# Yahoo's Reported NSA Assist To Complicate Privacy Shield

By Allison Grande
Law360, New York (October 7, 2016, 4:07 PM EDT) -- Recent reports that Yahoo secretly scanned all of its users' email accounts at the request of U.S. intelligence officials not only ramps up the already simmering tensions between federal investigators and domestic service providers, but also spells trouble for the already fragile trans-Atlantic Privacy Shield data transfer agreement.

Less than two weeks after Yahoo Inc. grabbed headlines by disclosing that a 2014 hack had compromised user data linked to at least 500 million accounts, the company took another hit when Reuters, citing anonymous sources, reported on Tuesday that Yahoo had secretly built a custom software program last year to search all of its customers' incoming emails for specific information provided by U.S. intelligence officials after receiving a classified request from the National Security Agency or the FBI.

Yahoo — whose core business Verizon Wireless Inc. agreed in July to scoop up for $4.83 billion — quickly hit back at the report, calling it "misleading" and asserting that the company "narrowly interpret[s] every government request for user data to minimize disclosure" and that "the mail scanning described in the article does not exist on [its] systems."

But despite the rebuttal — which experts pointed out fell short of being a flat-out denial of the accusations — Yahoo is likely to face heat from both its customers in the U.S. and regulators abroad, a reaction that highlights the increasingly complicated line that service providers need to navigate between law enforcement's need to access user data and their users' privacy expectations.

"The report shows us once again that this is a very difficult road to hoe in responding to court orders while trying to meet user expectations about privacy," Ballard Spahr LLP partner and former federal prosecutor Edward McAndrew said. "Requests from the government are getting more creative and perhaps more invasive, and this is just the latest iteration over the battle of how far third parties have to go in assisting law enforcement."

Officials in the U.S. and EU hammered out the Privacy Shield data transfer deal earlier this year to replace the long-standing and popular safe harbor pact that was struck down by the EU Court of Justice last October on the grounds that it hurt EU citizens' privacy rights because U.S. intelligence officials were being given unfettered access to their personal data.

A similar challenge to the Privacy Shield deal is expected to be brought in the near future, and Tuesday's disclosure about Yahoo's email scanning program is likely to add

additional fuel to the fire and give opponents of the revamped pact additional ammunition to contest the arrangement.

"Whatever the odds were that we were going to see a challenge to the Privacy Shield, those odds just went up," Dorsey & Whitney LLP partner and former federal prosecutor Robert Cattanach said.

The tightrope that service providers must walk when it comes to government access demands was most recently brought to the public stage earlier this year, when Apple waged a high-profile bicoastal battle with the government over the FBI's demand that the tech giant help it unlock phones belonging to a deceased mass shooting suspect in San Bernardino, California, and a confessed drug dealer in New York. The government ultimately dropped both fights after finding ways to break into the devices without Apple's help.

Microsoft has also pushed back at federal officials' ability to access user data, mounting a successful challenge to the government's use of search warrants to access email content data stored overseas and launching a new challenge in April to the government's ability to use gag orders to force service providers to keep customers in the dark about law enforcement demands to access user data, which received a groundswell of support from the tech, media, privacy and law enforcement communities.

In the wake of the Reuters report, Yahoo has caught flack for both the purported broad scope of its scanning practices — which experts say as described goes well beyond the usual practice of targeting certain accounts or keywords, and which companies like Apple have said they would never consider going along with — as well as its apparent decision not to fight the surveillance order, which most likely received approval from the secret Foreign Intelligence Surveillance Court.

"This is a gray area," Cattanach said. "The greater the potential risk, the greater the pressure placed on the tech company is, and it's easy to second-guess them. But at some point, any tech company is going to feel the tug of its corporate citizenship and not just turn a cold shoulder to compelling requests from the government."

Experts additionally noted that Yahoo has fought back at demands in the past, most notably in an unsuccessful challenge to the government's request to access its customer data as part of the PRISM surveillance program, a dispute that was rejected by the secret FISA court in 2008.

"Yahoo did their best to fight in the past and lost, so it's hard to fault the company for making the business and legal decision to take a different tact this time," said Bradley S. Shear, managing partner of Shear Law LLC.

However, these considerations are likely to do little to quell concerns not only with Yahoo's users, but also from overseas.

"The report has the potential to have a significant international impact, and to be another bit of bad news for advocates of the Privacy Shield agreement," McAndrew said.

The Yahoo report is likely to play a significant role in how regulators view the program, which more than 700 companies, including Google and Microsoft, have committed to using. Yahoo is yet to be listed among the companies that have signed up with the U.S. Department of Commerce to transfer data pursuant to Privacy Shield.

The collection of EU data protection authorities known as the Article 29 Working Party said in May that they would refrain from bringing any challenges to the pact for at least a year, when they would undertake a comprehensive review of the program.

"I'm absolutely certain that European data protection authorities will want the report to be part of their annual review process, and so Yahoo's response to this will be really important," said Paul Hastings LLP partner Ashley Winton, who is based in London.

At least one data protection regulator has already taken an interest in Yahoo's reported email scanning tactics.

The Irish data protection commissioner confirmed in a statement provided to Law360 that it is looking into the report, noting that "any form of mass surveillance infringing on the fundamental privacy rights of EU citizens would be viewed as a matter of considerable concern by this office."

"In Europe, they are very concerned about mass, indiscriminate interception, and that would likely be a focus of regulators' investigation," Winton said. "Certainly, complying with a lawful warrant in the U.S. can infringe European data protection and privacy laws."

In the U.S., the legal and regulatory fallout is likely to be minimal, especially if it's confirmed that a court had signed off on the scanning order and Yahoo had lawfully followed that directive.

While regulators like the Federal Trade Commission may have questions about what Yahoo promised their users about how their data would be shared with government officials and if their practices lived up to these privacy promises, the brunt of the fallout at least domestically is likely to be tied to the company's already damaged reputation, attorneys say.

"If you're responding to a lawful order, that's one thing, but just because you're dotting

your i's and crossing your t's legally, that doesn't mean its not going to impact your reputation," Shear said.

Yahoo has already been brought to task over its commercial email scanning practices, with consumers filing a putative class action over the practice in California federal court that the company in January agreed to settle by promising to make policy changes such as halting its scanning of emails for advertising purposes before users have a chance to read them.

And the service provider is still very much reeling from the disclosure of its massive data breach last month, which has already led to a flood of class actions, regulatory probes and concerns over the health of Verizon's proposed acquisition of the company.

The planned deal is likely to be dealt a further blow by the email scanning report, with the New York Post reporting Thursday that, according to anonymous sources, Verizon is pressing for a $1 billion discount off its pending agreement to buy Yahoo.

"Now the question becomes did Verizon know about this issue before it put in its bid, and if it did know about it, that could lead people to start questioning the practices of Verizon, which is one of the largest telecoms in the U.S.," Shear said.

Another telecommunications company, the U.K.-based provider TalkTalk Telecom Group PLC, recently experienced firsthand the downfall of inheriting bad security in a deal, with the U.K. data protection regulator on Wednesday leveling a record £400,000 ($509,834) fine for a breach that compromised data from an underlying customer database included in the company's 2009 acquisition of Italian telecom Tiscali SpA's U.K. operations.

"Companies are really beginning to see the importance of examining the cyber and privacy risks of the target they are seeking to buy, and this kind of due diligence should reveal any problems before making a giant acquisition like this one," Winton said.

Besides the importance of vetting acquisition targets, the Yahoo email scanning report also highlights the pressing need for both a conversation to be started between law enforcement officials and the tech communities in order to try to strike a balance that both sides can live with, as well as for Congress to update legislation such as the Electronic Communications Privacy Act, which was passed in 1986.

"Our privacy laws are stuck in the 1980s," Shear said. "Balancing lawful access with users' privacy expectations is always a big challenge, but we've reached a tipping point where Congress needs to act."

And while they wait, companies will most likely continue to press their cases in court, especially as public pressure mounts to fight back at what are perceived to be overbroad

government demands, attorneys say.

"I wouldn't be surprised to see an uptick in litigation over government requests for data and assistance," McAndrew said. "The private sector in recent years have been emboldened to challenge these issues, and I think it will continue."

--Editing by Katherine Rautenberg and Kelly Duncan.