

[iPhone 15: What to Expect](#) [Keep Your Eyes in Top Shape](#) [CNET Coupons](#) [Best Satellite Internet Providers](#) [Gen AI and 3D Design](#) [Meal Delivery Services Rated](#) [Mortgage Rates](#) [Best Solar Con](#)



Your guide to a better future

#### Why You Can Trust CNET

Our expert, award-winning staff selects the products we cover and rigorously researches and tests our top picks. If you buy through our links, we may get a commission. [How we test VPNs](#)

[Tech](#) > [Services & Software](#)


# What is Kape Technologies? What you need to know about the parent company of CyberGhost VPN

Analysis: VPNs should be about enhancing privacy, but CyberGhost's parent company gives us trust issues.



**Rae Hodge**

Aug. 12, 2020 7:00 a.m. PT

8 min read 



CyberGhost

As a virtual private network reviewer, one of the hardest lessons I've learned is that no matter how clean a company's code, how skilled its development team, how many transparency gestures it offers users -- VPNs are still businesses based on asking us to trust what can't be seen. We typically engage a VPN service to better protect our online privacy, while understanding that all of our data -- every click, every site, every background app -- is being funneled to a single company, whose servers most of us will never see with our own eyes.

Because VPNs ask for so much trust, reputation can make or break a service. Similarly, when I'm examining a service's parent company and background, I'm looking for red flags around potential privacy concerns. That's what's got under my skin about CyberGhost when I recently gave it a fresh review.

**Read more:** [How we review VPNs](#)

In CNET's first evaluation on CyberGhost in 2019, we praised the

service for its roster of competitive features, but noted lackluster results in speed tests, some problems with its privacy tools and -- most importantly -- security verification that it failed due to its lack of obfuscation technology. Its low price made it worth considering if you needed to change the appearance of your location online, but not if you wanted best-in-class

Since then, CyberGhost has seen a significant performance boost following the addition of more than 2,000 servers to the company's fleet over the past year, beating Norton LifeLock's Secure VPN in our speed tests. Its Netflix, gaming and torrenting-focused and proprietary NoSpy servers appear to be attracting more praise than complaints, with good results in my own tests as well. And the service is prepared to roll out a new suite of privacy tools in the coming weeks, all while remaining one of the cheapest VPNs we've reviewed at \$2.75 per month for a 3-year plan.

I was initially thrilled about the company's privacy-friendly Romanian jurisdiction, located outside of US intelligence-sharing agreements, and its crack team of German developers, who seemed eager to address questions large and small about CyberGhost's history and vision. To top it off, some of the smartest tech enthusiasts I know have grown to love the service, joining the base of loyal CyberGhost's fans known as "ghosties."

Unfortunately, I can't at present recommend you join the ghostie brigade, and that's not entirely CyberGhost's fault.

Sure, CyberGhost gets my side-eye for the excessive amount of trackers on its website and app. And, yes, its ad-blocker is almost wholly impotent and uses an untrustworthy method of traffic manipulation no VPN should touch. And, naturally, I have beef with CyberGhost for still not having proper obfuscation -- meaning your internet service provider can see that you're using a VPN, which endangers people in countries where VPNs are outlawed.

But the real thing holding me back from recommending CyberGhost is the sordid history of its parent company, Kape Technologies.

**Read more:** CyberGhost VPN review: Improvements to this privacy product are promising, but their parent company concerns us

## Changing hands

For maximum privacy, I recommend VPN providers with a jurisdiction outside of Five Eyes and other international intelligence-sharing agreements -- that is, one headquartered outside of the US, UK, Australia, New Zealand and Canada. So it initially seems like a positive

sign that, while CyberGhost has offices in Germany, it's [headquartered in Romania](#). German entrepreneur Robert Knapp says he founded the \$114,000 startup on the back of [low-wage Bucharest labor](#) before flipping it for \$10.5 million in 2017.

The issue is who he sold it to -- the notorious creator of some pernicious data-huffing ad-ware, Crossrider. The UK-based company was cofounded by an [ex-Israeli surveillance agent](#) and a billionaire [previously convicted of insider trading](#) who was later named in the Panama Papers. It produced software which previously allowed third-party developers to hijack users' browsers via malware injection, redirect traffic to advertisers and slurp up private data.

Crossrider was so successful it ultimately drew the gaze of Google and UC Berkeley, which identified the company in a damning 2015 study. (You can read the [Web Archive version](#) of that document.)

This practice, commonly called traffic manipulation, is condemned web-wide. And the only difference between it and one of the oldest forms of cyberattack, called man-in-the-middle (MitM), is that you clicked "agree" on the terms and conditions.

In a blog post that CyberGhost has since removed from its site (available now at the Web Archive), CyberGhost CEO Robert Knapp even noted that "while CyberGhost focused on privacy and security from day one, Crossrider started out as a company that distributed browser extensions and developed ad tech products. Quite the opposite of what we did."

Crossrider changed its name to Kape Technologies PLC in 2018, in CEO Ido Erlichman's words, to escape the "strong association to the past activities of the company."

The name change supposedly accompanied a full turnaround for Kape, as it said it was exiting malicious adware and moving into cybersecurity. However, in the same year, Kape still operated the infamous scareware Reimage -- a potentially unwanted program that positions itself as a computer performance enhancer but which has been known to signal false positives on security threats in order to persuade you to pay for its premium service.

And new Crossrider-Kape mutations have been cropping up on the web as recently as August 2019, even as people are still jumping through hoops to [remove older Crossrider malware](#).

When I asked to CyberGhost CTO Tim Bavel, he was quick to

when I spoke to CyberGhost CEO Timo Beyer, he was quick to distance his company and technology from Crossrider's previous practices.

"CyberGhost was never involved in Crossrider's technologies," Beyer told CNET in June. "So I can tell you right now CyberGhost is working independently. We have, of course, the Kape Group which is, from a strategic perspective, holding CyberGhost, an independent entity. And we have our own goals and strategies, vision and also our culture."

After buying CyberGhost, Kape then bought VPN ZenMate in 2018 and more recently Private Internet Access, a US-based VPN, in a move which Erlichman said in a press release would allow Kape to "aggressively expand our footprint in North America."

## Terms of service

While CyberGhost may currently function as an entirely independent holding under Crossrider-turned-Kape, it's worth pointing out that as late as 2018, Crossrider was still listed in CyberGhost's terms and conditions.

"Crossrider may cooperate with public or private authorities at its sole discretion as provided by law," the document read. "(The company) may process and use personal data collected in the setup and delivery of service (connection data). This includes Customer identification and data regarding time and volume of use."

Asked about the terms and conditions in August of 2019, a CyberGhost spokesperson told CNET it would look into it but was unclear at the time on why Crossrider's name appeared in them.

More concerning than UK-based Crossrider's previous access to user data, however, is that CyberGhost's current terms and conditions (Web Archive version here) don't appear to disclose that the company is still owned by the same (renamed) company, Kape Technologies. CyberGhost's privacy policy does say that CyberGhost can share your data with its unnamed parent company.

"We may disclose your Personal Data to any member of our group of companies (this means our subsidiaries, our ultimate holding company and all its subsidiaries) insofar as reasonably necessary for the purposes set out in this Policy," the document says.

Furthermore, CyberGhost's current terms of service hold that any potential customer disputes will be handled in the UK.

potential customer disputes will be handled in the UK.

"In case of disputes arising from the terms of this Agreement, the Parties hereby irrevocably submit to the exclusive jurisdiction of London, UK," it says. The same clause is found in ZenMate's terms of service, which also fails to openly name Kape.

In an email, I asked CyberGhost why neither its privacy policy nor terms of service list UK-based Kape Technologies as the parent company (or ZenMate and Private Internet Access as its sibling companies) with which it reserves the right to share user information. When I asked whether CyberGhost is willing to update its terms and privacy policy in the interest of better disclosure and transparency, the spokesperson for the company said it would.

"Our parent company and sisters are public information, so users can easily become aware of the entities that may have access to their data. Notably, as far as our US entities are concerned, we do not share EU user data with them," a CyberGhost spokesperson told me. "We will clarify this in our next policy update."

CyberGhost also said that user information is not shared with Private Internet Access or any party outside the EU "other than as disclosed in the Privacy Policy" and that the clause in the company's privacy policy

that allows CyberGhost to disclose your personal data to its sibling companies "covers situations of employees working on cross-group projects."

I also asked why someone should bother choosing a VPN in Romanian jurisdiction outside of Five Eyes if potential legal disputes would be settled in UK courts, and their information may be shared with a UK-based parent company along with its German and US-based sibling companies.

"The choice of jurisdiction applies between the company and the user. When it comes to authorities' requests, we are a Romanian company, and as per Romanian law and our no-logs policy, we do not provide any information about our users," the company replied.

"English law was intentionally selected to protect both the users and our company because it is less invasive. For example, Romanian or German law impose statutory requirements additional or different from what the parties agree. Under English law, the priority is given to the terms agreed between the parties. Both parties know exactly what to expect, and there are no surprises. What's more, English law fully embraces GDPR, and therefore data protection is tantamount to that of all EU states."

Bottom line: Even a cautious interpretation of these clauses suggests that, although CyberGhost's business jurisdiction is in Romania, CyberGhost could share your data with not only its UK-based parent company, but with its US-based sibling company.

## More transparency needed

Ideally, the [VPN you choose](#) should also have undergone -- and published the results of -- an independent third-party audit of its operations, including its use of activity logs. While CyberGhost was given a surface-level comparison to its peers by [AV-Test](#) in 2019 (which received average marks), it doesn't appear to have undergone any independent audits since 2012. CyberGhost told [CNET](#) in 2019 that it plans to have its data [privacy practices](#) audited by an outside organization "in the future," but it didn't provide a timeline.

CyberGhost does publish its own yearly transparency report, which includes information on any subpoena requests it receives so people can more readily see whether the service has been subject to inquiries from law enforcement agencies. The company also provides quarterly [updates](#) on its site. But customers shouldn't have to rely on a company's own self-evaluation in matters of privacy and data-sharing.

It's not enough. I want audits -- not only of CyberGhost, but of any entity or business to which CyberGhost can potentially send my information.

I'm talking about more than a gesture of transparency. I'm talking about real evaluations of the uncertain data collection policies that dog both CyberGhost and its sibling companies. These are even more important given CyberGhost's history of being called to the carpet for [potentially dangerous data collection](#) when it was discovered that certain user hardware details were being logged.

I want to see the Ghosties proven right. But first, we all need more transparency and we all need answers about Kape before I can recommend its products.

**Update, Aug. 14:** Adds comment from CyberGhost.

First published on Aug. 12, 2020 7:00 a.m. PT

### CNET VPN Coverage

VPN USE CASES



- [Best VPN](#)
  - [Best iPhone VPN](#)
  - [Best Free VPN](#)
  - [Best Android VPN](#)
  - [Best Mac VPN](#)

VPN REVIEWS - OUR TOP PICKS

VPN REVIEWS - OTHER SERVICES

STREAMING WITH VPN

VPN EDUCATION
- [Best Mobile VPN](#)
  - [Best VPN for Windows](#)
  - [Fastest VPN](#)
  - [Best Cheap VPN](#)
  - [Best VPN Deals](#)

More From CNET

- [Deals](#)
- [Reviews](#)
- [Best Products](#)
- [Gift Guide](#)
- [Shopping Extension](#)
- [Videos](#)

About

- [About CNET](#)
- [Newsletters](#)
- [Sitemap](#)
- [Careers](#)

Policies

- [Cookie Settings](#)
- [Licensing](#)
- [Terms of Use](#)

- [Help Center](#)
- [Privacy Policy](#)
- [Do Not Sell or Share My Personal Information](#)

