# It's warrant time: Do you know where your data is?

By Joseph Marks

1/30/15 5:00 AM EST

The furor over Google's decision to turn over European Wikileaks' employees' emails in response to a U.S. warrant highlights a big problem for users trying to keep control of their personal data: They generally don't know where it is.

At the center of the case are emails and other personal data from three Wikileaks staffers that Google turned over to the Justice Department in response to a 2011 warrant issued in the Eastern District of Virginia. A gag order that Google says it fought prevented the company from informing Wikileaks of the warrant until December last year.

Those Gmail accounts were all created outside the United States by non-Americans and were primarily accessed from Europe and Iceland, according to Wikileaks attorneys and Kristinn Hrafnsson, a Wikileaks spokesperson who was among the three employees whose emails were turned over. Yet it's likely that Google stored the emails, or copies of them, in servers somewhere inside the United States, experts say, creating a much simpler legal process for U.S. prosecutors to gain access to them.

It's also likely the emails, or copies of them, were stored in one or more other nations, which could likewise create a simpler pathway for those nations' law enforcement agencies to demand them from the local Google office.

The case highlights the difficulty of controlling data — or even knowing precisely where it is — in the cloud computing era. That uncertainty is unacceptable for some users in an era when revelations about surveillance by the NSA and other national spy agencies have made nations, businesses and citizens increasingly concerned about shielding their data from prying eyes.

Google declined several times to tell POLITICO where the Wikileaks emails were located at the point the company complied with the warrant.

The company won't disclose the location of any user data out of security concerns, senior law enforcement and security counsel Nicole Jones said.

"I … can't tell you the answer to your question because I don't know," Jones said when asked about the location of the emails during a Center for Strategic and International Studies panel discussion Wednesday. "But, also, for the security of any user, I wouldn't answer that question to anybody, to tell you where it is exactly that Google is storing your data so there's a map for somebody to target, to try to access [the data]."

Wikileaks attorneys said they're also in the dark about where the emails were stored and are attempting to find out if they were retrieved from non-U.S. servers. If that's the case, Wikileaks may take legal action against Google in that country, said Carey Shenkman, an associate for Wikileaks attorney Michael Ratner.

The opacity about Google's data practices has required some tricky legal footwork by Wikileaks attorneys.

"A key question is where was the data located," Shenkman said.

“Our guess is that if it was located outside the United States, Google may not have insisted on a mutual legal assistance treaty request,” he said, referring to an often onerous and lengthy legal process by which nations can ask each other’s law enforcement agencies to obtain data for them.

“In [that] case,” Shenkman said, “our clients would have certain legal rights against Google in the country where the data was located.”

There’s a good chance, however, according to technology experts, that the Wikileaks emails existed on servers in more than one country. That might be because Google “mirrored” the data on servers in multiple locations as a security precaution in case a natural disaster destroyed servers in one place. It could also be because the company shifts data from one location to another during periods of heavy Web traffic to maximize server utility — that’s called “load balancing.”

**Microsoft parallels**

In a somewhat similar case, Microsoft is fighting a December 2013 search warrant for emails that were solely stored on a server in Dublin.

Microsoft argues those emails — which don’t currently exist on U.S. servers — should be governed by Irish law — just as paper letters in a Dublin file cabinet would be. If U.S. law enforcement agencies want access to the emails, Microsoft argues, they should ask Irish police to request them using an MLAT.

The Justice Department argues it’s not really requesting information stored abroad because Microsoft could simply produce the emails from a computer in Redmond, Washington, without ever crossing an ocean, simply by transferring them over the Internet.

Microsoft lost the first round of that argument at the U.S. District Court for the District of New York in July and is currently appealing the decision to the U.S. Court of Appeals for the Second Circuit.

A who’s who of top tech companies, industry organizations and privacy groups has filed friend of the court briefs supporting Microsoft in that case, including Verizon, AT&T, the Chamber of Commerce and the National Association of Manufacturers. Google was not among them.

When asked whether Google supports Microsoft’s position in that case Wednesday, Jones said her company “is obviously watching [the case] very carefully” and is grateful the case has prompted a broader discussion about data privacy and territoriality.

She warned, though, that a decision in Microsoft’s favor wouldn’t solve all of industry’s problems with cross-border law enforcement data requests because of companies’ varying data architectures. “What might make sense and apply to one company in one situation may not apply at all to the way another company is set up,” she said.

One lawyer involved with the Dublin case suggested Google is concerned that if Microsoft prevails, the precedent will incentivize foreign governments to press for more data to be held inside their countries — out of concern criminals could evade police simply by storing their data abroad.

This process is often referred to as data localization. In a similar vein, Google and several other tech companies have long resisted placing data centers in mainland China out of concern that would give communist leaders access to the emails and other communications of dissidents.

As with other people contacted for this story, the attorney stressed he does not know how Google stores its data.

There's also concern from the other side, the attorney noted, that a loss by Microsoft could spur data localization by governments and companies concerned about giving U.S. law enforcement easy access to their data.

The attorney described the presumed Google position as "an outlier" among major tech companies.

While that may be true, many of the groups that filed friend of the court briefs in the Microsoft case took less absolute positions than Microsoft's.

An amicus brief filed on behalf of AT&T and several other companies, for example, allowed that there may be some limited situations in which the U.S. government should be able to access communications involving American citizens that was intentionally moved outside the reach of the U.S. government. The brief described theoretical situations in which data is moved to a hostile state, such as Iran, that the U.S. is very unlikely to be able to strike an MLAT agreement with, or to the high seas where there's no governing state to request assistance from.

**What's the solution?**

The panel discussion that Jones spoke at Wednesday focused on mutual legal assistance treaties and a series of proposals to improve them offered by the Global Network Initiative, a consortium of companies, civil society groups and academics.

Jones generally advocated for firmer understandings between nations about what can be requested and when and developing electronic systems to process MLAT requests more rapidly. Those calls were echoed by panelists from GNI and Microsoft.

While improved MLATs are likely to give companies better guidance in responding to government information requests — and to reduce the chance companies will end up facing off with governments in court — they'll do little for customers who still won't know which countries have access to their data and with what degree of legal difficulty.

The answer for the technically savvy is to make security and privacy high priorities.

Hrafnsson, the Wikileaks spokesman whose Gmails were obtained by the government, has used specialized systems with strong encryption for most of his professional emailing for the past several years, he told POLITICO.

"This is primarily information of a personal nature and most of it predates my involvement with Wikileaks as a journalist," Hrafnsson said of the emails accessed by the U.S. government.

"I use different email services for different purposes for obvious reasons," he added. "Gmail, I used primarily before I became more knowledgeable about the infringement, or possible infringement, of my privacy."

For people who are less privacy savvy, however, there may be some value in companies that store large amounts of data being clearer about where that data will be stored and whose laws will apply, some experts said.

"The takeaway message is maybe there's a need for increased transparency and clarity as to how data is being stored, so users and policymakers can make more informed decision," said David Thaw, an assistant professor of law and information sciences at the University of Pittsburgh and an Information Society Project fellow at Yale Law School.

“I’m not asking Google to give away trade secrets,” he added, “but to generally tell users what laws will end up applying.”

To view online:
https://www.politicopro.com/go/?id=43270