Protect your email the German way

After seeing off the police, Berlin email provider Posteo wants to expand user security and anonymity

Michael Scaturro
The Observer, Sunday 24 August 2014

Respecting your privacy: Posteo founders Patrik and Sabrina Löhr.

Last summer, German secure email provider Posteo faced a do-or-die moment: give in to police threats to seize its servers or fight back in court. Investigators in the state of Bavaria had contacted the Berlin-based startup because they wanted the identity of a Posteo account holder who was thought to be using the service for illicit purposes. But Patrik and Sabrina Löhr, the husband-and-wife team who run the swiftly growing email provider, told police time and again that they simply couldn't comply: Posteo is an anonymous email provider; it doesn't store any data on its customers' identities.

"We went around in circles with the authorities," Patrik Löhr says. "But when we looked at their search warrant, we saw that it didn't, in fact, give them permission to search our whole office. They were only allowed to receive a list of our bank transactions – which they already had gotten from the bank." Löhr filed a suit against police officials, accusing them of intimidation. That move, the media attention it generated, and a

stated commitment to transparency made all the more relevant in the wake of the Edward Snowden leaks, has helped Posteo become one of Germany's fastest growing email providers with a business model of fee-driven, privacy-oriented email services.

The immediate effect of Posteo's tangle with the German authorities was the pressure it put on global telecoms giant Deutsche Telekom. Just days after Posteo released Germany's first transparency report on government requests for information, Telekom dashed out its own paper detailing the extent of its cooperation with police and intelligence officials. The revelations were eye-opening. In 2013 alone, Telekom gave authorities in Germany nearly as much data on its customers as AT&T and Verizon had furnished that same year to US law enforcement.

This resulted in Germans ditching American email providers in Posteo's favour. "We went from 10,000 subscribers before the Snowden leaks a year ago to 70,000 today," Löhr says.

The site is currently only offered in German, though an English-language version is expected to be rolled out this autumn. It's not free: a 2GB account starts at €12 a year. But in exchange for that, Posteo promises users a private email experience. In fact, privacy is the company's unique selling point. Löhr says it doesn't deploy users' emails or contacts lists to serve up ads. It neither saves users' IP addresses nor tracks them as they click around the web. He says the company also deletes bank and card details immediately after it has processed payments. It even gives users the option of mailing or hand-delivering to the company's Berlin office payments in cash – around 20% of the service's customers have paid the annual fee in this way.

"We don't want the data from our customers," Löhr says. "We don't want their names, their addresses, their dates of birth. And because we don't have this data, we can't lose it or be compelled to give it away." He wants users to feel that Posteo is diametrically opposed to large, faceless email providers, that it adheres to an ethical standard that has become all the more topical since the NSA leaks last summer. But there's also the company's commitment to providing a personal touch. Löhr describes a situation – not unlike the early days of the internet, when people used local dial-up providers – in which "customers knock on our door and walk into our office to open an account".

But as friendly as the service claims to be, Posteo does resemble mainline email providers in a few key ways. For example, users' email is stored unencrypted on Posteo's servers in Frankfurt. The company states in its data protection policy that it has the ability to read any mail stored on its servers, much like its competitors. But it is working on a solution that will give users the option of encrypting their mailboxes using an open-

source system based on two-way encryption. Once this is rolled out, Posteo would not be able to read its users' mail. Posteo users can already encrypt their contacts lists this way. But there are drawbacks: users who forget their passwords are essentially locked out of their accounts. Once that happens, no one, not even Posteo's support team, can unencrypt the data. And here's another trade-off: encrypting mailbox content renders email searches impossible, thus disabling a key feature that many of us rely on daily.

While the company has had issues with reliability – on 15 June its site was offline for six hours after its server lost power– it defends its record on security. Indeed, the company has been a global leader in rolling out secure technologies. Last May, it became the world's first email provider to adopt DNS-based Authentication of Named Entities (Dane) on its servers. Dane makes it very difficult, if not impossible, for hackers or governments to launch man-in-the-middle "fishing" attacks on web browsers. According to the NSA documents leaked by Edward Snowden, Britain's GCHQ, for example, has launched such man-in-the-middle attacks using fake LinkedIn pages. "We protect your metadata with encryption and Dane," Löhr says. "But we are also encouraging our users to encrypt their email message with PGP."

PGP is a robust global encryption standard, but installing the software and registering for the requisite public encryption key can be a daunting process. Posteo's solution? It is opening a retail space in September, and will charge a flat fee for walk-in encryption tech support. It's a move that, for the Löhrs, is the next logical step in building a business around respect for its users' privacy. "We see it as part of our mission to help people understand encryption," Löhr says. "It's one of our business goals."