言论自由，关键就在于作为表达和传播的媒介是否广泛对普通公众开放，普通公众是否可以自由使用传播媒介。

现代大众传播媒介包括广播、电视、出版（这里的出版是指广义上的复制各种作品并发行）、互联网。在中国，广播、电
视、出版等事业全部由政府主办或由政府控股的单位主办，绝对禁止普通公民进入上述领域。甚至在互联网的信息传播作用日益增长的今天，上述格局也没有任何开
放性的改变，中国民众还是根本谈不上有大众媒体这个平台去行使言论自由。

互联网以及手机等现代电讯通讯工具的出现，从某种意义上改变了这个局面。新兴技术的兴起使得公民有了一定的空间去互
动性地接收传播信息。也就是说，中国公民可以利用互联网及现代电讯通讯工具开始行使一定言论自由权。在这个言论信息自由被完全剥夺长达几十年的国度，人们
一旦发现了这个新的天地，就将大量的热情倾注到这些方面，很快形成了不同于政府控制的大众媒体的新的舆论，在无边黑暗中点起了独立思考的火炬，并有望成长 为自由舆论的中坚力量。

从中国政府的一贯政策和立法意图来看，掌握公众舆论工具和控制言论自由是政府的一个主要目标。新兴技术的出现，打开
了一个缺口。而面对现代技术给控制带来的新难题，政府动用了巨大的国力去开发电子通讯技术，以便禁止现代媒体在中国作为独立的公众舆论平台发挥其独特作
用。政府的目标是将新兴的通讯平台掌控在政府手里，而不是通过立法、司法去调节管理。即使政府没法拒绝这些新兴技术以及由此开拓的通讯途径和平台，政府仍
然企图把这些空间和自由作为由它来掌控的“礼物”赐予给民众。

事实上，借助国际商业技术大公司的帮助，加上国家的巨大投资，中国政府已成功开发出全球最先进、最大规模和最严密的
现代电讯技术监管与监控系统，来遏制公民的言论表达和通讯自由。中国公民捍卫自己的言论通讯自由，面临重重障碍。但是，这场靠开发新技术来制约言论通讯自
由和反制约的争夺战，虽然双方在资源和力量各方面均无法抗衡，然而，“道高一尺，魔高一丈”，民间为自由的抗争在正义一边，又借助全球化的优势，寻找到各
种游击战术和有效途径来突破官方封锁和监控。

本报告披露中国对手机、电子邮件、QQ、MSN、Skype等现代电讯通讯工具进行监控的方式和途径、尤其是官方如何使用“关键词”过滤系统对使用互联网、电子邮件、手机短信、QQ的公民进行全面监控，探寻突破封锁和监控的使用经验。

本报告指出，依托新兴技术的中国言论空间还极为脆弱，主要原因是政府使用越来越严厉的、高尖技术监控。这种局面的改
变，一方面需要公民自身争取言论自由的努力，另一方面急需得到国际社会的普遍重视和积极干预。我们生活的这个星球上已经不再有“孤岛”——任何一个政府对
本国公民自由的压制，迟早会威胁其它地方、其他人享有的自由。

一、现代电讯工具在中国的开发及其对传统信息垄断的挑战

最新的统计数据显示，截至2007年6月底，中国手机用户超过4亿，根据政府和艾瑞市场咨询集团（IResearch Consulting
Group）的数据，每月中国4.55亿手机使用者使用短信共330亿次；电子邮箱注册用户总数已经超过4.3亿；在即时通讯工具方面，活跃用户数达
3.88亿，在中国最流行的即时通讯工具QQ的注册帐户总数7.153亿，其中活跃账户数达到2.92亿；MSN用户则有1892万；Skype在中国已
经拥有超过5100万的注册用户，中国市场也因此成为Skype全球用户最多、最活跃的区域市场。如此庞大的电讯通讯工具用户群，加上互联网和手机短信的
即时交流互动功能，不仅改变了中国信息的传播方式、速度和内容，更已经并且还在改变着中国的言论环境。

通过即时通讯、邮件、手机等工具，人们改变了在极权控制下的“孤岛”生存状态，人与人之间的交流变得十分方便、快捷，远比过去任何时候都自由。这些工具所共同具有的互动功能，突破了自然与人为的限制，正在迅速改变中国人的社会和政治生活。以下几个方面的突破尤其值得注意：

媒体自由：无数个小型的通讯交流社区正在并将继续形成，每个用户不仅可以接受信息，还可以发表意见，甚至自己充当信
息的发布者，形成了一个由官方掌控的传统媒体迥然不同的民间“新媒体”，无须在这个缺乏媒体自由的国家像传统媒体一样接受新闻审查官检查，也无须与官方保
持口径上的一致。人们重新拥有了缺席了差不多六十年的媒体自由。

信息自由：通过这些工具，信息以惊人的速度在民众中蔓延，人们能够迅速获得各种热点消息，公众普遍关注的问题得以迅
速成为大众传媒的议题；不同于官方的民间政治主张和诉求获得新的表达渠道。更重要的是，新技术打破了官方的信息封锁，使当局的言论信息管制越来越力不从
心，加剧了信息传播的泛中心化趋势，消解了官方传媒在信息制造和传播中的垄断地位，促进了信息的多样化，舆论压力：民间新媒体和信息多元化的出现，对当局 形成了某种前所未有的舆论压力。

官权削弱：这个依托于新技术的民间新媒体，正在改变中国社会自共产党执政以来官权与民权的极度不平等的态势，使民间社会的力量及公共空间在强大的技术支持下得到扩展。

[典型事例]：
在2007年的厦门PX事件中，新媒体所起的作用引人注目。厦门市民互相转发一条题为《反污染！厦门百万市民疯传同一短信》的手机短信。这些短信指出，因为政府推动要在市郊棕榈树间建立一家大型化工厂，“在厦门所有人头上投下一颗原子弹”，预言工厂将给这座中国南面边缘（紧邻台湾）城市的200多万居民，带来“白血病和畸形婴儿”（ 6月28日

《华盛顿邮报》
）。鉴于当地官方媒体实行新闻封锁集体沉默，而讨论此事件比较集中的一个论坛“厦门小鱼论坛”也因此被关闭，当传统媒体和网络被警告不敢登出关于抗议活动
的报道后，手机短信便成了新的传播渠道，厦门市民用手机短信相约走上街头游行，数万人以挂黄丝带散步的形式进行公民抗争，网友北风及令狐补充利用手机短信
及网络接力，成功地在博客上进行了全程的现场报道。在国内传统媒体普遍失声的情况下，这几乎成为唯一的连续的现场消息来源的手机短信直播吸引了超过20多万的点击，并迅速被网民所转载。美国华盛顿邮报对此事件的报道标题就是《短信在让中国人发出声音》，确实是一语中的。

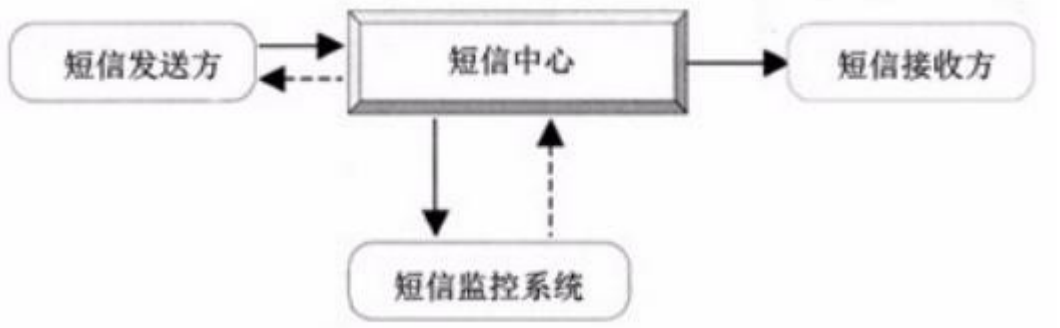
二、中国官方对现代电讯工具的管制、审查、和监控

现代电讯工具对言论自由的促进、对中国民间社会的发育成长所起到的重要作用，使得它日益成为政府实施威权统治的心腹
大患。政府通过一系列的政策、技术手段来对现代电讯工具实行管制、审查和监控，以便禁止和杜绝新兴技术在中国为形成独立的公众舆论基地提供有力的工具。下
面我们分别揭示中国官方是如何对几种主要电讯通讯工具进行监控的：手机短信、电子邮件、QQ即使通讯、Skype加密即时通讯通话。

1.对手机短信的监控

1.1.手机短信监控流程

手机短信是一种点对点的移动电话短消息传输交互功能，它必须经过移动电话运营商的短信中心中转，所以对短信的监控设置一般都在短信中心里进行。



短信监控流程图

短信中心接收到用户发送的短信后，会发送一个鉴权请求消息到短信中心关联的短信监控系统，监控系统根据配置信息对短
信内容或者地址（被当局列入监控范围的手机地址号码所发送的短信在这里会被系统核对后记录下短信内容）进行判断，返回给短信中心鉴权响应消息，如果短消息
内容合法。则返回鉴权成功消息，短信中心将该短信下发给短信接收方；如果内容不合法，则返回鉴权失败消息，短信中心将该消息直接丢弃，不下发给接收方，并 记录短消息。

1.2.手机短信监控措施

短信内容和发送频率监控：2005年10月，中国信息产业部下发通知，要求运营商对各类手机信息要进行实时监测[1]。目前“电信”、“联通”和“网通”三大运营商业公司已经对用户的短信发送频率和内容进行24

小时专人监控。监控的主要手段是对文字短信采取关键词过滤的方式筛选短信；同时安排专人对包含图片或视频的多媒体信息进行全天候内容监控。

“手机实名制”：信息产业部制定的《手机短信服务管理办法》目前正交由中国政府
各相关主管部门会签，近期将对外界公布。该管理办法最主要的内容就是强制推行“手机实名制”，也就是强迫要求手机用户都必须用真名登记，同时配合屏蔽关键
字、限制点对点发送的数量、限制非实名手机号码的短信功能等来控制短信发送。

“手机实名制”的出台是公安部门不断敦促通信管理部门和移动运营商的结果。公安部门声称这套办法可以为侦破“不法”短信提供方便，因为手机实名制要打击的主要对象就是“违法短信”。

与其它中国政府控制公众舆论工具的做法一致，手机实名制将增加政府控制社会的权力，加强政府对公民的言论监控和信息收集，侵犯公民的通信自由和隐私权。

地方政府多元监控措施：中国各地方政府部门、机构也出台了多项措施来审查、监控手机短信。例如
：

北京的300多家SP（电信增值服务提供商）单位组成“北京网络行业协会电信增值服务工作委员会”，下设“执行机
构”，对“制作、发布淫秽、赌博、反动”等短信进行检举、调查，同时北京警方在运营商前台设置过滤监测系统，一旦发现“有害短信”立即阻断，追查发布源头
并追究责任。北京市政府2007年12月17日发布《关于进一步规范本市手机短信息发布公共信息管理工作的通知》（以下简称“通知”），对以手机短信传播
的涉及公共信息的部分作了规定。如有通过手机短信“传播和散布谣言”并“涉及危害公共安全”行为，将由北京市公安局牵头，协同有关部门和通信局及相关通信
运营公司，根据有关法律法规对相关责任人进行查处。（参见《新京报》07年12月18日消息）北京市政府的“通知”是那些使用手机传递信息的公民头上悬置
的一个达摩克利斯之剑，给当局任意惩治羁押那些行使言论和表达自由去传播官方掩盖的信息、监督政府行为的公民提供口实。

山西省发布《关于进一步加强短信息宣传管理的意见》，督促电信运营商采取技术手段，对关键词语或未经证实的信息进行
拦截，严禁带有危害性的言论通过短信或互联网传播。这个《意见》规定短信群发重要内容须经有关部门批准才能发送：对于事关国家安全、社会稳定、国计民生、
人身安全、重大自然灾害、公共突发事件等信息内容的短信群发，发送范围为全省时，要求内容提供方提供省政府或省级领导批示的书面意见；发送范围为市级时，
要求内容提供方提供当地政府或当地政府领导批示的书面意见。对于谣言短信的制造者和恶意传播者应该依法作出惩戒，散布谣言，谎报险情、疫情故意扰乱公共秩
序的，可以处拘留，严重者可处五年以上有期徒刑。编造疫情等恐怖短信进行传播，或者明知道是谣言短信还故意传播，是一种扰乱公共秩序、破坏社会稳定的行 为，应该依照法律追究行政和法律责任。

值得关注的是，中国官方对所谓的“谣言”和“危害公共安全”一直缺乏严格的法律定义。官方这些行政规定所指的谣言通
常是指民众通过手机传播一些不利于政府的信息，比如说某个地方发生了警察和民众的冲突，或者是某个部门出现了严重的突发事件，引起了公众的强烈愤慨，或者
是某个地方发生了大规模的公众游行、示威。所有这些对政府不利的、公众有权了解的信息，都有可能

被随意界定为“谣言”或“危害公共安全”，视政治需要随意
进行打击，把许多表达正常的意见和传递信息的公民，用散布所谓的“谣言”和“危害公共安全”的罪名加以治罪。

下面我们举例来说明官方如何采取围追堵截的办法，千方百计地阻止公民通过手机短信表达政治意见，如何动用国家机器、采取强制措施禁止公民利用手机发送表达政治观点的信息，如何追究信息发布者的刑事责任：

个案之一：太湖蓝藻案

2007年6月，江苏无锡一名丁姓市民因蓝藻爆发太湖污染发送百余条短信，被警方以违反《治安管理处罚法》行政拘留
10天。警方称，“近日在工作中发现有人利用手机短信散布谣言，称‘太湖水致癌物超标200倍’，引起一些市民恐慌”。尽管后来官方发布的信息间接表明，
太湖水污染不但确凿无疑，而且首先是人为灾难，但是这位市民违反《治安管理处罚法》、“散布谣言，扰乱公共秩序”的定性并没有被改变。

个案之二：彭水诗案

2006年8月15日，重庆市彭水县教委人事科科员秦中飞，填了一首《沁园春·彭水》的词：

马儿跑远，伟哥滋阴，华仔脓胞。

看今日彭水，满眼瘴气，官民冲突，不可开交。

城建打人，公安辱尸，竟向百姓放空炮。

更哪堪，痛移民难移，徒增苦恼。

官场月黑风高，抓人权财权有绝招。

叹白云中学，空中楼阁，生源痛失，老师外跑。

虎口宾馆，竟落虎口，留得沙沱彩虹桥。

俱往矣，当痛定思痛，不要骚搞。

写好后，秦中飞把诗词输入手机，在接下来的十几天里，他发了10-15条短信，并在QQ上发给了4-6个网友。时隔
半月，警察突然找到了他。10多分钟后，他向他们承认，短信是自己写的，“我想，这事儿也没什么大不了”。警察搜查了他办公室的书籍、电脑等，并没收了秦
的手机及QQ号，随后又将他带到了公安局国安大队。第二天晚上，秦中飞被彭水县公安局以涉嫌“诽谤罪”刑事拘留，关押在看守所。他们反复追问秦写《沁园
春。彭水》的动机，说这首词隐喻了该县几个轰动的社会事件，隐喻了彭水县委县政府三个领导。审讯者试图揪出躲藏在诗词背后的“黑手”，以及核对转发的名
单。10天后，经过数次提审，公安局于9月11日对其正式下发逮捕令。在押期间，一直没有人告诉他，他诽谤了谁。检察院的起诉意见书称，秦中飞捏造了一首

引起群众公愤的词，利用QQ和短信方式进行发送，严重危害该县社会秩序和破坏了县领导人的名誉，触犯刑法246条之规定，涉嫌诽谤罪。网民们通过各种途
径，向重庆市有关部门反映情况，质疑彭水县公安局的行为。在舆论的关注下，这一事件在9月27日发生了戏剧性的变化，公安局动员其远房堂兄“取保候审”，
秦中飞被“强行保释”。他被关押了近30天后。其间，公安机关还传讯了接收短信的10多个人，以及这些短信的二次甚至三次传播和接收者，县公安局调查了
100多名接收并转发这条短信的人。秦中飞说他本意是纯粹消遣和“文人情绪的发泄”，“但没想到，自己在20分钟内的涂鸦之作，竟会给朋友带来这么大麻
烦。”结束了牢狱生活后，他说，“我感觉到自己像得了非典。”从看守所出来后的秦中飞说。这个武陵山脉深处的小城，四周群山禁锢，不费一炷香时间，消息从
城东传遍城西。秦霎时成为一个“不自量力与政府作对”的新闻人物。有人怕事开始躲他。“人人自危，不敢谈论政治。”一位退休干部说，“现在，没人敢对政府 官员说三道四。”

个案之三：陕西志丹短信案

2007年10月中旬，陕西志丹县数人因一条短信被处分，其中4名科级干部被免职。10月中旬，在志丹县城流传一条
手机短信，当地公安机关称“以极其低级下流的语言，对14名领导干部侮辱诽谤”。公安机关调查后认为李某、孙某编发并传播此条手机短信，“捏造事实诽谤他
人，该短信流传后，严重地损害了他人的人格和名誉，已触犯《刑法》，涉嫌诽谤罪，被依法逮捕”；另有刘某被刑事拘留。

志丹官方对转发传播该短信的左某、曹某、高某、刘某等4名科级干部予以免职，并进行相应的纪律处分；对传播该短信的
农行某营业所所长宋某，要求农行拿出处理意见，报经县纪检、组织部门同意后处理；一般干部和职工转发该短信，由所在党委拿出处理意见，报经县监察、人事部
门同意后处理，并由监察、人事部门备案，所在单位负责人作出书面检查。

据了解，被免职的4名科级干部分别为志丹县为卫生监督所所长左某、志丹县信用联社副主任刘某、旦巴镇中学原校长曹某、金丁镇农技站站长高某，据悉，事发前，除了曹某因学校实行校长竞聘而不在位外，其余三人均为在职科级干部。目前均已经离开原岗位。

对此，当地有人认为，政府和执法部门对这件事处罚过于严重。“作为领导，你无疑是公众人物，有些群众或者干部产生一些想法是正常的，何况发一条短信，在现在这个荤段子横行的时代，应该算是正常的。政府应该以此为戒，而不是来重罚这些人。”

随着调查的深入，该案被发现另有隐情。志丹官方真正要控制的是另一条质问“一位新任县委主要领导是清官还是贪官”的
短信。官方也从扩大宣传到集体沉默，几乎所有涉事部门、机关，在面对“短信这个事”时，都一致选择了避而不谈。这与该案开始时志丹官方对“短信案”持公开 甚至是扩大宣传的态度前后矛盾。

短信改编自民间广为流传的一个荤段子，内容讲的是一名遭到强奸的女子在向公安机关描述作案者特征时，编发短信者将县
上14名领导干部按照个人特点编入短信，并将该短信进行补充修改后，发给朋友，很快便流行开来。当地民众质疑说“这样的黄段子把联合国秘书长编进去的都
有，县上的领导怎么可能针对这样一条短信大动干戈。”

相关人员透露，早从年初开始，在志丹县就开始传播着另一则短信，这则短信矛头直指一位新任县委主要领导。内容大致为：志丹有个×××，光抓卫生不抓粮；六山绿化……；改河工程铲车摆了一河滩，志丹财政全弄完；十个工程九个自己干，他是清官还是贪官。

调查发现，短信所指的“抓卫生、六山绿化、改河工程”等，均列入志丹本届政府施政规划，政府在这些工作上确实巨资投入，由此给志丹财政带来沉重负担。“十个工程九个自己干”，是批评县上工程建设不透明。至于末尾“清官”、“贪官”一句反问，无疑是整则短信的问题落点。

“领导不是怕编他们的黄段子传开了，而是怕这则批评短信传开，此次大张旗鼓地实施打击，实际是选择黄段子开刀，进行
震慑。”一位短信案涉案人士分析说，政府拿黄段子短信开刀最为合适，如果从评议政府工作的短信下手，政府就会陷入被动。在这些官员眼中，法律只是一件玩
具，因为司法不独立，符合他们利益时，就用法律，不符合他们利益时就把法律一脚踢开。

像这类借短信压制不同声音、公然侵害言论自由的案件，有几点相通之处：

没有真正的监督，那么民众只好把短信当作一个发泄渠道，应该批评的是专制政府；通信自由与言论自由受到严重的伤害；
是不尊重法律，不遵守法律程序，以官压人；是借机打击自己的批评者，贪官污吏害怕短信把他们的劣行给传播出来。这种把戏是最高当局通过扫黄打非来压制异见 言论一个翻版，上行下效。

2.对电子邮件的监控

2.1.服务商自律安装过滤

除了官方的国家防火墙对电子邮件实行严厉监控外，中国大陆境内的的电子邮箱服务商也根据官方的部署安装电子邮件关键
字过滤系统，对含有敏感关键字的电邮拒发或接拒绝接收。如在搜狐邮箱发送含有关键字的邮件，画面会跳出“因邮件中存在敏感信息而被拒绝发送的提示”，这些
问题在其它中国电子邮箱服务商亦同样出现，因为按照中国官方从来不公开、秘密下达给服务商的规定，它们安装的电邮关键字过滤系统都是统一由官方制定的。

由于关键字过滤系统被广泛采用来监控网络、手机、电子邮件、QQ等，所以这个系统究竟包括哪些关键字，外界一直有很
多揣测，也总结归纳了不少，但是一直没有一份公开的官方关键字全文。本报告作者、网络专家于声雷（化名）经过特殊途径拿到了官方基本关键字过滤词表，并在
本报告里首次公之于世（请见附件一）。这份过滤词表含有基本关键字共1083个。它有助于世人了解中国当局的信息控制。

除了实行关键字过滤系统对电子邮件监控外，中国的网络警察还经常冒充机构、媒体记者、异议人士的邮箱对列入当局黑名
单对象散发带有木马病毒的电邮，以监控电脑、窃取邮箱密码和资料，甚至直接破坏电脑。这个散发病毒的方式一般是注册一个与媒体记者、异议人士邮箱相似的电
邮，发件人称呼里直接盗用这些人士的名字，这个鱼目混珠的做法经常使一些人上当。

2.2.“国家防火墙”

中国互联网络信息中心（CNNIC）[2]的历
次《中国互联网发展状况统计报告》都显示，电邮是互联网最重大的基本应用，超过90％的网民都有使用电子邮箱的习惯。中国电子邮箱注册用户总数已经超过
4.3亿，电子邮件服务覆盖范围仍在扩大，与人们日常工作生活的关联也日趋紧密。中国电子邮箱占前三位的是网易、新浪、搜狐三大服务商提供的电邮服务。

由于中国官方实施的网络封锁，也因为大部分网民不会使用代理软件突破封锁，因此对他们来说，想了解信息，电子邮件就成了一个重要的途径。目前除了网民互相发送信息共享的邮件外，还有大量海外传媒建立电子版平台，通过电子邮件发送给网民。

电子邮件因此成了官方严格管制、监控的对象。监控管制的主要工具是中国耗费巨资做成的臭名昭著的“国家防火墙”。防火墙，也成防火长城，是对中国政府在其管辖互联网内部建立的多套网络审查系统（包括相关行政审查系统）的俗称。[3]一般情况下防火长城主要指中国对互联网内容进行自动审查和过滤监控、由计算机路由器等网络设备所构成的软硬件系统，主要作用在于对中国境内外的网络资讯互相访问进行分析、过滤、阻断。

电子邮件在发送接收过程中，要经过不同的网络设备，如网关，路由器或其他电脑，这些设备都可以对传输内容进行自动扫
描。如果在邮件中直接使用被封锁的关键字，电子邮件就发送不到受件人的邮箱，并且会断开相关的连接若干分钟，而且双方的邮箱地址和IP地址都可能被记录或 监视。这就是国家防火墙IDS（Intrusion Detection
System，入侵检测系统）的功劳，它使用美国思科（CISCO）等公司帮助建立的关键字过滤功能，能够从计算机网络系统中的关键点（如国家级网关）收
集分析信息，过滤、嗅探指定的关键字，并进行智能识别，检查网络中是否有违反“安全策略”的行为。这个系统利用这些设备进行数据包内容的过滤，使数据流中
断。所以在访问gmail、hotmail等国外邮箱时，如果数据流里有敏感字词，即会立即被提示“该页无法显示”、“系统无法执行指定操作”或网页开启
后会突然停止，屏蔽时间与猜测敏感词等级以及所属网站有关。

2.3.监控涉外电邮机制剖析

中国国家防火墙建立以来，由于它实行的关键字过滤系统原因，导致国内几乎所有发送海外邮件的用户都不同程度地受到影
响。特别是国际贸易公司、进出口公司等视企业邮件为公司生命线的公司，日常和国外客户、总部及代理商的几乎所有沟通均须通过企业电子邮件传递，国家防火墙 对其海外业务造成了严重的影响。

2007年7月16日开始，几乎所有中国电子邮件服务商均告急，大量外贸邮件收发不正常，发往海外的邮件出不了国的
现象开始越来越严重，包括新网，新浪，TOM，网易，万网，尚易，263，21cn，中国频道，中资源等各大邮件厂商均发布了邮件不正常通信的公告。例
如，见下图：新浪VIP邮箱邮件不正常通信公告截图、万网企业邮局海外邮件通信公告截图、TOM国际电邮通信问题公告截图。

与海外邮件通信问题的重要通知

2007年7月17日

尊敬的用户朋友：

您好！

近期互联网国际线路出口不稳定，国内多数大型邮件服务提供商均受到影响，在此期间您与国外域名通信可能会出现退信、丢信等现象。为此，新浪VIP邮箱正在采取措施，力争尽快妥善解决该问题。

具体问题如下：

1、新浪VIP邮箱给国外域发信收到退信，退信提示“Remote host said: 551 User not local; please try <forward-path>”

2、新浪VIP邮箱用户给国外域发信，对方收到邮件时内容均为“aaazzzaaazzz”。

3、新浪VIP邮箱给国外域发信收到退信，退信提示“Connected to ***.***.***.*** but connection died. (#4.4.2)”

4、国外域给新浪VIP邮箱发信时收到退信，退信提示“Remote host said: 551 User not local; please try <forward-path>”

5、国外域给新浪VIP邮箱发信后，新浪VIP邮箱用户收到的邮件内容均为“aaazzzaaazzz”。

请您遇到上述问题后，将退信以附件的形式发送至：webmaster@vip.sina.com，（对于aaazzzaaazzz的问题，请写明是对方邮件地址），以便我们查看具体情况并解决邮件送达问题。或者拨打全国统一直拨客服热线：95105670（免长途费），我们的客服人员将会在第一时间尽全力帮您解决问题。如果您有任何意见和建议，也欢迎您反馈给我们，新浪邮箱全体人员在此向您致谢！

新浪VIP邮箱

2007年7月17日

（新浪VIP邮箱邮件不正常通信公告截图）

主题：万网关于海外邮件通信问题的说明

尊敬的中国万网企业邮局用户：

从7月16日开始，陆续有企业邮局用户反映给国外信箱投递后出现大量退信。退信中的报错信息如下：

1) I'm not going to try again; this message has been in the queue too long.

2) <xxx@xxx.com>: 551 User not local; please try <forward-path>

经过我们仔细检查，投递日志中的信息如下：

Connected to remote host, but connection died. (#4.4.2)

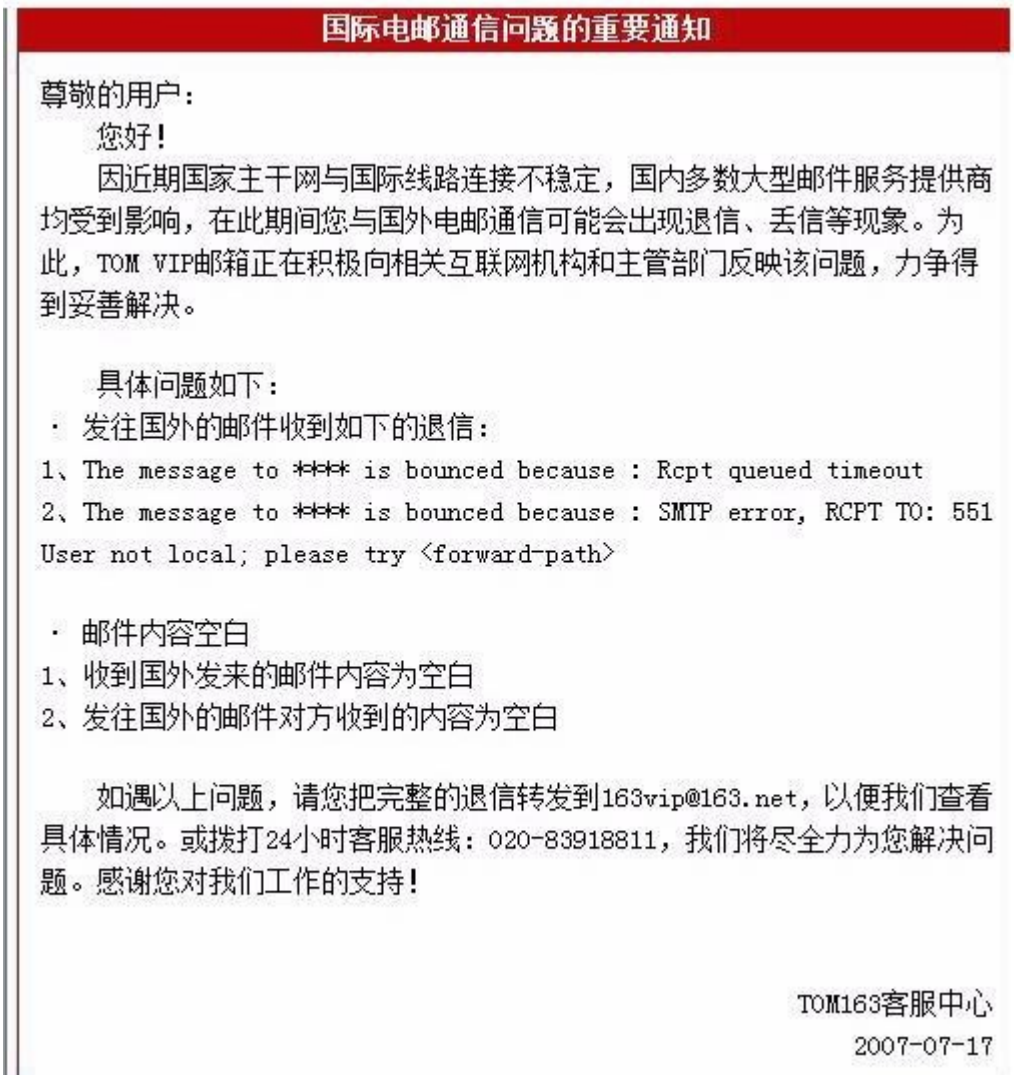
具体含义是远程主机断开了连接，但是对方没有提供任何断开的理由。

海外退信问题的原因，我们目前还无法准确判断，我们初步怀疑是互联网国际出口的技术问题导致，因为已经有多家邮局服务商出现完全相同的问题。我们已经联合其他邮件服务商共同将此问题积极向相关部门反映，并将在此问题得到妥善解决后第一时间通知您，请您再耐心等待一下，谢谢合作！

中国万网客服中心

2007年7月17日

（万网企业邮局海外邮件通信公告截图）



国际电邮通信问题的重要通知

尊敬的用户：

您好！

因近期国家主干网与国际线路连接不稳定，国内多数大型邮件服务提供商均受到影响，在此期间您与国外电邮通信可能会出现退信、丢信等现象。为此，TOM VIP邮箱正在积极向相关互联网机构和主管部门反映该问题，力争得到妥善解决。

具体问题如下：

· 发往国外的邮件收到如下的退信：

1、The message to **** is bounced because : Rcpt queued timeout

2、The message to **** is bounced because : SMTP error, RCPT TO: 551 User not local; please try <forward-path>

· 邮件内容空白

1、收到国外发来的邮件内容为空白

2、发往国外的邮件对方收到的内容为空白

如遇以上问题，请您把完整的退信转发到163vip@163.net，以便我们查看具体情况。或拨打24小时客服热线：020-83918811，我们将尽全力为您解决问题。感谢您对我们工作的支持！

TOM163客服中心

2007-07-17

（TOM国际电邮通信问题公告截图）

所有邮件服务商碰到的问题都是同样的：

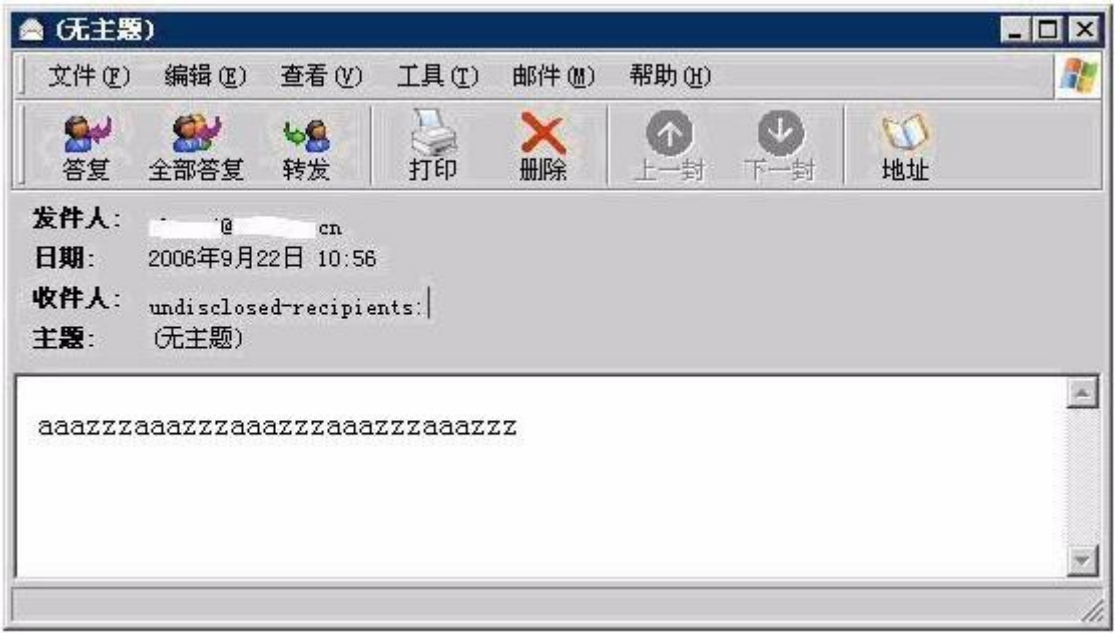
①、国内邮箱给国外域发信收到退信，退信提示“Remote host said: 551 User not local; please try <forward-path>”

②、国内邮箱用户给国外域发信，对方收到邮件时内容均为“aaazzzaaazzz”。

③、国内邮箱给国外域发信收到退信，退信提示“Connected to ***.***.***.*** but connection died. (#4.4.2)”

④、国外域给国内邮箱发信时收到退信，退信提示“Remote host said: 551 User not local; please try <forward-path>”

⑤、国外域给国内邮箱发信后，新浪VIP邮箱用户收到的邮件内容均为“aaazzzaaazzz”。



邮件内容截图

出现这些问题是因为国家防火墙对电子邮件的拦截监控，中国网民称此为“”有中国特色的SMTP现象“。

为了证实国家防火墙的监控阻止电子邮件发送的说法是否属实，我们进行了以下的测试：（注：域名和IP信息有修改）

从sales2@test.com（在大陆）发给construction@recipient.com（香港分公司）,在发件人的服务器查到如下日志：

Oct 12 10:43:37 localhost postfix/smtpd[30005]: E50DD4187A5: client=unknown[125.0.0.1], sasl_method=LOGIN, sasl_username=sales2@test.com

Oct 12 10:43:43 localhost postfix/cleanup[28691]: E50DD4187A5: message-id=<20061012024337.E50DD4187A5@slave.mail51.cn4e.com>

Oct 12 10:43:44 localhost postfix/qmgr[17170]: E50DD4187A5: from=<sales2@test.com>, size=36652, nrcpt=2 (queue active)

Oct 12 10:48:53 localhost postfix/smtp[1140]: E50DD4187A5: to=<construction@recipient.com>, relay=202.67.0.1[202.67.0.1], delay=316, status=deferred (conversation with 202.67.0.1[202.67.0.1] timed out while sending MAIL FROM)

Oct 12 11:43:20 localhost postfix/qmgr[17170]: E50DD4187A5: from=<sales2@test.com>, size=36652, nrcpt=2 (queue active)

Oct 12 11:43:30 localhost postfix/smtp[28474]: E50DD4187A5: to=<construction@recipient.com>, relay=202.67.0.1[202.67.0.1], delay=3593, status=deferred (lost connection with 202.67.0.1[202.67.0.1] while sending message body)

Oct 12 13:43:20 localhost postfix/qmgr[17170]: E50DD4187A5: from=<sales2@test.com>, size=36652, nrcpt=2 (queue active)

Oct 12 13:43:22 localhost postfix/smtp[5424]: E50DD4187A5: to=<construction@recipient.com>, relay=202.67.0.1[202.67.0.1], delay=10785, status=bounced (host 202.67.0.1[202.67.0.1] said: 500 error (in reply to MAIL FROM command))

Oct 12 13:45:22 localhost postfix/qmgr[17170]: E50DD4187A5: removed

发件人sales2@test.com收到退信：

<construction@recipient.com>: host 202.67.0.1[202.67.0.1]

said: 500 error (in reply to MAIL FROM command)

在香港分公司查到如下日志：

Oct 12 10:44:45 hk postfix/smtpd[21468]: 3BCDC2B000F: client=unknown[218.85.0.1]

Oct 12 10:44:45 hk postfix/cleanup[22131]: 3BCDC2B000F: message-id=<20061012020145.3BCDC2B000F@hk.com>

Oct 12 10:44:45 hk postfix/qmgr[25450]: 3BCDC2B000F: from=<sales2@test.com>, size=475, nrcpt=2 (queue active)

Oct 12 10:44:53 hk postfix/smtp[22352]: 3BCDC2B000F: to=<construction@recipient.com>, relay=maildrop, delay=8, status=sent (recipient.com)

Oct 12 10:44:53 hk postfix/qmgr[25450]: 3BCDC2B000F: removed

说明这封信已经成功发过去了，但是为什么发件人会收到退信呢？退信是从那来的呢？对比一下这两条日志：

Oct 12 10:43:44 localhost postfix/qmgr[17170]: E50DD4187A5: from=<sales2@test.com>, size=36652, nrcpt=2 (queue active) （在发件人服务器上的日志）

Oct 12 10:44:45 hk postfix/qmgr[25450]: 3BCDC2B000F: from=<sales2@test.com>, size=475, nrcpt=2 (queue active) （香港收件服务器上的日志）

发件人发送的时候size=36652,而到了香港却被变成了size=475！再看一下construction@recipient.com收到的这封信的内容竟然是aaazzzaaazzzaaazzzaaazzzaaazzz：

Return-Path: <sales2@test.com>

Delivered-To: construction@recipient.com

Received: by mail.hk.com (202.67.0.1) (Postfix, from userid 12346)

id 3BCDC2B000F; Thu, 12 Oct 2006 10:44:53 +0800 (CST)

X-filter: Passed

Received: from unkoown (218.85.0.1)

by mail.test.com (Postfix) with ESMTP id E50DD4187A5

for <construction@recipient.com>; Thu, 12 Oct 2006 10:43:56 +0800 (CST)

Message-Id: <20061012020145.3BCDC2B000F@hk.com>

Date: Thu, 12 Oct 2006 10:44:45 +0800 (HKT)

From: sales2@test.com

To: undisclosed-recipients:;

aaazzzaaazzzaaazzzaaazzzaaazzz

事实很清楚，在发件人发给香港的时候，被中国国家防火墙截住，返回给发件人500 error，同时其把内容更改后发给了收件人，于是就出现发件人收到500 error，而收件人收到aaazzzaaazzzaaazzzaaazzzaaazzz的奇怪事情。

所有服务商的通知都把问题归究为互联网国际线路出口不稳定，事实上他们都相当清楚这是因为中国国家防火墙的拦截影响，但他们不敢也不能公开事实的真相。

由此可见，中国对电子邮件的监控措施，不但侵犯了中国公民的言论自由权利和通信自由权利，也对中国的经济活动、商务往来造成极大的阻碍。

3.对QQ的监控

作为使用频率最高的网络软件，即时通讯软件（instant message，简称im），被认为是电子通讯工具之骄、现代交流方式的象征，它改变人们的社会交往关系。有人甚至认为它是迄今为止对人类社会生活改变最为深刻的一种网络新形态。

QQ是中国目前最流行的即时通讯工具，活跃账户数达到2.92亿。那个可爱的小企鹅形象以及“滴滴滴”的提醒声，几乎成了中国网民上网的象征，在大陆地区几乎一统天下，被认为是平民化的im.由于QQ可通过限制条件添加好友，网民们可以根据自己的喜好和乐趣认识新的聊天对象，在QQ上形成自己的小圈子（QQ称之为群[4]），使志同道合的人们很快聚集在一起。正因为如此，它具备了其他任何软件都不具备的影响力。这些“圈子”同时在社会生活中也可以发挥很大的作用，如拓展公共舆论空间、争取民众话语权等。

QQ在中国即时通讯软件的霸主地位使它成了当局监控的重点对象。而QQ的开发商腾讯公司也积极配合当局进行监控。

腾讯在QQ中加入了后门程序，采用了关键字检测技术，当用户的聊天谈话带有敏感内容时，这些内容会被自动记录下来，并在用户不知情的情况下，秘密发回腾讯服务器。因为用户的真实IP地址已被记录下来，警察可以随时决定是否采取进一步的行动[5]。

“QQ确实有后门程序，”腾讯公司的内部技术人员向本报告作者证实说，“不过一般点对点的聊天不会激发后门程序，多用在QQ群聊天上，如果谈话内容带有关键字会被立即记录下来发给我们服务器，再交给警察处理。

北京《华夏时报》05年8月刊发记者谷龙关于腾讯QQ监视用户的报道，“QQ是如何监视你的聊天记录”，指出腾讯
QQ记录用户聊天信息并传回服务器。但腾讯的公关公司回答说，是腾讯方面接到了上级有关部门的指令，才监视用户的使用情况。该报道当时引起广泛关注，但不
久就遭封杀令，媒体不许继续报道，各网站也接到指示，要求删除该报道及相关讨论。这篇调查报告把问题说得相当清楚，因而值得在这里与读者分享全文。（请见
附件二：“QQ是如何监视你的聊天记录”）

4.对Skype、MSN的监控

4.1对Skype的监控

Skype是一种可以用来网上发短信、打电话、传文件的工具，在中国相当流行，已经拥有超过5100万的注册用户，中国市场也因此成为Skype全球用户最多、最活跃的区域市场。

在2005年9月，SKYPE与TOM公司合作，在中国推出TOM-
Skype版本。TOM的大股东李嘉诚和周凯旋都和中国政府有千丝万缕的关系，所以TOM根据当局的要求，对面向中国用户推出的TOM-Skype版本加入了木马功能，对关键字实行过滤，并收集用户信息。

当用户安装TOM-Skype时，用户的电脑就会自动安装审查过滤程序contentfilter.exe而不会通
知用户。经检查，我们发现，安装TOM-
Skype时，安装程序就下载了所谓的"keyfile"阻断关键字加密文件到用户的电脑里。即使卸载TOM-
Skype后，该过滤程序仍然保存在用户电脑上。据了解，TOM-
Skype版本的关键字过滤主要应用在文字聊天上。该关键字过滤器不会显示在Skype
聊天上。当发现有敏感字后，它会记录下来并加密发送到出去。

在2006年4月接受英国《金融时报》的采访时，Skype的负责人Niklas
Zennstr？m在回答关于Skype的中文版本实行言论审查时解释说，Skype只是遵从不和当地法律相抵触的原则。“TOM-Skype实施了关键 字过滤，但是在中国这个市场大家都这样做"，《金融时报》引述Niklas
Zennstr？m说。"这些都是规定".

带有木马功能的TOM-Skype主页

目前中国大陆所有用户访问Skype网站http://www.skype.com时都被中国国家防火墙强行劫持域名转到TOM-Skype的网站http://skype.tom.com，也就是说大陆用户下载使用的多半是带木马病毒的TOM-Skype版本，而不能下载真格的Skype国际版。

为了使网民知道如何鉴别自己使用的Skype是何种版本，现介绍鉴别办法如下：

打开自己的Skype，点击help（帮助），在跳出的菜单的最下面，有about Skype（关于），就会跳出来先下面的截图。从这里便可清楚地看到自己使用的Skype是哪一个版本了。（见图一、图二）

图-1 TOM-Skype版本

图-2 Skype国际版本

4.2.对MSN的监控

MSN的跨国界使用范围是QQ目前还无法比拟的，在中国国内msn被标上了“白领专用”的标志，有1892万中国用户使用。

由于MSN使用的是ASCLL码，采用明文传输的方式来传送即时消息的，而这种传输方式不会经过任何加密过程，非常
轻易被专门的监听软件截取谈话内容。目前中国大陆境内的异议人士的MSN都受到不同程度的监视，由于MSN的安全缺陷，警察不需要在被监控对象的机器上装
任何的东西，MSN对话全部尽收眼底。如江苏扬州警察在找一名异议人士谈话时，就拿出一大叠通过监控得到的MSN谈话打印记录作为指证。

三、关于安全使用电讯通讯工具的建议

1.一般性安全措施

（1）避免使用关键词

目前中国的手机短信、电子邮件、QQ、SKYPE等都是用关键字来进行言论审查监控，所以可以对列入官方的本关键字表的文字进行修改来避开审查。

（2）不要使用国产杀毒或防火墙软件

诸如瑞星、金山、天网等等，这些国内的公司与国安局都有合作，已经多次被发现有后门或者是其它不可告人的代码存在，是不安全的，建议使用国外软件如卡巴斯基、Antispyware、McAfee等。

不要使用拼音加加2004v3.02，新华五笔，这两个软件已经发现有后门和敏感词汇汇报功能存在，会在不知不觉中泄漏您的隐私。

不要安装3721和上网助手等流氓插件。

2.电邮安全措施

电子邮件在传输过程中要经过网关、路由器或其他电脑等不同的网络设备。这些设备都可以对传输内容进行自动扫描。一旦
发现邮件中有敏感字，就可以终止该内容的传输，并且断开相关的连接若干分钟。对于这类封锁可以采用内容加密或传输图片的方法加以防范。通常我们使用的加密 网址（https://xxx.xxx.xxx.xxx，https://中的s代表传输加密的意思）即可解决这个问题。采用这样加密的网站在实际应用中被破解的可能性几乎为零，所以有足够适用的安全度。因为它是加密代理，在访
问它时，往往会弹出一个窗口，问是否接受这个安全证书（Certificate），请选择接受，才能够继续浏览。

中国境内的电邮服务商自我审查相当严格，比如新浪、网易、TOM等。这一层审查会比政府的防火墙更加严格，可以说使用境内服务商的邮箱基本不安全。境外邮箱一般较为安全，但取决于服务商与中国是否有利益交换。比如一定要拒绝使用以出卖师涛等人而臭名昭著的Yahoo.

Gmail相对来说比较安全一些，因为Gmail的服务器都在国外，且没有完全公开，还要通过邀请添加帐户，因此安
全系数相对而言要高一些，Gmail登陆网页也因此经常被中国当局封锁，不过可以使用代理软件登陆。当你在使用gmail邮箱时，应进行加密：在流览器那
里输入https://mail.google.com，请不要丢了“http”后面的那个“s”。
S代表“安全”（Security）。这样你的邮件收发过程就会在加密状态下进行，网络监控者无法看到邮件的内容。但是收发你邮件的朋友也必须使用这个办法进入gmail邮箱，否则也不能保证别人偷看不了你的邮件内容。

作者在此特别推荐使用加密功能很强的邮箱：Hushmail.Hushmail使用的时候需要下载一种Java小程
序，收发邮件都是在客户端，而不是在服务器端进行。如果所有过程都在服务器端进行，你的信息是被记录的，包括个人信息、收发邮件内容，服务商可以看到，这
些信息被劫取可能性大。如果收发邮件过程在客户端，那谁也不知道你发了什么内容的邮件，Hushmail也不知道。第二，Hushmail用的是商业系统
最高的加密，中国监控部门很难破解。如果收发双方都使用Hushmail，安全系数是目前最高的。

还有另外一些非盈利的网络服务商提供加密收发电邮的服务，帮助用户提高通信安全。比如，www.riseup.net；ww.vaultetsoft.com；www.bluebottle.com；www.fastmail.fm；www.safe-mail.net.
其中值得推荐的是riseup，它比gmail要安全，当然使用riseup邮箱也需要用户与其联系用户之间同时使用，这样才能达到邮件内容安全不被外泄
的效果；否则，只有你一方使用riseup邮箱，而对方使用的是Yahoo或者sina等邮箱，虽然邮件内容在你这里是加密状态的，但是当你的朋友在非加
密状态下收到时，你的邮件内容还是会被网络监控系统发现。

此外，设置好电子邮件的通行密码很重要，不容易被破译的密码不得低于8位，不要使用纯数字、纯字母，不要使用给你本
人有关的词语，如姓名，生日，家乡，家属姓名等等。密码位数越长，被破译的几率越小。最安全的密码需要数字、大小写字母、各种字符混合组成，如
12ABde#*89.（打开你的电脑，最好也需要设置这样的开机密码，并设置为每隔几分钟自动关闭频幕，以防你离开电脑时其他人趁虚而入。）即使你的密
码设置的非常复杂，也需要经常更换。而且最好不要将你的邮箱、电脑、skype等即时通讯的密码设为同一个，那样的话，一个被破译，则其他的通讯方式的密 码也就同时被破译了。

千万不要让电脑记住你的通行密码。网民在每次登陆电子邮件时，电脑总是提示是否需要记住该密码，请在登陆前选择不要记住你的通行密码，这是很不安全的。电脑如果被攻击或没收，他人将轻易进入你的电邮。

还有最好不要查阅陌生人发来的邮件，尤其是附件，以免打开携带病毒的破坏性文件。即使是以“朋友”名义发来的，最好检查电邮地址，有时是经过很巧妙细小的变化后冒充的。当然，对于那种盗窃别人信箱发邮件的犯罪行为，是很难设防的。

3. QQ安全措施

由于QQ的后门问题，腾讯公司是即时通讯软件里帮助当局进行言论审查和迫害最主要的帮凶，建议坚决拒绝使用QQ.确迫不得已要使用的话，不要在使用代理软件突破网络封锁和进行敏感谈话时同时使用QQ.群内聊天是使用QQ最危险的，基本有敏感词语都会被记录下来。

4. SKYPE安全措施

（1）。绝对不能安装TOM-
Skype版本：一定检查一下，看你是否已经装错了，除非你十分希望自己的所有秘密暴
露在监控人员眼下。由于中国用户正常访问Skype网站会被强行劫持，所以要安装Skype国际版只能通过自由门、无界网络等代理软件，使用这些代理软件
时是可以在Skype标准网站下载国际版本的。同时比较大的软件下载网站一般都有提供Skype国际版下载，只须不要误下TOM-Skype即可。

（2）。清除聊天记录：按照以下介绍的步骤，把你的skype聊天选项设置好，减少网监网警和网盗侵犯你通讯自由和
隐私权的机会。万一你的电脑被盗、或被警方没收，有人可能会打开你的电脑、甚至非法进入你的Skype账户进行搜查，包括查阅你的聊天纪录。这种情况很难
设防。有一点你可以做到，就是随时清除你的“聊天历史”，按以下步骤设置“不保留会话记录”：

登陆进入skype账户后，点击视窗左上角的“文件”；当选项菜单出现后，点击“隐私（X）”；这时，另一个视窗就
会打开，在这个视窗里的“保留会话记录时长”下面，有两个地方供你选项：左边那个，你点击一下，就会看到五个选择：“永久保留”，“没有历史纪录”，“两
周”，“一个月”，“三个月”。请选择“没有历史纪录”。这样一来，你的打字聊天内容今后在你的电脑上就不会留下纪录。在另一个小长方块里，如果你点击
“清除会话纪录”，你在此之前给朋友聊天的纪录也就会从你的电脑上消失。

（3）提高Skype打字聊天安全系数：对skype打字聊天目前还没有实现全面监控。但是用户可以采取一些措施去
提高skype聊天对话的安全系数，如，避免所谓“敏感”字眼，打字聊天时尽量其他词语和符号；弄清楚你在给谁聊天：即使你使用原版Skype，最好能事
先确定你的聊天伙伴的真实身份，然后再开始打字会话。

5. MSN安全措施

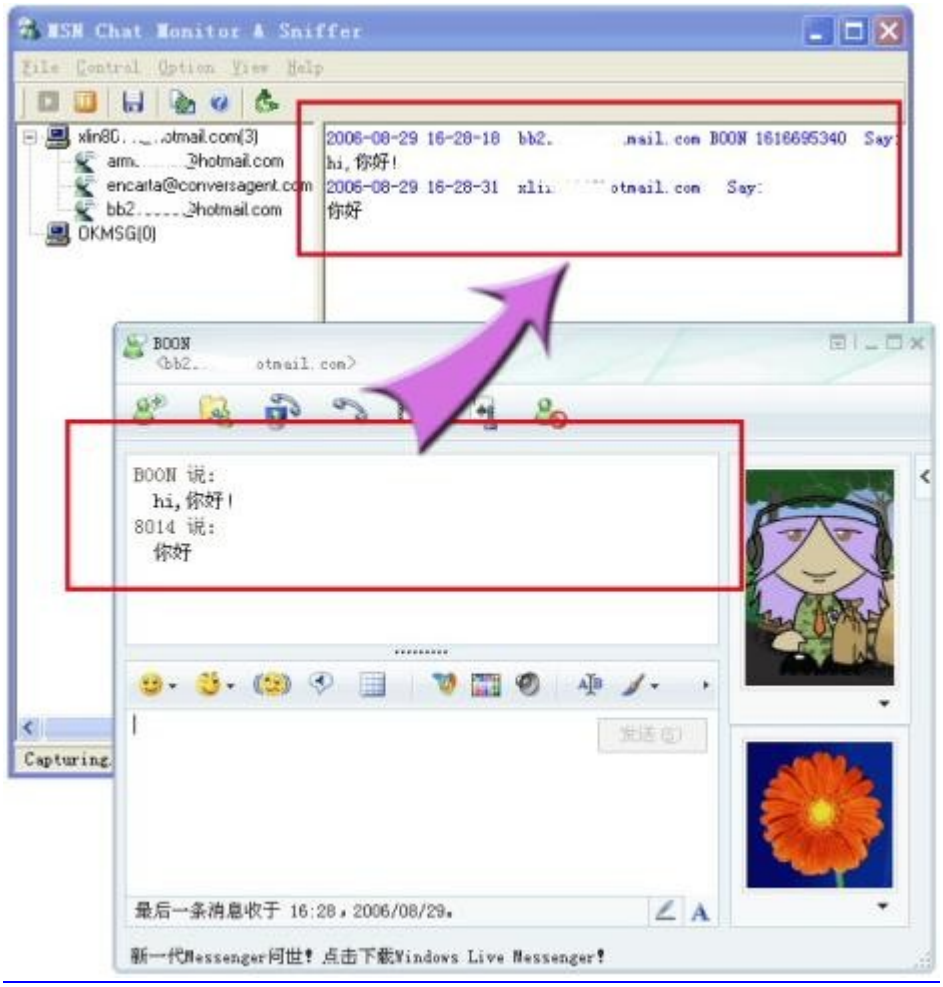
要保护自己的聊天信息不被记录，可以使用MSN Shell的聊天加密功能。MSN
Shell是一个支持MSN而提供多种扩展服务及功能的免费插件。MSN
Shell加密MSN聊天内容的前提是MSN聊天的双方必须都使用MSN Shell才行，若是只有一方使用MSN Shel，是无法实现加密聊天内容的。当聊天的双方进行通信时，MSN
Shell会首先检查对方是否开启了加密功能，如果对方没有安装，就仍然以明文的方式发送和接收消息了。如果已安装，则双方自动交换公匙，下面就可以开始
放心大胆地用MSN聊天了，因为这时的聊天内容是加密的，别人拦截到的数据即使看到也不过是一堆乱码而已。无论是局域网内或路由级别的嗅探工具亦无法偷窥
您的MSN聊天内容，挡住来自网络的偷窥行为

MSN Shell可以在网商的网站下载：http://my.msnshell.com/

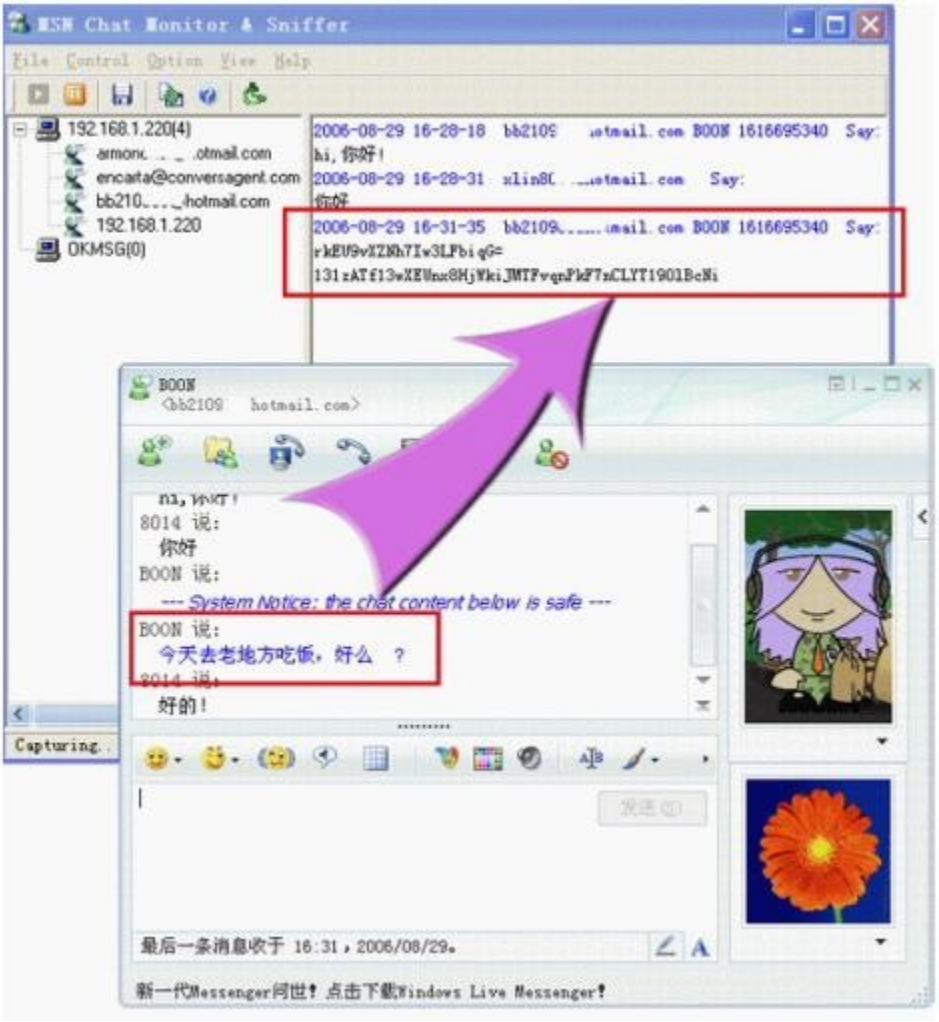
使用步骤：

Shell菜单->设置->加密聊天->启用加密聊天

可选向没有启用加密聊天的联系人发送推荐信息。只有双方都使用了本软的功能加密才能成功。可选颜色提醒，以区别是否进行了聊天加密。可选在消失重插入安全提示信息，可选声音提示会话安全性。



效果截图：没有加密前，可以被窃听软件直接看到对话内容



效果截图：开启加密后，窃听软件拦截到的数据是加密后的乱码

四、保障公民言论自由和通信自由

由于中国政府对现代电讯通讯工具所作的严厉监控严重侵犯公民的基本人权，我们有理由敦促中国政府遵守向国际社会所作的维护人权的保证，保障和尊重公民的言论自由和通信自由权利。

任何政府部门和立法机构都没有权力颁布政策和法规剥夺基本自由人权，任何削弱、打压、限制、监控公民言论自由权的政策、措施都不能高于位阶远在它们之上的法律，宪法，国际人权法。

譬如在无锡蓝藻短信案中，无锡警方根据《治安管理处罚法》认定，丁某属于“散布谣言，谎报险情、疫情、警情或者以其
他方法故意扰乱公共秩序”（第二十五条第一款），故对丁某作出拘留十天的最重处罚。但是《治安管理处罚法》还规定，“实施治安管理处罚，应当公开、公正，
尊重和保障人权，保护公民的人格尊严”（第五条）。而《宪法》中最重要的人权条款第三十五条规定：“中华人民共和国公民有言论、出版、集会、结社、游行、
示威的自由”。既然是宪法权利，执法者在运用下位法时必须优先考虑对言论自由的保障，两者之间妥善加以权衡，不宜轻易以维护公共秩序为由做出对公民的重 罚。

公民的言论自由权利应得到保障和尊重。中国政府在1998年就签署了联合国《公民权利和政治权利国际公约》，该《公

约》第十九条规定：“一、人人持有主张，不受干涉。二、人人有自由发表意见的权利；此项权利包括寻求、接受和传递各种消息和思想的自由，而不论国界，也不
论口头的、书写的、印刷的、采取艺术形式的或通过他所选择的任何其他媒介。三、本条第二款所规定的权利的行使带有特殊的义务和责任，因此得受某些限制，但
这些限制只应由法律规定并为下列条件所必需：（甲）尊重他人的权利或名誉；（乙）保障国家安全或公共秩序，或公共卫生或道德。”以上国际公认的原则确立了
保障言论和传播信息的自由是常态，运用法律加以限制是例外。

公民的通信自由也是受到国际法、我国宪法和刑法保护的基本权利。《公民权利和政治权利国际公约》第十七条规定：“任
何人的私生活、家庭、住宅或通信不得加以任意或非法干涉”。中国宪法第四十条规定：“中华人民共和国公民的通信自由和通信秘密受法律的保护。除因国家安全
或者追查刑事犯罪的需要，由公安机关或者检察机关依照法律规定的程序对通信进行检查外，任何组织或者个人不得以任何理由侵犯公民的通信自由和通信秘密。”
《中华人民共和国刑法》第二百五十二条规定：“隐匿、毁弃或者非法开拆他人信件，侵犯公民通信自由权利，情节严重的，处一年以下有期徒刑或者拘役。”而在
现代社会，所谓“通信”早已超出了信件来往的范畴，通过互联网和手机进行的通信理应包括在内。根据国际惯例，除非公民涉嫌刑事犯罪和给社会和他人造成明显
可见的灾难性后果的行为，除非是在战争等非常时期，否则跟踪和截获公民的通讯内容本身是违法的。

为此，我们向全国人大、政府提出以下建议：

一、在《宪法》中增加规定国家不得制定剥夺或压制言论出版自由权利的法律。

二、对涉嫌侵犯公民言论自由和通信自由权利的法律、法规、规章等规范进行违宪审查，并依法纠正。

三、除《宪法》第四十条规定的因国家安全或者追查刑事犯罪的需要，由公安机关或者检察机关依照法律规定的程序对通信进行检查外，禁止政府和执行公务人员以任何理由任意侵犯公民的通信自由和隐私权。

四、保障公民通过互联网、电讯通讯工具对任何国家机关和国家工作人员提出批评、建议、申诉、控告、检举的权利。

五、尊重《中华人民共和国国家通用语言文字法》规定的“公民有学习和使用国家通用语言文字的权利”，禁止在互联网上使用关键字词过滤手段破坏国家通用语言的使用，以及限制使用国家通用语言文字来表达思想观点的自由。

六、政府部门不得制定和执行剥夺或压制上网用户户言论出版自由权利的规则，任何屏蔽、监视、禁止、限制、破坏向公众
提供电子公告类信息发布服务（电子公告牌、电子白板、电子论坛、网络聊天室、留言板、电子邮件、博客、QQ、msn、skype即时通信等）的网站并监视
个人信息交换的措施都应该废除，并依法追究有关政府部门的责任。

1、信息产业部《进一步加强移动通信网络不良信息传播治理的通知》, 见http://tech.sina.com.cn/t/2005-10-10/1158736111.shtml
2、CNNIC的职能见http://baike.baidu.com/view/21970.htm.
3、 其名称得自2002年5月17日Charles R. Smith所写的一篇关于中国网络审查的文章《The Great Firewall

of China》，取与Great Wall（长城）相谐的效果，简写为Great
Firewall，缩写GFW，戏称功夫网。随着使用的广泛，GFW已被用于动词，GFWed是指被防火长城所屏蔽。
4、QQ网站"QQ群使用帮助"的说明："群是为QQ用户中拥有共性的小群体建立的一个即时通讯平台。比如可创建"我的大学同学"，"我的同事"等群，每个群内的成员都有着密切的关系，如同一个大家庭中的兄弟姐妹一样相互沟通。" http://www.qqjia.com/learn/qqgroup.htm
5、
根据法轮功明慧网报导，中国公安根据它们监控QQ的纪录，追查中国国内的法轮功学员的真实IP地址。例如，2001年，某个黑龙江法轮功弟子说，她就是因
爲使用QQ，被黑龙江省公安厅约谈，该公安还威胁说，它们利用QQ，已经监控2000多个人。这位法轮功学员还表示，他曾和河北的法轮功弟子聊天，该位人
士是某个网站的作者，也被国安威胁说，QQ监控达6000多个。

（-全文完-）

附件：

附件一：中国网监目前使用的关键字基本过滤词表[相关部分]

附件二：QQ是如何监视你的聊天记录？

附件一：中国网监目前使用的关键字基本过滤词表[相关部分]

本报告作者、中国网络专家于声雷（化名）经过特殊途径拿到了中国官方关键字基本过滤词表，并将本词表中非法过滤所谓
敏感（“政治类”）言论或人物姓名部分以及英文部分在本报告里公之于世。此关键字过滤词表是最基本的，但在实际使用中，监控部门会根据政策、形势等增加词 表，服务商也会因自我审查而增加词表。

政治类：

三个代表，一党，多党，民主，专政，政治，大法，弟子，大纪元，真善忍，明慧，大法，洪志，红志，洪智，红智，法
轮，法论，法沦，法伦，发轮，发论，发沦，发伦，轮功，轮公，轮攻，沦功，沦公，沦攻，论攻，论功，论公，伦攻，伦功，伦公，打倒，民运，六四，台独，王
丹，柴玲，李鹏，天安门，江泽民，朱容基，朱镕基，李长春，李瑞环，胡锦涛，魏京生，台湾独立，藏独，西藏独立，疆独，新疆独立，警察，民警，公安，邓小
平，大盖帽，革命，武警，黑社会，交警，消防队，刑警，公款，首长，书记，腐败，城管，暴动，暴乱，李远哲，司法警官，高干，人大，尉健行，李岚清，黄丽
满，于幼军，文字狱，宋祖英，天安门，自焚，骗局，猫肉，吸储，张五常，张丕林，空难，温家宝，吴邦国，曾庆红，黄菊，罗干，吴官正，贾庆林，专制，三個
代表，一黨，多黨，民主，專政，大法，弟子，大紀元，真善忍，明慧，洪志，紅志，洪智，紅智，法輪，法論，法淪，法倫，發輪，發論，發淪，發倫，輪功，輪
公，輪攻，淪功，淪公，淪攻，論攻，論功，論公，倫攻，倫功，倫公，打倒，民運，六四，台獨，王丹，柴玲，李鵬，天安門，江澤民，朱容基，朱鎔基，李長
春，李瑞環，胡錦濤，魏京生，臺灣獨立，藏獨，西藏獨立，疆獨，新疆獨立，警察，民警，公安，鄧小平，大蓋帽，革命，武警，黑社會，交警，消防隊，刑警，
公款，首長，書記，腐敗，城管，暴動，暴亂，李遠哲，司法警官，高幹，人大，尉健行，李嵐清，黃

麗滿，於幼軍，文字獄，天安門，自焚，騙局，貓肉，吸儲，
張五常，張丕林，空難，溫家寶，吳邦國，曾慶紅，黃菊，羅幹，賈慶林，專制，八九，八老，巴赫，白立朴，白梦，白皮书，保钓，鲍戈，鲍彤，暴乱，暴政，北
大三角地论坛，北韩，北京当局，北京之春，北美自由论坛，博讯，蔡崇国，藏独，曹长青，曹刚川，柴玲，常劲，陈炳基，陈军，陈蒙，陈破空，陈希同，陈小
同，陈宣良，陈一谘，陈总统，程凯，程铁军，程真，迟浩田，持不同政见，赤匪，赤化，春夏自由论坛，达赖，大参考，大纪元新闻网，大纪园，大家论坛，大
史，大史记，大史纪，大中国论坛，大中华论坛，大众真人真事，戴相龙，弹劾，登辉，邓笑贫，迪里夏提，地下教会，地下刊物，第四代，电视流氓，钓鱼岛，丁
关根，丁元，丁子霖，东北独立，东方红时空，东方时空，东南西北论谈，东社，东土耳其斯坦，东西南北论坛，动乱，独裁，独夫，独立台湾会，独立中文笔会，
杜智富，多维，屙民，俄国，发愣，发轮，发正念，反封锁技术，反腐败论坛，反攻，反共，反人类，反社会，方励之，方舟子，飞扬论坛，斐得勒，费良勇，分家
在，分裂，粉饰太平，风雨神州，风雨神州论坛，封从德，封杀，冯东海，冯素英，佛展千手法，付申奇，傅申奇，傅志寰，高官，高文谦，高薪养廉，高瞻，高自
联，戈扬，鸽派，歌功颂德，蛤蟆，个人崇拜，工自联，功法，共产，共党，共匪，共狗，共军，关卓中，贯通两极法，广闻，郭伯雄，郭罗基，郭平，郭岩华，国
家安全，国家机密，国军，国贼，韩东方，韩联潮，何德普，何勇，河殇，红色恐怖，宏法，洪传，洪吟，洪哲胜，洪志，胡紧掏，胡锦涛，胡锦滔，胡锦淘，胡景
涛，胡平，胡总书记，护法，华建敏，华通时事论坛，华夏文摘，华语世界论坛，华岳时事论坛，黄慈萍，黄祸，黄菊，黄翔，回民暴动，悔过书，鸡毛信文汇，姬
胜德，积克馆，基督，贾庆林，贾廷安，贾育台，建国党，江core，江八点，江流氓，江罗，江绵恒，江青，江戏子，江则民，江泽慧，江泽民，江澤民，江
贼，江贼民，江折民，江猪，江猪媳，江主席，姜春云，将则民，僵贼，僵贼民，疆独，讲法，酱猪媳，交班，教养院，接班，揭批书，金尧如，锦涛，禁看，经
文，开放杂志，看中国，抗议，邝锦文，劳动教养所，劳改，劳教，老江，老毛，黎安友，李长春，李大师，李登辉，李红痔，李宏志，李洪宽，李继耐，李兰菊，
李岚清，李老师，李录，李禄，李鹏，李瑞环，李少民，李淑娴，李旺阳，李文斌，李小朋，李小鹏，李月月鸟，李志绥，李总理，李总统，连胜德，联总，廉政大
论坛，炼功，梁光烈，梁擎墩，两岸关系，两岸三地论坛，两个中国，两会，两会报道，两会新闻，廖锡龙，林保华，林长盛，林樵清，林慎立，凌锋，刘宾深，刘
宾雁，刘刚，刘国凯，刘华清，刘俊国，刘凯中，刘千石，刘青，刘山青，刘士贤，刘文胜，刘晓波，刘晓竹，刘永川，流亡，六四，陆委会，吕京花，吕秀莲，抡
功，伦功，轮大，轮功，罗干，罗礼诗，马大维，马良骏，马三家，马时敏，卖国，毛厕洞，毛贼东，美国参考，美国之音，蒙独，蒙古独立，密穴，绵恒，民国，
民进党，民联，民意，民意论坛，民运，民阵，民猪，民主，民主墙，民族矛盾，明慧，莫伟强，木犀地，木子论坛，南大自由论坛，闹事，倪育贤，你说我说论
坛，潘国平，泡沫经济，迫害，祁建，齐墨，钱达，钱国梁，钱其琛，抢粮记，乔石，亲美，钦本立，秦晋，轻舟快讯，情妇，庆红，全国两会，热比娅，热站政论
网，人民报，人民内情真相，人民真实，人民之声论坛，人权，瑞士金融大学，善恶有报，上海帮，上海孤儿院，邵家健，神通加持法，沈彤，升天，盛华仁，盛
雪，师父，石戈，时代论坛，时事论坛，世界经济导报，事实独立，双十节，水扁，税力，司马晋，司马璐，司徒华，斯诺，四川独立，宋平，宋书元，宋祖英，苏
绍智，苏晓康，台独，台盟，台湾独立，台湾狗，台湾建国运动组织，台湾青年独立联盟，台湾政论区，台湾自由联盟，太子党，汤光中，唐柏桥，唐捷，滕文生，
天安门，天怒，天葬，童屹，统独，统独论坛，统战，屠杀，外交论坛，外交与方略，万润南，万维读

者论坛，万晓东，汪岷，王宝森，王炳章，王策，王超华，王
丹，王辅臣，王刚，王涵万，王沪宁，王军涛，王力雄，王瑞林，王润生，王若望，王希哲，王秀丽，王冶坪，网特，尉健行，魏京生，魏新生，温家宝，温元凯，
文革，无界浏览器，吴百益，吴邦国，吴方城，吴官正，吴弘达，吴宏达，吴仁华，吴学灿，吴学璨，吾尔开希，五不，伍凡，西藏，西藏独立，洗脑，下体，项怀
诚，项小吉，小参考，肖强，邪恶，谢长廷，谢选骏，谢中之，辛灏年，新观察论坛，新华举报，新华内情，新华通论坛，新疆独立，新生网，新闻封锁，新语丝，
信用危机，邢铮，熊炎，熊焱，修炼，徐邦秦，徐才厚，徐匡迪，徐水良，许家屯，薛伟，学潮，学联，学习班，学运，学自联，雪山狮子，严家其，严家祺，阎明
复，央视内部晚会，杨怀安，杨建利，杨巍，杨月清，杨周，姚月谦，夜话紫禁城，一中一台，义解，亦凡，异见人士，异议人士，易丹轩，易志熹，尹庆民，由喜
贵，游行，于大海，于浩成，余英时，舆论，舆论反制，宇明网，圆满，远志明，岳武，在十月，则民，择民，泽民，贼民，曾培炎，曾庆红，张伯笠，张钢，张宏
堡，张健，张林，张万年，张伟国，张昭富，张志清，赵海青，赵南，赵品潞，赵晓微，赵紫阳，哲民，真善忍，真相，真象，镇压，争鸣论坛，正见网，郑义，正 义党论坛

英文：

bitch， shit， falun， tianwang， cdjp， bignews， playboy， renmingbao， rfa， safeweb，sex，
simple， svdc， taip， tibetalk， triangle， triangleboy， UltraSurf， unixbox， ustibet， voa， wangce，
wstaiji， xinsheng， yuming， zhengjian， zhengjianwang， zhenshanren， zhuanfalun， anime， censor，
hentai， [hz]， （hz），[av]， （av），[sm]， （sm），boxun， chinaliberal， chinamz，
chinesenewsnet， cnd， creaders， dafa， dajiyuan， dfdz， dpp， falu， falun， falundafa， flg，
freechina，freenet， fuck， GCD， gcd， hongzhi， hrichina， huanet， hypermart， incest，
jiangdongriji， japan， lihongzhi， making， minghui， minghuinews， nacb， na？ve， nmis， paper，
peacehall， playboy， renminbao， renmingbao， rfa， safeweb， sex， simple， svdc， taip， tibetalk，
triangle， triangleboy， UltraSurf， unixbox， ustibet， voa， wangce， wstaiji， xinsheng， yuming，
zhengjian， zhengjianwang，
zhenshanren，zhuanfalun，xxx，anime，censor，hentai，[hz]，（hz），[av]，（av），[sm]，
（sm），porn，multimedia，toolbar，downloader

附件二：“QQ是如何监视你的聊天记录”？

“QQ是如何监视你的聊天记录”？

北京《华夏时报》2005年8月XX日[5]

杭州的徐小姐是腾讯QQ的老用户了，不过，最近发生的一宗QQ号码被封事件，开始让徐小姐变得警觉、惊恐直至愤怒了。

（一）事件——QQ号码被查封

6月里的一天，徐小姐像平时一样打开电脑上网，登陆QQ时，突然弹出一个窗口，提示“禁止使用”，徐小姐试了几次，
仍然是这样。徐小姐后来回忆说：“我先是通过电子邮件询问，没人理我，一个星期后，我终于忍不住打长途电话到深圳，问腾讯的客服，要她给我一个号码被封的

理由。客服几分钟就查到了，说我下载了有关政治性的敏感文档，是有记录的，所以号码才会被查封。”

记者在征得徐小姐的同意后，即以该QQ号码的使用者身份致电深圳腾讯公司，了解号码被查封的情况，在报出QQ号码和密码后，该客服人员让记者稍等，几分钟后，客服人员告诉记者，这个QQ号码在5月30日下载过敏感的信息，所以被查封，而且，“不可能要回来了”！

按照徐小姐的回忆，她的确是曾经下载过一个文档，“如果不是腾讯有记录，我都想不起来了。可我连看都没有看全，又没有散布，这也要封号码？”更奇怪的是，徐小姐当时并没有使用腾讯的TE浏览器下载该文档。

徐小姐怀疑，难道只要装了QQ就可以监视用户的电脑使用情况，并且可以把用户电脑中的资料回传到腾讯的服务器上？如果这是这样，那么，还有什么个人隐私可言？况且作为QQ会员的徐小姐，她本人的身份证号码、手机号码都是按照腾讯公司要求记录在案的。

其实还不仅仅是涉及隐私问题这么简单，如果政府部门或者商业机构中有人在电脑中装有QQ，就有可能造成严重的信息外泄的安全隐患了。QQ捆绑的TE浏览器提供的“谁与我同在”的功能，就可以追踪和了解QQ用户访问了那些网站。

（二）调查——用户信息被记录

一位在软件安全问题方面颇有研究的业内人士向记者证实，通过Iris抓包软件，可以看到QQ在向服务器回传不明数据，并且这些数据是经过加密处理过的。

《科学时报》刊登的一篇文章也表明，腾讯附加在QQ程序中的浏览器程序，提供的一项叫做“谁与我同在”的功能，能让任何用户都可以查到当前浏览的网页上有哪些其他的腾讯QQ用户，同时，也可以监控用户正在察看哪些页面，这些搜集来的用户浏览资料，是可以被商业化利用的。

就在记者开始着手调查并要求对腾讯进行采访的当晚，徐小姐的QQ号码竟然自动解封，可以使用了。

记者致电腾讯公司市场部，并通过电子邮件发送采访提纲要求采访。记者的主要问题是：

1，QQ是否在监视每个用户的使用情况？包括访问那些网站、下载了什么文档？

2，QQ在多大范围内监视这些信息，监视哪些信息？

3，作为一家民营的商业性质的公司，用户的个人资讯和使用习惯如何保证不被他用？

4，对于QQ的监视功能，如果被黑客或者其他情报机构利用，腾讯该负什么责任？

5，对于政府部门或者商业公司的机密，腾讯是否也可以获知？

（三）理由——企图染上政治色彩

记者的采访提纲发出后，腾讯方面并未给予任何书面的文字答复，也没有做出正式的采访安排，而是通过北京的一家公关公司与记者联系沟通。

该公关公司的人员按照记者留下的号码拨通了记者的电话，试图说服记者不要就此事进行追查和报道，她告诉记者，腾讯目前正处于强劲的上升趋势，而市面上各种即使通讯软件也是层出不穷，竞争十分激烈，如果因为记者的报道，引起腾讯QQ在商业上的损失，这是腾讯方面所不希望的。

对于徐小姐QQ号码被封一事，该公关公司人士透露，是腾讯方面接到了上级有关部门的指令，才监视该用户的使用情况并
封掉了她的号码，她不肯透露是是哪个部门要求腾讯这么做的，只是告诫记者，如果就此事进行报道，有可能会“牺牲”。显然是试图把商业问题蒙上一层政治色
彩。而在听到这一消息后，徐小姐表示震惊和愤怒：“我怎么觉得阴森森的？把我当成国家的敌人了？”徐小姐还信誓旦旦地对记者保证，她绝没有通过QQ发布过
任何不良信息，“如果有，让他们拿出证据来，发给谁了？”

据记者调查了解到，对于网络公司及通讯软件公司，上级主管部门的确是提出过要求，对网络上有害的不良信息进行技术过
滤和屏蔽，不得散布和传播，但却没有哪家公司接到过要求监视用户使用情况的指令，“真是要监视一个人，哪用得着他们呀”，一位曾作过情报工作的朋友这样告 诉记者。

（四）警惕--通讯软件安全有隐患

一家通讯软件公司的技术人员告诉记者，在即时通讯软件中加进监控程序，在技术上不难实现，只要在用户本地机上加入几个关键词检索和过滤，就可以把关键信息传回服务器，而不用监视所有的聊天记录。

有关人士介绍说，即时通讯软件都存在着安全隐患，作为消费者是有权知道这些的，而作为一家商业公司却没有权利监视跟踪用户操作记录的，尊重和保护用户的隐私及安全是国际上的通行商业准则。

据赛迪网报道，6月14日，美国纽约州首席检察官办公室表示，AOL时代华纳旗下的Netscape将支付10万美元和解金，该公司因使用追踪用户下载情况的软件而遭投诉。

另一方面，由于QQ本身的安全性能缺陷，针对QQ的各种黑客软件也在不断增长，在中国软件史上，QQ应该是受各种攻击最多的在线即时通讯软件。不少商业公司已经意识到QQ的安全问题，北京的一些单位和商业公司里，是严禁使用QQ软件的。

在记者发稿前，腾讯方面通过电子邮件，给编辑发来了书面答复意见，而杭州的徐小姐却表示不会善罢甘休，她要“打电话问问看”。但无论如何，腾讯记录了该用户的使用信息，这不能不引起更多的使用者对网络通讯软件的安全问题引起重视。

附录：

腾讯公司的书面答复意见

谷龙你好:

关于就杭州用户号码被封一事所发来的提纲，腾讯公司的正式答复如下，希望你凭着客观公*正的态度去报道。

首先需要严正申明的一点是，海量的信息之下，腾讯公司采取点对点的消息收发方式，决定了腾讯不能去监视用户在电脑上的操作情况。任何进行不实情况的报道的单位或个人，则需负相应责任。

作为一种即时通信软件，腾讯QQ在技术上采用的原理是一种点对点的方式。也就是
说，在大部分情况下，用户之间的沟通是从一个用户到另一个用户，不需要通过腾讯服务器的中转。只有在网络不稳，网络情况复杂或用户下线等特殊情况下，腾讯
服务器才会帮助用户保存并中转留言。按照上级的网络安全信息处理的规定，通过服务器中转的留言，作为腾讯公司发出的消息，将会经过信息安全的过滤机制，该
名用户正是因为通过腾讯服务器中转了含有敏感词汇的留言内容，因此腾讯做了封号处理。至于后来解封，是因为该用户的留言内容虽含有敏感内容，但还不属于有
意传播非***法内容的情况。为了保障用户权益，我们对这个号码做了解封的处理。

腾讯公司一向注重并保护用户隐私。关于该用户的留言内容，发送时间与对方号码，腾讯目前不能提供。

如有需要，腾讯会在法律手续齐全的情况下提供。

腾讯QQ为海量用户提供服务，每天有超过两千万用户上线沟通、聊天。发送消息量在10亿条/天左右，腾讯无必要也无能力保存每位用户的每条留言纪录，更谈不上监视一亿六千万用户的电脑使用行为。

在主管部门的要求下，腾讯会配合主管部门对网络安全工作进行协助，并按主管部门要求做一些处理。一切行为均符合有关规定与要求。

腾讯公司

中国网络监控报告之一：揭开中国网络监控机制的内幕