Microsoft Steps In Privacy Quagmire With Email Snooping

Share us on: By **Allison Grande**

Law360, New York (March 21, 2014, 8:56 PM ET) -- While Microsoft Corp. will likely dodge criminal charges for sifting through the email of a user who allegedly received trade secrets from a former employee, the company will have a harder time quelling backlash from users irate over policy terms the company claims give it license to read their personal communications, attorneys say.
Microsoft has faced a barrage of criticism since federal prosecutors **filed a criminal complaint** Monday against former employee Alex A. Kibkalo that revealed the company had snooped on the Hotmail account of the blogger to whom Kibkalo is accused of leaking proprietary information.

In a statement Thursday, Microsoft deputy general counsel John Frank **sought to quell the backlash** by assuring users that the company had taken "extraordinary actions based on the specific circumstances." Frank maintained that Microsoft's actions fell within the bounds of the law and its own policies, which allow it to access user data to "protect the rights or property" of the company.

The terms are likely to help the company stave off litigation, but they won't provide much comfort to users left skeptical by recent high-profile security breaches and accusations that service providers are **providing the National Security Agency** blanket access to users' communications, attorneys say.

"Regardless of what the terms of service say, looking at emails really seems to infringe on what users' reasonable expectation of privacy is," Fox Rothschild LLP privacy and data security practice leader Scott Vernick told Law360. "When users sign up for an account, they don't expect that the service provider is reading their emails. It's like saying the postal service has the right to open my mail."

Microsoft also announced Thursday that it planned to add protections for customers to its policies for accessing user email accounts and other data.

Currently, Microsoft limits its searches to circumstances that would warrant the issuing of a court order, claiming it doesn't actually need to obtain an order because it is searching content on its own service. According to Frank, it relies on legal counsel separate from the investigation to determine if that criterion has been met.

Under the planned changes, Microsoft will take the extra step of submitting evidence of a potential crime to an outside lawyer who is a former federal judge to help it make that determination, Frank said. The company will also publish information about the number of these searches and the number of customer accounts affected in its biannual transparency report, alongside data on searches in response to law enforcement requests, according to Frank.

But attorneys doubt the vow to restrict access to a small batch of internal investigations will be construed as narrowly as promised.

"We'll have to see the final policy revisions, but I would not think Microsoft is intending to so drastically restrict the available reasons for accessing data," said Torin A. Dorros, the managing attorney of Los Angeles-based boutique firm Dorros Law. "Rather, I would think the move is really to add the additional layer of procedural protection for itself and its users."

The foundation for Microsoft's current predicament was laid in 2012, when the company received a tip from an anonymous source who had been contacted by a French blogger who wanted guidance on proprietary code the blogger had acquired for a program meant for internal Microsoft use only.

Upon examining the blogger's email account, Microsoft's Office of Legal Compliance stumbled upon messages from Kibkalo, who was stationed in Lebanon at the time, indicating he had leaked the information, as well as a series of updates to Microsoft's Windows 8 software suite, which had not been publicly released at that time.

Although attorneys say Microsoft's actions make sense given the importance of the confidential business information at issue and the time it would have taken to get court permission for the search, they doubt users will view them so generously.

"If trade secrets get out, there's no way to put the genie back in the bottle," Mintz Levin Cohn Ferris Glovsky & Popeo PC member Donald Schroeder said. "But the countervailing fact is that people might not want the company's products if they feel like Big Brother is watching."

Microsoft is likely to face scrutiny from federal prosecutors, as well as from the blogger whose data was accessed, who might question whether the company's conduct violated eavesdropping statutes such as the

Computer Fraud and Abuse Act or the Stored Communications Act.

The CFAA prohibits unauthorized access to protected electronic communications, while the Stored Communications Act requires a warrant based on probable cause for emails that have been in storage for less than 180 days.

But Microsoft will probably avoid criminal charges based on its arguments that users agreed to policy terms that gave the company permission to access their data for investigatory purposes and that it does not need legal process to access their own users' accounts, attorneys say.

"It's hard to imagine that they will face criminal liability given the circumstances surrounding their motivation for doing it, why they did it, the lack of harm to the victim, and the fact that they were trying to get back their own valuable code," said Weisbrod Matteis & Copley PLLC partner and former federal prosecutor Peter Toren.

While a civil suit filed by the blogger is more likely, those claims would also face an uphill battle, according to attorneys.

"Microsoft didn't do it on an ad hoc basis. They went in and presumably were trying to assure that their trade secrets were secure, and the blogger had the information wrongly in the first place," Schroeder said.

Regardless of how the controversy plays out for Microsoft, the situation should serve as a note of caution for companies that are increasingly facing both internal and external threats to their confidential and valuable business data, according to attorneys.

"The lesson to be learned here is that companies need to consider whether they believe the benefits of engaging in self-help remedies are worth the legal and public relations risks involved," Toren said.

--Additional reporting by Lance Duroni and Alex Lawson. Editing by Kat Laskowski and Philip Shea.

Related Articles

- Microsoft Adjusts Policies After Email Snooping Outcry
- Ex-Microsoft Employee Pleads Guilty To Trade Secret Theft
- Microsoft Warrant Ruling Puts Service Providers In Bind
- Feds Question Stay In Microsoft Overseas Data Warrant Case
- Microsoft May Feel Privacy Heat Despite Xbox Backtracking

View comments

- Printable Version
- Rights/Reprints
- Editorial Contacts

Related

Sections

- Employment
- Intellectual Property
- Privacy
- Technology

Law Firms

- Fox Rothschild
- Mintz Levin
- Weisbrod Matteis

Companies

- Microsoft Corporation

Government Agencies

- National Security Agency