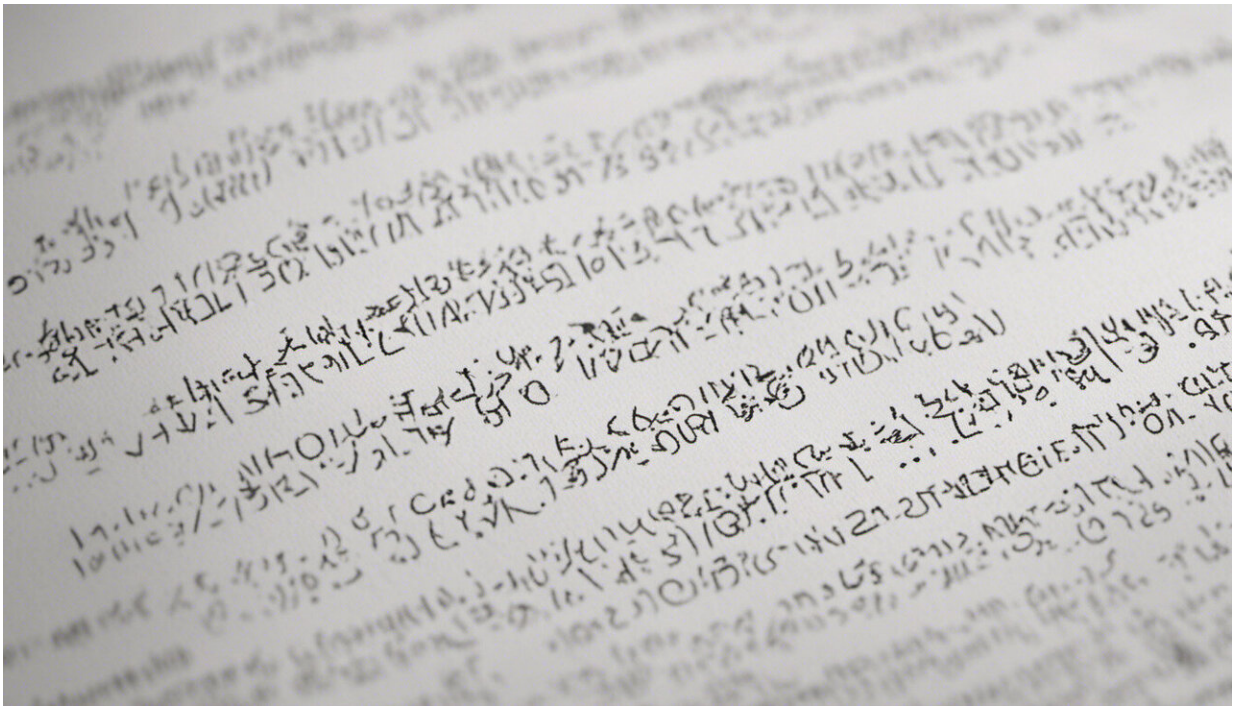
Worried your emails might be spied on? Here's what you can do

October 11 2016, by Monique Mann



Credit: AI-generated image (disclaimer)

We live in a post-Edward Snowden world, in which US tech companies have been accused of complicity in mass surveillance by the US National Security Agency (NSA). One recent allegation is the claim that Yahoo scanned hundreds of millions of emails at the NSA's request.

We don't truly know how much or how often this is happening within the companies that host millions of people's email accounts.

According to Reuters, Yahoo was ordered by the secret US Foreign Intelligence Surveillance Court (FISC) to scour emails for a specific string of characters. This is significant, as it required Yahoo to create a custom-built program for real-time surveillance of email traffic.

The power for this type of surveillance was expanded by the US Patriot Act, which allows for the use of secret National Security Letters (NSL) to compel service providers to hand over customer data. The letters come with gag orders, prohibiting companies like Yahoo from even admitting that they have been ordered to monitor customers.

But email scanning does not only occur at the behest of national security agencies. The past decade has seen the rise of "surveillance capitalism" and "data brokers", who collect your information for behavioural profiling and targeted advertising.

Google has admitted to scanning emails to deliver targeted advertising and customised search results. Facebook is currently facing legal action for scanning private messages to do the same. And earlier this year Yahoo itself settled a class action lawsuit for scanning non-Yahoo customer emails without consent.

Protecting your privacy

So with all this going on, is it possible to protect your privacy? And if so, how?

One way is through encryption, which allows only the sender and the receiver to read the content of messages, as it converts information into a secret code that requires a key to decode it.

Public-key cryptography is one type of encryption, involving two paired keys – one public and one private. When an encrypted email is sent it is encoded or "locked" with the receiver's public key. Only the receiver can "unlock" it with their private key.

End-to-end encryption involves encrypting information before it leaves your device, with it only being decrypted once it reaches the receiver's device. In other words, it is encrypted "at the ends" where the keys are held. This means that security and privacy are not dependent on the channel of communication – in this case the email provider – because if the message is intercepted it cannot be deciphered. This prevents eavesdropping in transit.

There are now numerous services that promise free end-to-end encrypted communication, including ProtonMail, Tutanota, and the messaging app Signal. Look for those with open source code because it enables peer-review, guaranteeing there are no backdoors.

The push-back against encryption

With increased encryption comes more demands from authorities for companies to "unlock" information. The best example may be the Apple-FBI case, which saw the FBI attempt to compel Apple to unlock a suspect's iPhone. In the end this wasn't necessary. There has also been a simultaneous rise in companies like Cellebrite who offer digital forensic services to decrypt and extract data.

Therefore, the best services use principles of privacy by design, that limit how much information the service provider themselves can collect or access. ProtonMail and Signal, for example, cannot access their users' information, no matter how hard they try. If issued with a subpoena all they could provide is the date and time a user registered and the last date of connection.

Partly as a result of this encryption war, some states are considering outlawing encryption entirely. Criminalising encryption has been discussed in the United States, Britain, Australia, and elsewhere.

Tech companies safeguarding secrecy

But not all hope is lost. There is a growing trend of tech companies fighting back and refusing to comply with surveillance orders.

In 2014 Lavabit chose to shut down rather than turn over the private encryption key to a customer's account. This customer was later revealed to be Edward Snowden. Microsoft has refused to hand over emails stored on its servers in Ireland, arguing that this would constitute an impermissible extraterritorial search by the FBI. And of course, Apple refused to disable inbuilt security features to crack an encrypted iPhone.

This shows that service providers are aware of the importance of developing and maintaining consumer trust in matters of privacy. They are intimately, and commercially, invested in protecting it.

Transparency reports and warrant canaries

Another way companies have attempted to gain trust is through transparency reports that detail the orders they have received from authorities. These can be found on company websites and are often reported in the media. Many of these reports feature a workaround to the restrictions on letting customers know if surveillance has been ordered. Companies simply include a statement that they have *not* been subject to a secret order. If this statement ever goes missing, customers know an order has been issued. This is known as a "warrant canary".

Several companies routinely issue transparency reports with warrant

canaries. Apple and Reddit have set them off, implying that they have received secret orders to provide data.

The same workaround may not be available in Australia however. Recent data-retention laws introduced journalist information warrants that made it an offence to disclose information about the existence (or *non-existence*) of the warrant, effectively outlawing warrant canaries for journalists in Australia.

The future

Encryption and transparency reports are some of the last protections that consumers have against both governments and the big tech companies we rely on. As more of our lives transition online, we will need them to protect civil rights and individual privacy. We can't afford for either to be weakened or outlawed.

There are a couple of challenges under way. NSL statutes and gag orders are currently being challenged by the Electronic Frontier Foundation and members of the US Congress as unconstitutional. Watch this space.

This article was originally published on The Conversation. *Read the* original article.

Source: The Conversation