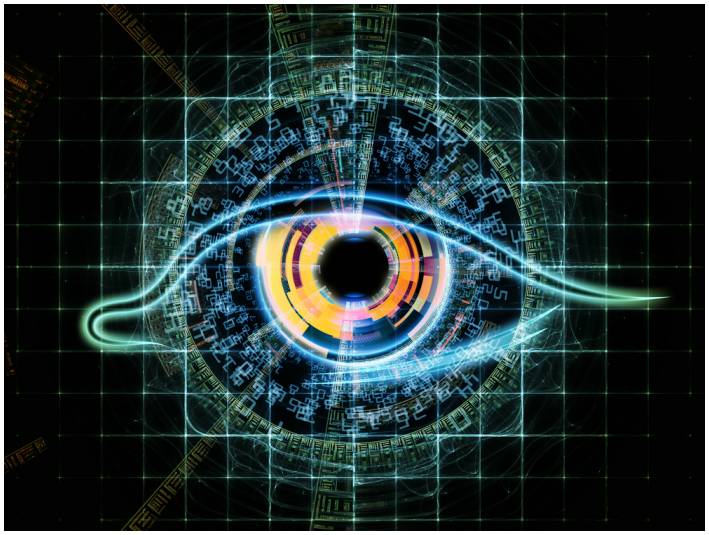
Signal Disclosed User Data To US Government

Open Whisper Systems (OWS), the company that develops the security-oriented Signal communications application and protocol, has disclosed it handed over data on a user to the US federal government earlier this year, the first time it said it has been asked to do so.

But because the company keeps few records on its users and doesn't have access to their encrypted communications, the only information it was able to provide were the date and time the account was created and when it last connected to Signal's servers, the company said.



User data

OWS' Signal Protocol is used by its own application and by third-party tools including Facebook Messenger, WhatsApp and Google Allo.

Those companies, however, retain more user data on their servers – Facebook subsidiary WhatsApp, for instance, keeps encrypted messages backed up on its servers so they can be restored when a user sets up a new device.

Signal made the disclosure as part of a case brought by the American Civil Liberties Union (ACLU), which it hired to challenge a gag order initially placed on the case, which would have kept Signal from making the demand public for a year.

The ACLU said the US government quickly agreed the gag order was excessive and allowed the publication of some of the case's details.

The case originated with a federal grand jury proceeding in the Eastern District of Virginia, and OWS was subpoenaed to provide a wide range of details on user accounts connected with two telephone numbers. One of the numbers wasn't associated with any Signal account, OWS said.

The ACLU argued the case indicates that the government routinely places gag orders on its demands for information, meaning there are necessarily many that haven't been disclosed.

“While this (demand) – the only one ever received by OWS – is now public, there are many more like it, hiding in the filing cabinets in the U.S. attorney’s offices across the country,”
wrote ACLU attorney Brett Max Kaufman in a blog post.

Privacy concern

Privacy advocates have said most companies’ practices of holding user data means that data is susceptible to being disclosed to government authorities on demand – and could also be vulnerable to hacking, even if it is encrypted.

“The FBI came after #Signal, only to find they log only account creation date & last login time. @Google, take note,” wrote privacy advocate Edward Snowden in a Twitter post.

The US government has maintained that its collection of communications records is necessary to uphold the law and to further the country’s interests, while campaigners argue the practices go too far.

In the latest incident to fan surveillance controversy, a report on Tuesday claimed Yahoo secretly scanned all customer’s emails for US intelligence services using a real-time surveillance software system it built specifically for the task last year.

The company searched emails for a certain set of characters, either in the body of an email or its attachment, as they arrived into customer accounts, the report said, citing former Yahoo employees.

***Quiz:** What do you know about cybersecurity in 2016?*