匿名日志

这是份匿名登录网上日志〔博格〕的简易操作索引，尝试探讨在一个行政低透明度的国家中，政府部门中工作的举报人会遇到的问题。这不是要教人成为专业网络加密者〔cypherpunks〕，只是给身在发展中国家，担心自身安全且想以简便方式保护其隐私的人。

莎拉的案例

莎拉在政府部门中担任会计。她发觉自己的上司—副部长，正从政府部门中窃取巨款。她想让大众知道这宗正在发生的犯罪行为，但又担心因此丢掉工作。如果她向部长汇报此事〔如果她能和部长订到约会的话！〕，则可能惹祸上身。她打电话给本地报社的一名记者，但记者说，无法报导这没有更多讯息与相关文件佐证的指控。

因此，莎拉想建立网上日志，以便透过它告诉大家自己所知道这桩正发生的事。为了自我保护，她想确定没有人会依循她的网上日志地址而找到她—她需要匿名建立日志。

当她尝试以匿名登入网上日志时，有两种主要方式可找到作者。其一是她在发表的内文中透露身分，例如莎拉说：「我是矿业部副部长的主要会计助理」。那么，网络日志的读者将很可能以此迅速指认出她的身分。
电子前沿基金会〔The Electronic Frontier Foundation〕的指南"How to Blog Safely"中，提供了些很好的建议，教人如何避免因其 blog 的内容而泄漏自己的真实身分。

另外会让莎拉身分曝光的原因是：如果有人能从网络浏览器 web browsers 或 email 程序中提供的讯息认出她的身分。每台计算机上网时都对应〔或共享〕一个称为 IP 的网络地址。这是一串号码，中间以“.”隔开为四组数字，是从 0 到 255 之间的任意整数，如 213.24.124.38。当莎拉通过网络浏览器在部长的 blog 上发表评论时，她所使用的 IP 地址便会显示在她的帖子上。

只要花一点功夫，部长的计算机程序员就很可能由 IP 地址追查到莎拉的身分。如果莎拉此时正在家中用电脑拨接上网，网络服务供货商〔ISP〕会纪录下这个 IP 地址是在哪个特定时间，由哪个电话号码上线。在某些国家，部长可能还需要申请法院传票以取得这些纪录；在另一些国家中〔特别当网络服务供应商是国营企业时！〕，网络服务供货商便会轻易地泄漏讯息，莎拉将因此陷入困境。

有许多办法可以在上线时隐藏莎拉的真实身分。想当然，越安全的办法就需要越多的手续来隐藏身份。莎拉，以及任何想匿名上网络日志的人，要先考虑自己会多紧张、多疑神疑鬼怕被揭发，然后再考虑愿意付出多少力气来保护自己的真实身分。各位将会在下面看到，有些线上保护策略需要使用者有充足的计算机专业知识与技巧。

方案一—假名

有个简单的办法可隐藏莎拉的真实身分，就是使用非其所在国家主机提供的免费电子邮箱和免费网上日志。〔使用付费邮箱或网络主机服务是下下策，因为是以连结信用卡帐户、支票帐户或转帐付费，由此即可轻易循线找到莎拉。〕她可以在注册网上帐号时编个新身分—假名，当部长看见她写的帖子，他只会发现这是一位叫"A. N. Ymous"网民所发，其 email 地址是。anonymous.whistleblower@hotmail.com.

提供免费邮箱：
- Hotmail
- Yahoo
- Hushmail：高度加密的免费邮箱

提供免费连结网上日志主机：
- Blogsome：免费 WordPress 日志
- Blogger
- Seo Blog

此战略会产生的问题：当莎拉登入网络邮箱或日志时，她所登入的网络服务器将会记下 IP 地址。如果能循这个 IP 地址追踪到她、如果此时他正在家中或办公室里用电脑、如果这 email 或往上日志所属公司被迫透露使用者相关讯息，那么，她将很可能被追踪。虽然要从大部分网络公司得到使用者的讯息并不是件简单的事；例如：部长需有法院传票，说不定还要与有法律强制力的局署合作，才能从 Hotmail 得到莎拉上网的 IP。但如果政府能从网络邮箱或日志的主机查出他的身分的话，那么莎拉或许不想冒这个可能被发现的险。

方案二—公用电脑

莎拉可做一个附加步骤来隐藏身份—从一台多人使用的电脑进入网上日志。与其从家中或工作单位的电脑设定网络邮箱或日志，不如由网吧、图书馆或大学计算器中心的电脑上进行设定。部长若追踪这个 IP 地址，他将发现这地址在一间网吧，任何人都可能是电脑使用者。

此战略的缺点在于：如果网吧或计算器中心的电脑会保留某人、在某时段、使用某台电脑的纪录，这可能也会危及莎拉的真实身分。她就应避免在深夜、身边无旁人时在计算器中心上网写帖子—或许哪个过分好奇的值班人员会记住她是谁。而且，她也必须常常更换网吧。如果部长察觉所有的举报人发帖地址都来自 Main Street 的"Joe's Beer and Bits"网吧，就可能派个人去盯哨，查看是谁在写这网上日志以便将莎拉逮个正着。

方案三—匿名代理服务器

关于匿名代理服务器，详见下附的“绕道”一章。

莎拉开始感到厌烦，每次要贴日志都必须到 Joe's 网吧。在一个网络极客邻居帮助下，她在自家电脑上做了设定，通过匿名代理服务器中转上网。现在，当她使用网络邮箱及日志时，是通过代理服务器为中继，而非直接以自家电脑的 IP 地址访问网站。这将使部长更难追踪到她。

首先，莎拉用 Google 搜寻"proxy server"〔代理服务器〕，在线寻找提供服务器网站的清单。而后，莎拉从 publicproxyservers.com 网站里选取一个提供高度匿名"high anonymity"服务器的网站。她抄下代理服务器 IP 和清单上的连接端口名。

提供公用代理服务器名单：

- publicproxyservers.com – 列出匿名与透明代理服务器
- Samair (http://www.samair.ru/proxy/) - 只列出匿名代理服务器并包含支持 SSL 的服务器信息。
- rosinstrument proxy database(http://tools.rosinstrument.com/proxy/) -数据库中可搜寻代理服务器。

然后开启「喜好」"preferences "。在「一般」"general"，「网络」"network" 或「安全」"security"〔通常是在这里〕选项下，可找到设定连接网络的代理服务器。〔我所用的火狐 Firefox，通往此选项的路径为：Preferences - General - Connection Settings〕。接着，打开「手动设置」"manual proxy configuration"，键入代理服务器 IP 取代 HTTP 和 SSL 传输，并存取设定。最后，重启浏览器，便可开始上网。

她将发现连接速度有点慢，因为每开启一网页都需绕道，即是以先连上代理服务器，再经此连上 Hotmail 的方式，代替直接访问 Hotmail.com。当 Hotmail 回传网页时，同样也是经由代理服务器后再传回给莎拉。同时也会出现访问网站发生困难的情形，特别是那些莎拉想登入的网站。但至少她的 IP 不会在网上日志留下纪录。
有个关于代理服务器的有趣例子：访问 noreply.org 网，这是个受欢迎的转寄网站，他会以告知你 IP 的方式和你开玩笑：嗨！pool-151-203-182-212.wma.east.verizon.net 151.203.182.212，幸会啦！

现在，连上 anonymizer.com 网站，这是可让人通过匿名代理服务器浏览网页的网站。在 anonymizer 页的右上角键入网页地址：http://www.noreply.org〔或直接点击连结 [http://anon.free.anonymizer.com/http://www.noreply.org]〕。你将发现 noreply.org 会认为你是来自 vortex.anonymizer.com.的访问者〔Anonymizer 是个不错的方法，能测试代理服务器又不需更改浏览器设定〕。但是他无法支持大部分较复杂的网络服务器，如电子邮件及日志。最后依照上述指示设定好浏览器，以匿名代理访问 noreply.org，看看它认为你是从那儿上网的。
可代理也不是最佳办法啊！如果莎拉所在的国家有监控互联网的法律，许多网民就会通过代理服务器访问被封锁的网站，政府便会封锁某些常用的代理服务器；网民因此有会转而使用其它的代理服务器，政府又会再封锁这些代理服务器，如此，反复循环不以。这些循环过程便往往会耗费网民大量的时间。
还有另一重问题：如果莎拉是极少数几个在其国家使用代服务器的人，并且，发表的文章都来自同一代理服务器；甚至，部长有权进入本国所有网络代理商的系统，那么，部长便能查出莎拉的电脑是少数几个使用代理服务器的。所以，最好要使用最普及的代理服务器并常更换使用新的代理服务器。

方案四—代理服务器第二种选择—这回是私人的！

莎拉开始假想：如果使用的代理服务商与政府妥协，会有什么后果？倘若部长说服代理服务商—无论是以合法或非法手段—保留通信纪录，并查验是否有该国人民使用此代理服务，以及通过代理服务访问了哪些网站。莎拉仅依靠代理服务的管理员来保护自己，但她甚至不知道这管理员是谁！〔事实上，通常管理员也不会知道她在使用代理服务器，除非有意外，否则代理服务器是不对外开放的〕。
莎拉有个朋友在加拿大—这是个不太对网络进行监控的国家—这位朋友将十分愿意帮助莎拉进入网络日志，同时又能保护她的身分。莎拉打电话给这个朋友，请她在其系统上设置「绕道」。所谓绕道，就是某人在自己电脑上建立代理服务器，让其它人可通过此代理服务上网。莎拉的朋友吉姆从网上下载了 Circumventor (http://www.peacefire.org/circumventor/simple-circumventor-instructions.html)，将之安装在自己的 Windows 上。安装工作并不简单，必须先安装一种脚本语言：Perl 而后再安装 OpenSA，最后才是绕道系统。从今以后，他必须随时让电脑在联机状态，好让莎拉可随十使用代理而无需每次使用前请吉姆开启联机。吉姆装好软件后，打莎拉的手提电话

告诉她一个网页地址，莎拉便可开始通过吉姆电脑作为代理服务器上网。这是对莎拉而言较适合的办法，从此可使用自家电脑或网吧电脑连接代理服务器，而不需改动电脑里的任何系统。

当莎拉正对吉姆的帮助感到非常满意时，也正面临一个待解决的主要问题。吉姆的电脑因为运作 Windows 的关系，常常要重启。每次一重启，网络供货商就会为电脑换一个新的 IP，每次这情况发生，代理服务就会中止，吉姆就必须再次联系莎拉，告诉她绕道系统现在用的新 IP。这问题会造成金钱上的浪费，同时也非常烦人。莎拉亦担心，如果她长时间使用同一 IP，自己的网络供货商若屈服于政府压力之下，便会开始封锁她的 IP。

方案五—随机路由传输

吉姆建议莎拉通过 Tor 上网。这是一种较新的技术，专为高度匿名上网而设计。随机路由传输的灵感源自代理服务器—电脑随你的利益需求而运作—甚至可到很复杂的程度。每次请求传输信息，都会透过随机路由网络，绕经二至二十台挂靠电脑，让追索原请求传输电脑的行动变得很困难。通过随机路由进行的每一连串步骤都是经过加密的，这让莎拉所在地的政府更难追查到她的地址。此外，在这一连串传输线上的每部电脑都只会知道最邻近的几台电脑地址。换言之，路由器 B 只知道路由器 A 经过它传输一网页，而这个传输请求可能又经过路由器 C 代转。这些传输请求都是加密的—路由器 B 无法清楚知道莎拉访问的网页到底是什么，或者，最终是哪个路由器接到网络服务器执行传输。

电脑相关技术总是让人感到很复杂，但莎拉兴奋地发现 how easy it is to install Tor (http://tor.eff.org/cvs/tor/doc/tor-doc-win32.html)，这是个随机路由传输系统。莎拉下载并安装 Tor 到自己的系统，而后下载并安装 Privoxy，这是伴随 Tor 一起运作的代理服务器，它有个令人满意的附带好处：可清除大部分莎拉访问网页中的广告。
安装完软件并重启电脑后，莎拉连上 noreply.org，发现自己成功地被 Tor「隐蔽」起来—noreply.org 认为她是从哈佛大学上网的。她又重新进入 noreply.org，这回，她被认为是来自德国的访客。由此可知，每经过依次传输，Tor 就会改变一次莎拉的身分，以便保护她的隐私。可是这会造成其它的后果。当莎拉经 Tor 使用 Google 时，就面临语言不断被转换的困扰！在某次查询中，她先在英语查询系统里，再来，变成了日语，而后又换成德语、丹麦与及荷兰语，转换每数分钟发生一次。莎拉不介意趁机学点新语言，但她担心其它伴随而来的后果。莎拉想在维基〔或维琪〕百科 Wikipedia 上发表文章，但发现，当她使用 Tor 时，维基百科便无法显示她编辑的文章。

连结其它代理服务器时，莎拉发现使用 Tor 也会发生同样的问题。她的网速比从前不使用代理服务器时慢了些—她发现自己只在进入敏感网页内容及在日志贴帖子时才使用 Tor。并且又再次只能在家中上网，因为她无法在公用电脑上轻易安装 Tor。
最让她担忧的是，她发现 Tor 有时竟无法运转！想当然，是因为她的 IP 阻挡了某些 Tor 的路由—当 Tor 试着要使用被堵塞的路由时，莎拉等上好几分钟还是见不着自己要连结的网页。

方案六—MixMaster，隐形日志和 GPG
可以确定的是，即使 Tor 的设计如此精密，还是有个解决贴日志又不需使用代理服务的办法。
和当地某网络高手讨论一阵后，她发现一个新的接口：Invisiblog

(http://www.invisiblog.com/)，一个由澳大利亚的匿名集团〔而且他们疑心病真是够重〕操作的网站，叫 vigilant.tv，是个隐形日志。你无法像使用一般网络日志一样，从网络上直接到隐形日志贴帖子，必须经由一种特殊格式化的电子邮件，经过 MixMaster 转寄邮件系统，以密码署名。

为了了解如何操作，莎拉花了些时间设定了 GPG (http://www.gnupg.org/)─Pretty Good Privacy 的 GNU 设置，是个公用码加密系统 public-key encryption system (http://en.wikipedia.org/wiki/Public-key_cryptography)。

简言之，公用码加密，是一种让用户寄出的信息只有特定收件人才能解读的系统，但收件人不需使用相同的一套密码即可阅读，且能让你亦可阅读其它人寄送给收件人的信息。公用码加密亦可让寄件人在文件上用数码签名方式署名，使人无法辨认签名笔迹。

她在电脑里生成一副密码，用以在日志上贴帖子—以「私人码」署名寄送文章，日志的服务器便能以她的「公用码」辨认出帖子是莎拉寄出的，并将之贴上日志。

關於密碼，亦請看「如何確保電子郵件傳輸的安全？」一章。

莎拉随后又设置了 MixMaster，这是能模糊原始寄件人身分的寄件系统。MixMaster 运用一连串匿名转寄—电脑程序会消除电子邮件中所有关于身分的信息，再将之寄送到目的地—让信件保持高度匿名。经由二至二十次的转寄，即便其中一个或多个转寄「出问题」、留下关于寄件者的蛛丝马迹，信息来源还是变得难以追溯。「建立」MixMaster 必须要编译原始码，这工作需要请求高手协助。

莎拉寄送第一个经由 MixMaster 的信息到持有她公用码的隐形日志上，隐形日志便用这公用码贴上她的新帖子，署名为"invisiblog.com/ac4589d7001ac238"，这一长串字列是她 GPG 码的最后十六字节。她接着又从 MixMaster 寄送下一封信息到隐形日志上，再以公用码署名。
这方式远比前贴帖子要慢得多。MixMaster 间接寄送邮件及表示了邮件需要二小时至二天不等的时间送达网上日志服务器。并且，她在网上看日志时也必须特别留心—如果她太常查看，她的 IP 就会过常出现在登录纪录上，显示她可能是这些帖子的作者。但可确定的是，隐形日志的版主完全不知道她是谁，而且她至少知道更认识一直想了解的自由及开源〔open-source〕软件。
隐形日志的主要问题在于：它难以使用得超出想象，简直不是给常人用的。大多数的人觉得安装 GPG 对他们已经是项挑战，对于复杂的公用码及私人码设定更感到难以理解。于是，开始有许多便于使用的编码工具，如：Ciphire，就是被设计来帮助这些专业水平最低的人，即便如此，还是很难使用。结果，很少人—包括那些真正非常需要使用它的人—大都不用它来寄送匿名邮件。

本文作者注：使用 MixMaster 是项对专业技术的大挑战，如果是使用 Windows 的用户，可在 downloading it
http://prdownloads.sourceforge.net/mixmaster/mix204b46.zip?download.下载一个旧版的 DOS 来使用。我已下载并测试过，可是完全无法运作…或者，可能是我的邮件还在转寄中，尚未抵达目的地。若有人想使用较新版的 DOS 或想用在 Linux 或 Mac 上，必须自行补充某些程序，这对专家而言也是超级困难。如果隐形日志可接收来自一般网络转寄的邮件，如 riot.eu.org，它可能变得更实用。只是，目前为止，我实在不认为它能帮助

那些最需要它的人。

在一个受高度管制的国家，使用还高度加密会产生一连串的问题。要是莎拉的电脑被政府没收，她的私人码也被发现了，就成为最强有利的证据，证明莎拉是那些具争议性帖子的作者。而且，在那些加密上网还不普遍的国家，仅是从 MixMaster 寄出信息—高度加密包裹的邮件—莎拉使用户联网的举动就可能引起当局得密切注意。

什么样的匿名措施才算足够？遭遇什么样的骚扰算过分？

莎拉的解决方案—学习运用密码学及软件以操作 MixMaster─也是你寻求解决上网困扰的方案吗？或者，只需合并使用 1-5 方案就足够让你安心匿名上网贴帖子呢？这件事没有标准答案—任何需要匿名上网的人都需同时考虑所在地条件、自己的技术专业水平和自己会多紧张、疑神疑鬼。如果你有足够的理由害怕因为所贴的文章会危及自身安全，而又能安装 Tor 软件，那么利用 Tor 上网贴帖子是非常好的办法。

噢！最后别忘了千万别在日志署上真名！