MIT Technology Review

Microsoft's Surveillance Collaboration: Voluntary Aid, or New Legal Tactic?

Microsoft redesigned its systems to aid U.S. surveillance programs, but whether it did so voluntarily or under duress is unknown.

By: Tom Simonite – July 12, 2013

In July of last year, Microsoft began publicly testing an online e-mail and chat service called Outlook.com. Soon afterward, according to the British newspaper the *Guardian*, the company reëngineered it in a way that allowed the National Security Agency's PRISM surveillance program collect chat data before it was encrypted.

Privacy campaigners and surveillance experts are now pondering whether Microsoft's actions were forced by a previously unknown legal tactic, or whether the company voluntarily made the changes to aid surveillance. The *Guardian* report marks the first time that a major Internet company has been described to have modified its systems to enable government surveillance, as opposed to simply providing access to data it already held.

"The $1 million question is whether Microsoft was forced to reëngineer its systems to include new surveillance capabilities, or whether it did so voluntarily," says Christopher Soghoian, principal technologist and senior policy analyst with the Speech, Privacy and Technology Project of the American Civil Liberties Union.

A Microsoft statement released Thursday said that "we provide customer data only in response to legal processes." Soghoian believes that Microsoft could have enabled the interception of communications but then only allowed those capabilities to be used when presented with a court order.

The *Guardian*'s report says that in addition to modifying how Outlook.com functioned, Microsoft worked with the FBI to enable access to data in its cloud storage system, SkyDrive, and to increase the government's access to calls over Skype, which Microsoft owns. The FBI acts as an intermediary between intelligence agencies, including the NSA, and Internet companies. The changes made by Microsoft were part of an NSA program called PRISM that also collects data from Facebook, Google, Yahoo, and Apple. Data from PRISM is passed from the NSA to the FBI and CIA.

In its statement Thursday, Microsoft hinted that some of its actions were made under legal duress. It said that "when we upgrade or update products legal obligations may in some circumstances require that we maintain the ability to provide information in response to a law enforcement or national security request."

Federal law seems to protect companies from being required to enable surveillance access, says Jennifer Granick, a lawyer and director of civil liberties at Stanford University's Center for

Internet and Society. The part of the Electronic Communications Privacy Act governing wiretapping-style access to online communications makes provisions only for court orders that compel installation and use of surveillance devices, says Granick. “That seems to me to say they can install equipment on the system. But they can’t force system design.”

However, if Microsoft chose to object to NSA and FBI requests for data its fate would be decided by the Foreign Intelligence Surveillance Court (FISC), which last month was shown to have been using interpretations of existing laws that surprised some scholars of surveillance law (see “NSA Surveillance Reflects a Broader Interpretation of the Patriot Act”). The court handles requests for warrants made using the Foreign Intelligence Surveillance Act and allows collection of a person’s data, including his communications with others, if there is a “51 percent” likelihood that the person in question is not a U.S. citizen and is outside the United States.

Julian Sanchez, a research fellow at the Cato Institute, a nonpartisan think tank, believes the FISC might now see the law in a way that allows the government to compel changes—at certain times—to computer systems to aid surveillance. “One never knows with a secret court, but it seems extremely unlikely the FISC would order a company to fundamentally redesign their software or network architecture to enable interception,” he says. “It is certainly possible, however, that if Microsoft was independently engaged in a redesign, they could be ordered to do it in a way that enabled compliance with a surveillance order, within limits.”