Do you Log?

Travis - 2022-01-07 - Frequently Asked Questions

Here at Private Internet Access, we do not log. Ever.

At Private Internet Access, privacy for the world and our users is at the soul of what we do and how we approach creating our application and working with other businesses. Our business partners have occasionally been surprised when we say up front that we want privacy first, business second – but that is just the passion we have. Making money is a matter of being able to continue pursuing the primary goal of privacy, on a sustainable basis.

Given this, we are sometimes asked: "Why we don't fly warrant canaries on our web page? Or "Why we don't have a short statement designed to technically circumvent gag orders about what, when, or where various authorities have legally coerced us to give up private information on our customers?"

A warrant canary can look like this:

> "In 2014, this company did not receive any coercing legal request for private customer information."

The idea is that if and when this statement disappears, it's the equivalent of saying authorities were grabbing what they wanted and are preventing the company from talking about it – so what the company does, to circumvent the gag, is to remove the statement so that it appears as if it never happened.

Doing this is going about the problem in the wrong way when you're a private company like we are. The right way is to not have any collectible information in the first place.

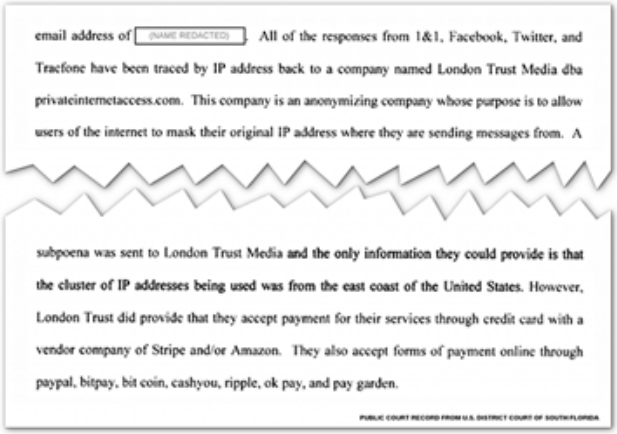
A warrant canary is a little bit like a fire alarm going off. Great. You know there's a fire. Now, what do you do?

This is why at Private Internet Access, we have designed our operations to prevent this from happening in the first place. There are no logs. No identifying information can be collected, regardless of the amount of force applied to us. Several companies have claimed that they do not log but do anyway at the end of the day. In contrast, we have public court records that state (under threat of perjury) we don't log anything, available for anyone to read (pages 11-12):

> "All of the responses from 1&1, Facebook, Twitter, and Tracfone have been

> traced back by IP address to ... privateinternetaccess.com. [...] A subpoena was sent [...] and the only information they could provide is that the cluster of IP addresses being used was from the east coast of the United States. However, [Private Internet Access] did provide that they accept payment for their services with a vendor company of Stripe and/or Amazon. They also accept forms of payment online through PayPal, Bitpay, Bitcoin, Cashyou, Ripple, Ok Pay, and Pay Garden."

The actual court record looks like this, with this passage divided across a page break:



email address of [NAME REDACTED]. All of the responses from 1&1, Facebook, Twitter, and Tracfone have been traced by IP address back to a company named London Trust Media dba privateinternetaccess.com. This company is an anonymizing company whose purpose is to allow users of the internet to mask their original IP address where they are sending messages from. A

subpoena was sent to London Trust Media **and the only information they could provide is that the cluster of IP addresses being used was from the east coast of the United States.** However, London Trust did provide that they accept payment for their services through credit card with a vendor company of Stripe and/or Amazon. They also accept forms of payment online through paypal, bitpay, bit coin, cashyou, ripple, ok pay, and pay garden.

PUBLIC COURT RECORD FROM U.S. DISTRICT COURT OF SOUTH FLORIDA

As you can see with this public court record, provides proof that there is nothing that can be logged from our application or servers that can identify our users. Now the question remains what to do if Private Internet Access is coerced into something – or rather, if authorities try to coerce Private Internet Access into something, such as was the case with Yahoo back in 2016, when the NSA had forced Yahoo into spying on its users.

There is a precedent for this, and it is Lavabit choosing to shut down operations instead of selling out its users (specifically, selling out Edward Snowden). That's also precisely what Private Internet Access has already done once, when Russia demanded that we start logging our users' identities, after seizing Private Internet Access servers.

Our response was to shut down operations in Russia immediately:

> The Russian Government has passed a new law that mandates that every provider must log all Russian internet traffic for up to a year [...] Upon learning of the above, we immediately discontinued our Russian gateways and will no longer be doing business in the region.

In summary, this is why Private Internet Access can demonstrate that we do not log. Ever.

For further questions, please feel free to contact support, here.