反思 • 2026年6月29日

← 上一页

你并不匿名

你未曾选择的信任

简单来说：通过你的邮箱，任何人都可以在几秒钟内查出你在哪里注册了账号，有时甚至能查出你的照片和名字。这不是什么故障：这就是互联网的正常运作方式。问题不在于他们能否看到你——他们能——而在于你被迫信任谁。而唯一一个中间没有人的地方，就是直接对话，从一台设备到另一台设备。

一个电子邮箱就足够了。不一定非得是你的：任何人的都可以。将它输入少数几个免费工具中——这些工具合法、公开、任何人想搜都能搜到——几秒钟内就会出现一个列表：这个邮箱在哪些服务上注册过，有时还会有一张头像，有时还会有它的主人以为从未泄露给任何人的名字和姓氏。你不需要懂技术。也不需要破解任何密码。更没有犯下任何罪行。所有这些信息原本就在那里——被公开、被记录或者被泄露——只等某个人费心去把它们拼凑起来。

人们很容易把这解读为一个错误：一个漏洞、一次疏忽、一个某人应该去修复的东西。事实并非如此。这就是开放网络的正常运作方式。每次你在一个服务上注册、填写一份表格、发表一条评论，或者出现在他人的数据泄露中，你都在留下痕迹。这些痕迹中没有任何一条单独来看是严重的。问题——如果这算是个问题的话——源于将它们拼凑在一起，而拼凑它们非常简单。

在此，许多人用一句听起来很合理的借口来为自己辩护：“我没有什么可隐藏的”，或者“我很小心我的账号”。第一句话混淆了隐藏与选择；我们稍后再谈。第二句话忽略了一个事实，即这些痕迹中的大部分并不是你留下的：是商业登记处留下的，是遭受数据泄露的网站留下的，是那个上传了有你的照片并圈出你的熟人留下的。互联网上的匿名性几乎从来都不是你可以拥有的属性；充其量，它只是一种隐晦：一种暂时的状态，仅仅是因为还没有人费心去查看。

到目前为止，我们谈论的还是一个人手动在几秒钟内能做到的事。现在，把人去掉。多年来保护我们大多数人的不是匿名性，而是缺乏兴趣：要找到你，必须有人费心去看，而没有人有时间去看每个人。这最后一道屏障——去查看的精力——恰恰是机器所不需要的。自动化系统可以进行同样的交叉比对，而且不是针对单个目标，而是针对全部人口；不是一次，而是不知疲倦地进行；不是基于怀疑，而是默认进行。过去一个调查员在一个目标身上要花几小时的事，现在可以在不耗费任何人的时间或注意力的情况下，同时对数百万人进行。我们无需去猜测谁想这么做——一家公司、一个组织、一个国家——只需明白，现在已经不需要去选择要查看谁了。所有人都可以被查看。

这就是为什么“他们能找到我吗？”是一个错误的问题。答案是肯定的，而且这种情况会越来越普遍。真正有用的问题是另一个：为了在网络时代生活，我被迫要信任谁，以及信任多少？因为这正是你每天

都在做的事，几乎总是不假思索。你信任你注册的服务会妥善保管你的数据。你信任你的运营商不会窃听你的通话。你信任每个人都在使用的即时通讯应用——比如WhatsApp——它会履行其声称的承诺。你信任中间的服务器，信任管理它的公司，信任它所在的国家，信任某人在网上发布的免费工具。所有这些环节的每一个，都是一次信任的决定。不同之处在于，你几乎没有有意识地做出过这些决定：它们是打包附带的。这些潜入你和对方之间的环节，用行话来说，被称为受信任的中间人；叫什么名字并不重要，重要的是它们在那里，而且数量众多。

有一个诚实的方法可以验证这一切：用你自己来做实验。而且你不需要我们提供任何东西。打开你的浏览器，写下三四个字——比如“互联网知道我的邮箱什么信息”——网络本身就会把这些工具摆在你面前。这种轻而易举本身就是一半的答案：如果你能在十秒钟内找到它们，任何人也能找到它们关于你的说法。

我们没有为你提供我们自己的列表，这是有意为之的。如果我们给你，你就必须信任我们：信任我们挑选得好，信任这些页面在五年后仍然可靠，信任它们背后——无论是今天还是明天——都没有心怀恶意的人。对于我们无法控制的页面，我们无法做出这样的承诺，而且我们宁愿不去做出无法兑现的承诺。这恰恰是本文的主题。但是，你自己去寻找是有代价的：搜索引擎无法区分合法与陷阱。建立一个模仿真实工具、要求你提供邮箱并把它截留的网页是轻而易举的事。因此，在任何地方写下任何东西之前，最好先知道如何阅读网址。

注 —— 在信任它之前先看清网址。 一个假冒网页可以复制真实网页的每一个像素；但它几乎永远无法伪造的是它的网址。在任何网站上输入内容之前，请看地址栏，而不是网页本身。起决定作用的名字是紧挨着最后一部分左侧的那个（.com、.org、.cn）：在anquan-yinhang.qiguai-wangzhan.top中，真正的所有者不是你的银行，而是qiguai-wangzhan.top。对被篡改的字母（用0代替o）、多余的词、在意想不到的地方出现的连字符以及奇怪的后缀保持警惕。小锁图标和https只能说明连接是加密的——不能说明所有者是诚实的——骗子也有小锁。而那些被标记为“广告”的搜索结果排在前面，是因为有人付了钱，而不是因为它们值得信赖。所有的这些检查，本质上都是同一个问题：我对这个网址有多信任，为什么？

说到这里，有必要描述一下这一切的对立面：一个没有中间人的渠道。两个人，独自在山顶上交谈。中间没有邮递员，没有交换机，没有服务器，没有公司，也没有国家。然而，请注意：信任在那里也没有消失。如果你向另一个人吐露秘密，你就是在信任他。这种信任无法被移除——也没有必要——因为这是你唯一真正选择的信任：你知道你信任谁，以及为什么。

山上没有的，是所有其他的东西。中间没有任何人。而这，绝无仅有，是唯一可以在数字领域中诚实复制的模型：一条从一台设备到另一台设备的直接通道，途中没有任何事物或任何人。它并没有消除信任——那是撒谎——它消除了中间人。它让你只剩下那唯一不可避免的信任，那个你真正选择的信任。顺便说一句，这就是我们编写这些页面所基于的架构；但无论谁来构建，这个论点本身都是成立的。

所以不，你并不匿名，你可能再也不会匿名了。但那从来都不是一场重要的战役。人不可能在不信任任何人的情况下生活——或上网——；试图这样做的人并没有更自由，只是更孤独。成熟不是不信任，那是另一种形式的天真。成熟是变得苛求：知道你把信任交给了谁，交出了多少，换取了什么，以及——最重要的是——知道你何时在没有做出决定的情况下，就把信任交给了某人。

生活中几乎没有什么非黑即白；几乎所有事物都生活在中间的灰色地带，而学会在这片灰色地带中游走，很大程度上意味着拥有判断力。唯一的例外是那些出厂时就制作精良的东西：那些从设计上，就不要求你信任除了你已经决定与之交谈的人之外的任何人的东西。其余的——所有其他的一切——都是信任多少和信任谁的问题。

编者按： 当本 Cuadernos 提及公司或产品名称时，并非为了指责。这些产品的开发者所做的工作被数百万人使用和欣赏。我们指出的是结构性问题——是模式问题，而非品牌问题。品牌作为例子出现，是因为读者熟悉它们。

来源及延伸阅读

- OSINT（开源情报） —— 从已公开的数据中收集信息；它不是入侵或间谍活动。
- Reglamento (UE) 2016/679 (RGPD) —— 关于个人数据的处理，包括对单独公开的数据进行汇总。
- 公共记录（商业、司法、财产登记） —— 几乎全欧洲的合法且丰富的个人信息来源。
- 在同一系列中：关于端到端加密的笔记本和《一个签名无法解决的问题》从另一个角度拓展了同一个理念。

← 上一页签名无法解决的问题

最近阅读

- 思考 · 2026年5月27日 签名无法解决的问题
- 分析 · 2026年5月26日 真实隐私 vs 表象隐私：你应该问自己的问题
- 分析 · 2026年5月25日 作为专业实践的自托管 (Self-hosting)

随身携带本文，以备不时之需。

↓ Markdown ↓ 纯文本 ↓ PDF

文件将下载到您的设备中。您可以从那里将其保存、导入 Solo2 或在任何地方共享。Cuadernos 不会为您决定文件的去向。

火漆印章 · SHA-256 057792b5fd113d8a8bea5431cb78c5f3555a4bba7c18c90980b8338aec7ae884

Cuadernos Lacre · Menzuri Gestión S.L. 的出版物 ·
由 R.Eugenio 撰写 · 由 Solo2 团队编辑。