theguardian | TheObserver

Skype under investigation in Luxembourg over link to NSA

Ten years ago, the calling service had a reputation as a tool for evading surveillance but now it is under scrutiny for covertly passing data to government agencies

Ryan Gallagher
theguardian.com, Friday 11 October 2013 06.30 EDT

Skype is being investigated by Luxembourg's data protection commissioner over concerns about its secret involvement with the US National Security Agency (NSA) spy programme Prism, the Guardian has learned.

The Microsoft-owned internet chat company could potentially face criminal and administrative sanctions, including a ban on passing users' communications covertly to the US signals intelliigence agency.

Skype itself is headquartered in the European country, and could also be fined if an investigation concludes that the data sharing is found in violation of the country's data-protection laws.

The Guardian understands that Luxembourg's data-protection commissioner initiated a probe into Skype's privacy policies following revelations in June about its ties to the NSA.

The country's data-protection chief, Gerard Lommel, declined to comment for this story, citing an ongoing investigation. Microsoft also declined to comment on the issue.

Luxembourg has attracted several large corporations, including Amazon and Netflix, due to its tax structure.

Its constitution enshrines the right to privacy and states that secrecy of correspondence is inviolable unless the law provides otherwise. Surveillance of communications in Luxembourg can only occur with judicial approval or by authorisation of a tribunal selected by the prime minister.

However, it is unclear whether Skype's transfer of communications to the NSA have been sanctioned by Luxembourg through a secret legal assistance or data transfer agreement that would not be known to the data protection commissioner at the start of their inquiry.

Microsoft's acquisition of Skype tripled some types of data flow to the NSA, according to top-secret documents seen by the Guardian.

Microsoft bought Skype for $8.5bn (£5.6bn) in 2011.

The US software giant was the first technology group to be brought within the NSA initative known as Prism, a scheme involving some of the internet's biggest consumer companies passing data on targeted users to the US under secret court orders.

Having once been considered a secure chat tool beyond the reach of government eavesdropping, Skype is now facing a backlash in the wake of the Prism revelations.

"The only people who lose are users," says Eric King, head of research at human rights group Privacy International. "Skype promoted itself as a fantastic tool for secure communications around the world, but quickly caved to government pressure and can no longer be trusted to protect user privacy."

Skype's legacy of encryption and security

Founded in Scandinavia in 2003, Skype was designed to connect callers through an encrypted peer-to-peer internet connection, meaning audio conversations between Skype users are not routed over a centralised network like conventional phone calls. Video and chat connections are also encrypted.

Attracting millions of users worldwide – 12.9 million people had registered to use the service by 2004, and by 2011 that figure had reached more than 600 million – Skype's reputation for privacy and security led to it being adopted by journalists and activists as a tool to evade government surveillance. But some criminals, too, turned to the tool to dodge law enforcement agencies – frustrating police, who had previously been able to eavesdrop on suspects' conversations by 'wiretapping' phone lines.

A turning point came in 2005, when US company eBay purchased Skype for $2.6bn (£1.6bn). The same year, Skype formed a joint venture with Hong Kong-based internet company Tom Online to launch a Chinese version of Skype, which was tweaked to be compliant with dragnet surveillance.

Skype China customised for monitoring

A former Skype engineer, who declined to be named because of the sensitive nature of the issue, told the Guardian that the company worked to build in a "listening element" to help Chinese authorities monitor users' communications for keywords, triggering a warning to alert the government when certain phrases get typed into its chat interface.

In response to questions about suspected monitoring of Skype chats in China, Skype has previously stated that its software is made available in the country "through a joint venture with Tom Online. As majority partner in the joint venture, Tom has established procedures to meet its obligations under local laws."

While publicly insisting it was unable to help law enforcement agencies eavesdrop on calls, Skype set up a secretive internal initiative called "Project Chess" to explore how it could make calls available to authorities, according to a New York Times report published in June.

A year later, Skype was purchased from eBay by an investor group including US private equity firms Silver Lake and Andreessen Horowitz. During this period, work began on integrating Skype into the NSA's Prism program, documents leaked by NSA whistleblower Edward Snowden have revealed.

The first 'eavesdropped' Skype call

In February 2011, according to the NSA files, Skype was served with a directive to comply with NSA surveillance signed by the US attorney general. Within days, the spy agency reported that it had successfully eavesdropped on a Skype call. And when Microsoft acquired Skype in May 2011, the relationship with the NSA appears to have intensified.

Caspar Bowden, who served as Microsoft's chief privacy adviser between 2002 and 2011 and left shortly before the completion of its Skype takeover, says he was not surprised to learn the company had complied with the NSA's surveillance of the chat tool.

While working for Microsoft, Bowden says he was not privy to details of secret data-collection programs – but fully briefed the company on the dangers of US spy law the Foreign Intelligence Surveillance Act (FISA) for the privacy of its international cloud customers. He was met with a "wall of silence," he says.

A letter obtained by the Guardian, sent by Skype's corporate vice president Mark Gillett to Privacy International in September 2012, suggested that group video calls and instant messages could be obtained by law enforcement because they are routed through its central servers and "may be temporarily stored."

But Gillett also said in the letter that audio and one-to-one video calls made using Skype's "full client" on computers were encrypted and did not pass through central servers – implying that the company could not help authorities intercept them.

Separately, in July 2012, Skype contributed to UK parliamentary committee hearings on the government's proposed expansion of surveillance powers under the controversial communications data bill. Skype representative Stephen Collins claimed in testimony to the committee that "there are no keys held by Skype to decrypt communications."

Microsoft calls for more government transparency

Skype told the Guardian that it would not answer technical questions about how it turns over calls to the authorities or comment on the extent of its compliance with US surveillance. The company insisted the information it provided the UK parliament was accurate, though would not explain apparent discrepancies between its public statements and access to Skype calls claimed by the NSA.

In a statement, Skype said it believed that the world needed "a more open and public discussion" about the balance between privacy and security but accused the US government of stifling the conversation.

"Microsoft believes the US constitution guarantees our freedom to share more information with the public, yet the government is stopping us," a spokesperson for Skype said, referring to an ongoing legal case in which Microsoft is seeking permission to disclose more information about the number of surveillance requests it receives.

However, the law that underpins the Prism program – FISA – allows the NSA to target not only suspected terrorists and spies, but also "foreign-based political organisations," which could encompass an array of advocacy groups and potentially news organisations, too.

'Journalists should avoid Skype'

Grégoire Pouget, an information security expert at Reporters Without Borders, believes that journalists should not underestimate the risks posed by NSA Skype surveillance.

"It is what many of us feared, and now we know for sure," Pouget says. "If you are a journalist working on issues that could interest the US government or some of their allies, you should not use Skype."

Although the NSA has access to at least some Skype calls, it remains unclear whether police and security agencies outside the US enjoy a similar level of access.

Hacking Team, an Italian company, sells surveillance software to law enforcement and intelligence agencies in 30 countries that allows authorities to covertly infiltrate computers with spyware that records communications before they are encrypted. The Milan-based firm explicitly markets the Trojan tool as a means to get access to Skype conversations – and says authorities still frequently complain about a lack of ability to eavesdrop on Skype calls.

"When you talk to law enforcement about what their concerns are, they'll right away mention Skype," says Eric Rabe, Hacking Team's spokesman.

Rabe declines to name customers, citing confidentiality agreements, but says Hacking Team's business has been "growing very nicely" in recent years. The company's public accounts show that its revenue more than doubled from $5.3m in 2010 to a projected $11.8m in 2012.

The new wave of encrypted services

At the opposite end of the spectrum, new companies are now emerging in response to fears about surveillance of Skype, promising users access to encrypted chat tools that do not have secret 'backdoors' for NSA surveillance.

Washington DC-based Silent Circle is one such company, going to extraordinary lengths to shield customers against spying. With founders including Phil Zimmermann, who devised the Pretty Good Privacy (PGP) email encryption product, and a former Navy Seal, Silent Circle offers a series of encrypted phone apps and a Skype-style internet chat platform.

It is registered as an offshore company and uses computer servers outside the US in a bid to evade government coercion. It recently closed its own encrypted email service because it could not guarantee security, and said it would focus instead on chat and telephony.

The FBI has already held meetings with Silent Circle, according to CEO Mike Janke, accusing it of being a "ghost provider" that could cause harm to the US because it stores virtually no information about its users' communications.

But Janke, a 45-year-old former Navy Seal sniper, says his company will not cede to government pressure to secretly comply with surveillance. "I feel that we can use Skype as a template," Janke says, "for what we don't want to do."