介绍

你不能阻止政府监视你，这是人们普遍的一个误解。你可以。不要让政府镇压的恐惧阻止你发表意见。Ritser隐私工具包旨在帮助你保持安全和保持知情的状态。

互联网是怎么办到的

互联网上的所有计算机都有一个IP地址，用来互相通信。网站也有IP地址，但是为了让浏览互联网变得更容易，它们也有域名（例如www.facebook.com以及www.google.com)链接到他们的IP地址。当你的计算机想转到www.google.com执行搜索时，它获取与之有关联的IP并与该计算机通信以获取信息，在这个情况下会是你的Google搜索结果。

您的ISP（互联网服务提供商）将你的计算机连接到互联网。你可能有一个调制解调器，通过电话、电视或光纤电缆连接到ISP的网络。因为你的互联网通过他们的基础设施，他们可以看到你传输的所有数据和你将信息发送到了哪个IP地址。

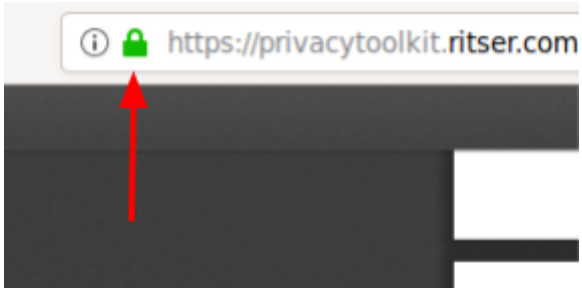
但这并不代表他们必须知道你在访问哪些网站。如果你使用HTTPS加密数据，他们将看不到正在进行的操作，包括URL (www.google.com/search?q=news）。他们只知道你要连接的IP地址，你连接的时间，以及你发送的加密数据的大小。

政府可以追踪到什么

我们来看看政府/ISP能追踪到什么。假设你使用的是HTTPS而不是Tor，你的政府可以追踪你使用的网站和时间。这意味着他们可以知道你在晚上7点38分时访问了IP地址www.facebook.com，但他们不知道你访问了哪些页面或个人档案。他们只知道你游览过www.facebook.com。

如果你*不*使用HTTPS，你的政府也可以追踪你发送到网站的内容。这包括密码和各种URL。

你怎么知道你使用的是HTTPS？通常，当你使用HTTPS浏览时，浏览器会显示如下所显示的锁符号。



HTTPS的工作原理是对浏览器和网站之间的数据进行加密。这意味着它使用数学算法来确保这些数据在传输过程中是不可读的。现代加密算法被认为是安全的，因为即使是最强大的情报机构也无法破解它们。

未加密的连接（没有S的HTTP）如下所示：

从: 70.210.154.182

到： 103.190.246.203 (baidu.com)

时间: 4:42 AM 2020-09-02

数据 (70字节):

游览的网站: baidu.com/account

用户名: alex2

密码: password

加密连接（HTTPS）如下所示:

从: 70.210.154.182

到 : 103.190.246.203 (baidu.com)

时间: 4:42 AM 2020-09-02

数据 (68字节):

o866)F(Yu~1]TEjP47h6(vIEs!dq_'|/Sl^ZMbFriN_"LejUyUYZ%d?sRx;F##Coq9M&

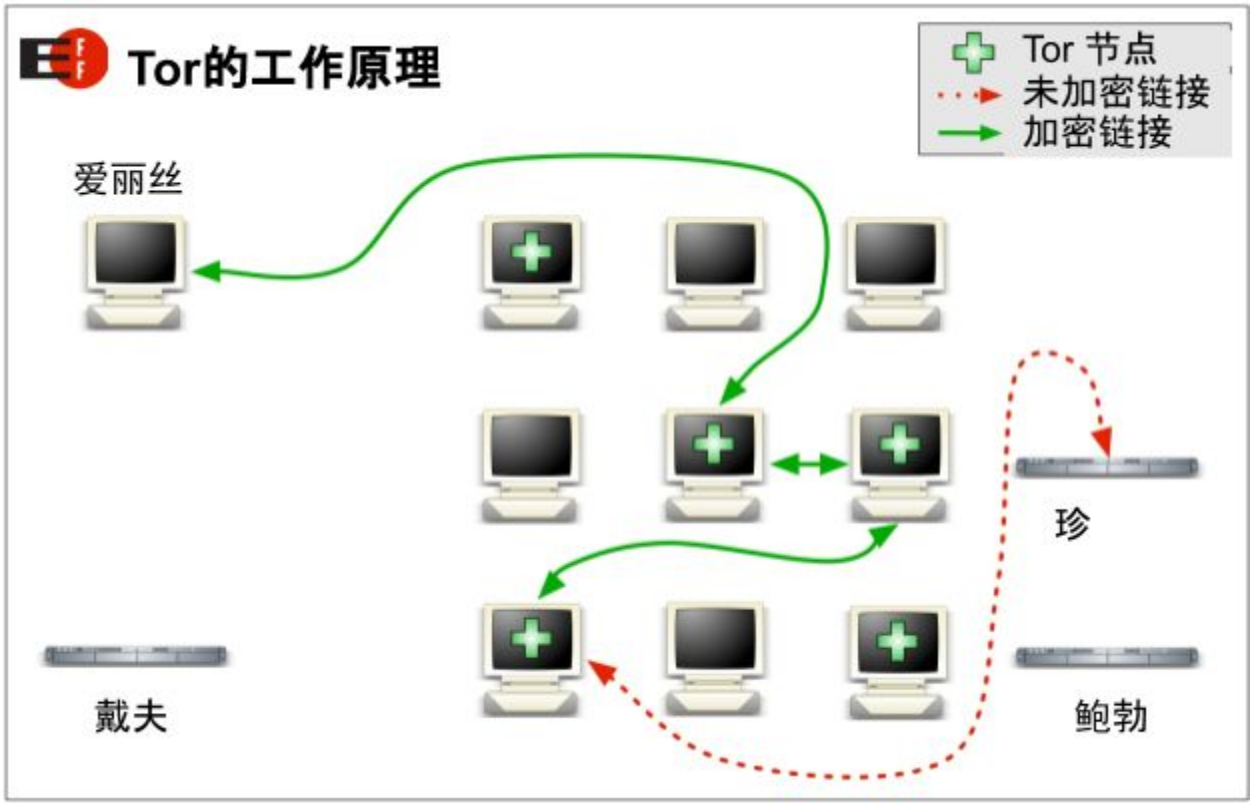
政府可以在网站主人的帮助下追踪什么

然而，HTTPS并**不**阻止网站向警方提供你的数据。你在互联网上访问的每个网站都可以看到你的IP地址。如果一个网站决定给政府你帐户背后的IP地址，**他们可以用它来找到你的真实地址**。重要的是要确保当局找不到你的在线帐户背后的IP地址。

Facebook、Reddit和Google等大型网站都有处理政府要求用户数据的程序。这个过程通常是透明和公平的，因为他们通常不理会独裁政府的法律。例如，谷歌在2014年至2018年间处理了3个埃及用户数据请求。他们全都否认了。

在网站上隐藏你的身份

然而，把你的安全交给跨国盈利性公司不是一个明智的想法。如果你生活在一个国家，而你的身份被暴露了，你的安全就会受到威胁，那么最好使用Tor（包含在本工具包中）。Tor通过在你的网络流量到达网站之前由其他计算机发送它，从而隐藏起你的IP地址。网站将能够看到最后一台计算机的IP而不是你的。你的政府会知道你在访问Tor，但他们不知道你通过它发送了什么，也不知道你在和谁交流。



使用Tor的另一个好处是，由于ISP不知道你正在访问哪些网站，所以他们无法封锁它们。

Tor不是绝对可靠的。如果政府知道你的大致位置，而网站所有者告诉他们你在使用Tor，他们可以在你浏览网站的同时，查看访问Tor的人，以获得你的真实身份。联邦调查局以前也这样做过，但这不应该成为一个问题。如果你担心这个，你可以使用公共WiFi。

旁注： VPN在在线保持匿名方面不如Tor有效。

显而易见的

通常人们被抓不是因为政府获得了他们的IP地址。而是他们向互联网上提交的东西，显示了他们的身份或向他们的朋友透露了他们的身份。人们被抓是因为愚蠢的错误。以下是一些你应该经常做的事情：

1.提交故事时，含糊其辞，编造细节。一小部分信息，比如你兄弟姐妹的数量，可以用来揭露你的身份。

2.在网上提交照片时要**非常**小心。从你上传的所有照片中删除EXIF数据，并验证是否没有可用于识别你的详细信息。

3.如果其他人使用你的电脑，确保你的浏览记录没有被保存。不要将任何可能泄露身份的内容保存到计算机中。

4.不要用你的真名注册那些你用着匿名身份的账户。

5.不要向现实生活中认识的人透露你的匿名身份。

6.不要向你通过匿名身份认识的人透露你的真实身份。

结论

如果你使用匿名的Reddit或Facebook账户，你有时还可保持安全。但如果你的生活依赖这些公司的话，你可能不会想要信任这些公司。如果你想自信地保持匿名，使用Tor。PrivacyTools是其他以隐私为目标的软件的一个很好的资源。

记住：只有你能对自己的安全负责。