Internet Access, Privacy ‘Essential for Freedom’: Proton Chief

Internet privacy company Proton can spot attacks on democracy in a country before they hit the headlines, simply by watching demand for its services explode, its chief told AFP.

When Russia blocked access to independent news sites following its invasion of Ukraine a year ago, the small company which provides virtual private networks (VPNs) saw “a 9,000 percent increase in sign-ups over just a period of a few days”, company chief executive Andy Yen said in an interview last week.

Switzerland-based Proton also saw a huge surge in demand for its VPNs, which are used to skirt online restrictions, in Iran last October as authorities cracked down harder on internet access amid flaring protests following Mahsa Amini’s death in custody.

“It was a factor of 10 at least,” Yen said.

Speaking at Proton’s headquarters outside Geneva, the 34-year-old particle physicist, who worked at Europe’s physics lab CERN before founding Proton in 2014, said the company had noticed that spikes in sign-ups “almost match… one-to-one” to places where democracy and freedom are under attack. “If there is a coup happening in Africa, we see it in our data before it makes the news.”

Severe consequences

Proton, perhaps best known for its encrypted email service,

sees its mission of ensuring privacy and online access as a vital tool in shoring up democracy in the digital age.

“Privacy is something that is essential for freedom,” said Yen. The Proton chief, who grew up in Taiwan and says the Chinese threat hanging over the democratic island colored his world view, acknowledged the company’s mission had taken on added urgency since Russia’s invasion of its neighbor.

“We all see in Ukraine how important it is to have digital technologies that protect privacy and give people freedom of information so they can see real news sources,” he said.

There, as inside Russia, in Iran and elsewhere, Yen insisted it was “essential” for companies like Proton to stay “even if there is a financial loss”.

“If we abandon these markets, actually the consequences are quite severe.”

Privacy in focus

Proton, which began nine years ago with 10,000 users crowd-funding 500,000 euros, today counts more than 70 million users worldwide. The company, Yen said, has pursued a fundamentally different business model than that of big tech companies like Google and Facebook, which offer “free” services in exchange for selling users’ data to advertisers.

“If you’re a Google user, you’re not Google’s actual customer. What you actually are is a product,” he said.

Influenced by former US National Security Agency (NSA) contractor Edward Snowden’s disclosures of mass digital spying by US government agencies, Yen said he had been even more concerned about “corporate surveillance, which was much more massive”.

“If you consider what the NSA might have on you, it’s probably only a drop in the bucket compared to what Google and Facebook

have.” Proton does offer free end-to-end encrypted email and VPN services, but instead of compensating by selling user data, it makes its money by selling monthly subscriptions for under $10 for extra features.

The company says its end-to-end encryption means that it has no access to the data transiting its servers and thus has no data to sell even if it wanted to.

It also means that it cannot turn over email content to governments that might demand it.

‘Cat and mouse’ – This, along with the VPNs helping skirt censorship, has put Proton’s team of around 400 employees in the crosshairs of powerful governments.

“We have had situations both in Russia and Iran where the entire resources of the state were thrown towards us,” Yen said, describing how the company has a team of engineers permanently on call to ensure its services “remain available and accessible”.

“It’s not rockets or missiles flying in the air, but there definitely is a fight for the future of the Russian internet, the Iranian internet and the internet in general.”

Yen recalled one sleepless Friday night in October when Proton’s VPNs came under a massive attack in Iran, and the nail-biting decision to roll out a new stealth VPN technology, aimed at making VPN traffic invisible to sensors.

The technology, which was developed to deal with issues in Russia, had yet to be tested on a large scale, and the engineers did not know for sure if it would hold up.

“We pulled the trigger, and it worked,” Yen said. “But it also could have gone the other way.”

In Iran, Russia and elsewhere, “it’s a cat and mouse game,” he said.

“I like to think that we’re a pretty fast mouse, but it’s also a pretty good cat sometimes.”

Related: ProtonMail Launches VPN Application for macOS

Internet Access, Privacy ‘Essential for Freedom’: Proton Chief