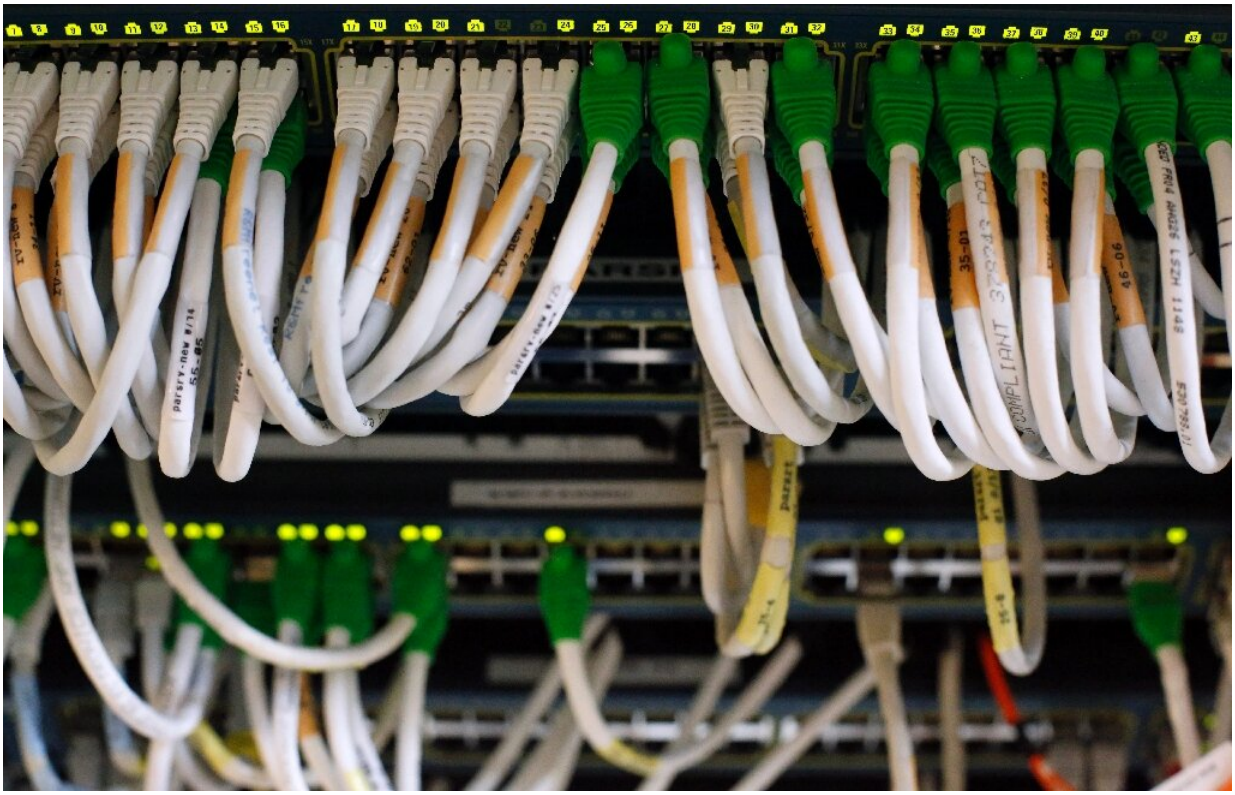
US, EU spar over sharing electronic evidence in investigations

May 12 2019, by Charlotte Plantive



Cross-border acess to cloud computing evidence is hampered by outdated agreements on international legal cooperation and evidence sharing written before the rise of the internet

In August 2016, the lifeless bodies of a young French man and woman were discovered on a beach in Madagascar, with murder suspected.

The secret to the case could be in the last messages they sent, but those are stored in the databanks of US tech giants who don't have to turn over the information to French investigators.

The case is one of a growing number highlighting how key evidence needed to solve crimes could sit in computers a continent away under completely different legal jurisdiction.

Washington and Brussels have both proposed solutions to facilitate relatively easy cross-border access to the data for law enforcement officials.

But the issue has stirred up a hornet's nest of opposition over privacy rules and legal procedures.

Rights groups fear the solutions will lower the barriers to access private data, allowing abuse by governments who could conceivably use their access powers against political opponents or rights groups.

Extraterritorial evidence

The young French man and woman, volunteers for a local whale protection group, communicated Facebook's instant messaging service Messenger and via emails on Microsoft's Outlook.

Knowing their final messages and movements could be "decisive" in settling the investigation, according to sources familiar with the case.

The United States and the European Union are trying to balance privacy with access for law enforcement to data on far away computers in countries under different legal jurisdiction

But given the rise of cloud computing, such evidence is often stored far from the jurisdiction of investigating police.

Getting to it is hampered by old, bulky agreements on international legal cooperation and evidence sharing written before the rise of the internet and social media.

The problem has been growing for several years.

In 2013 US authorities obtained a search warrant in a narcotics case to get user information held by Microsoft.

But even though it is a US company, Microsoft fought back in court, saying the data was on extraterritorial Microsoft servers located in Ireland, out of the reach of US investigators.

Ten months to obtain evidence

In the European Union, 85 percent of criminal investigations involve electronic evidence, of which two-thirds is stored in another country.

But obtaining potential evidence from Facebook account today takes Europeans on average ten months.

Obtaining potential evidence for a criminal probe from a Facebook account takes Europeans on average ten months

A European investigating judge must ask an official of his government to send an official request to the US government.

Then a US judge, who isn't familiar with the case, then makes the request to Facebook.

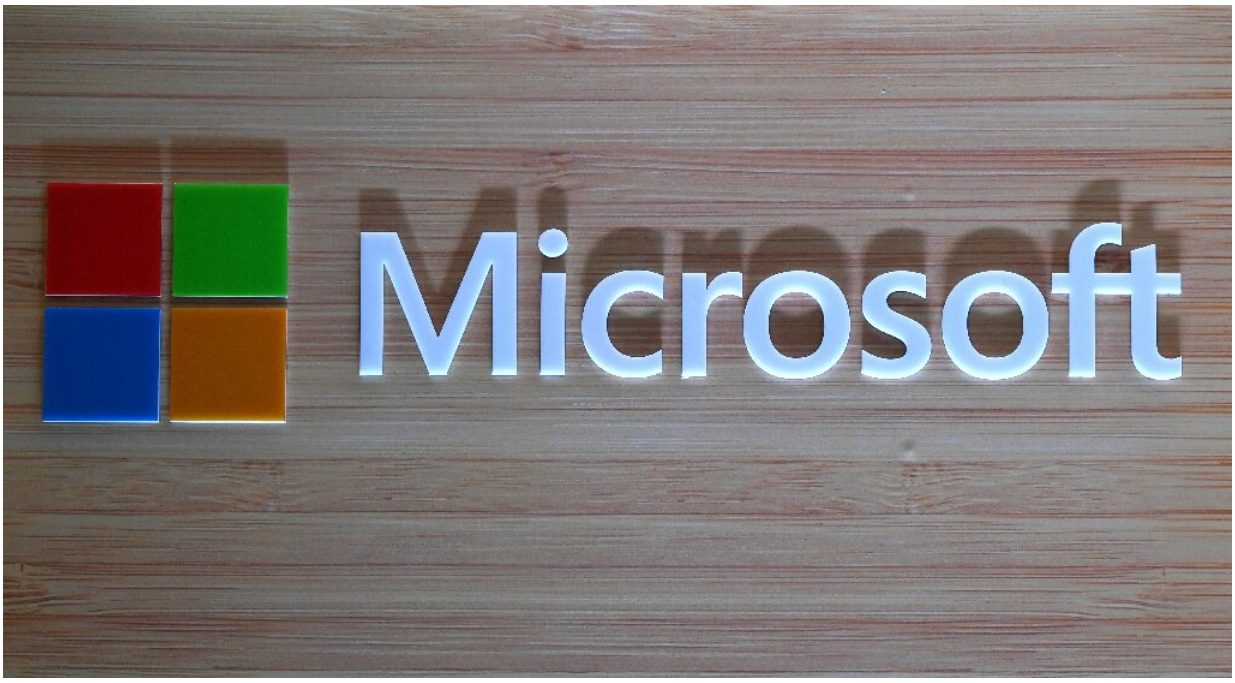
The FBI then reviews the evidence to ensure it does not contain confidential information unrelated to the original request.

The data is then sent to the requesting government which passes it to the investigators.

"This doesn't work, the operations are totally blocked," a frustrated European justice official said.

"We all know that virtually every serious threat we investigate today requires access to electronic evidence like the contents of emails, instant messages, photos, traffic data, session logs, subscriber information, and the like," Richard Downing, a top US Justice official, said in a speech in London last month.

"Our collective safety and security depends on our ability to maintain lawful and efficient cross-border access to that evidence."



The French couple found dead on a Madagascar beach were volunteers for a whale protection group and communicated on Messenger, Facebook's instant messaging service and via emails on Microsoft's Outlook

US seeks bilateral deals

Seeking a longer-term solution, in March 2018 the United States passed the Cloud Act, which sets up the possibility of easier cross-border cooperation in obtaining the communications and other digitally-stored evidence needed in investigations.

The act would allow foreign governments to request the information—emails, text messages, and stored records—directly from US-based communications and internet companies holding it.

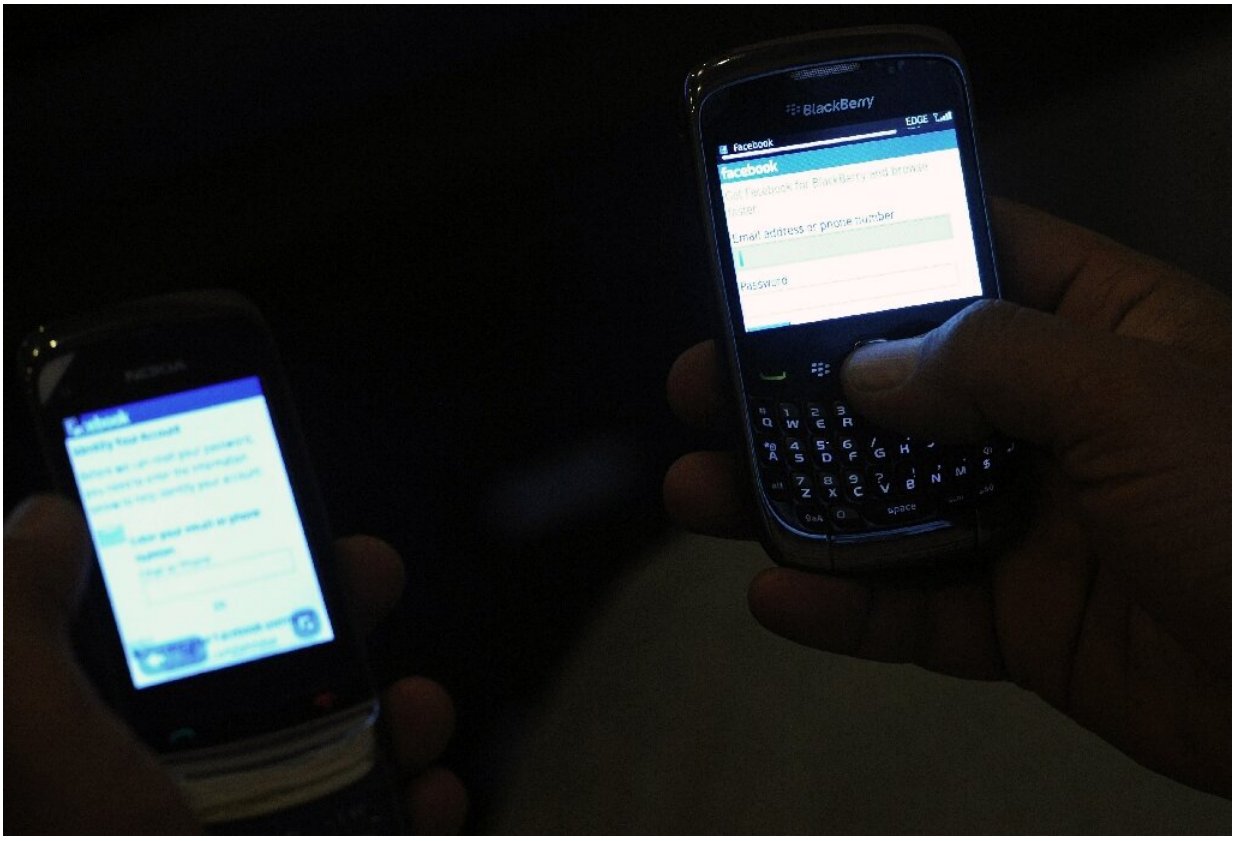
The act would require bilateral agreements that give Washington

reciprocal rights to obtaining electronic evidence.

But many Europeans remain suspicious of Washington's bilateral approach, rather than dealing with the European Union as a whole.

Some believe the US would use the Cloud Act to collect information on European citizens, and not just Americans.

"No one can accept that a foreign government, even American, could come and with no warning look for data on our societies stored here by American companies, without us able to respond," said French Finance Minister Bruno Le Maire.



Rights groups fear that current proposals to make it easier for law enforcement

to access data on foreign servers could result in abuses by governments, who could use it to target political opponents

EU plan: 'E-evidence'

However—as the French murder investigation shows—Europe recognizes the need for new rules.

The European Commission has proposed its own solution, "E-evidence" for easing cross-border requests for electronic evidence.

As with the Cloud Act, it bypasses existing structures for evidence sharing: authorities would make requests directly to the service providers directly, regardless of where the data is stored.

The service providers would have 10 days maximum to respond.

Both systems have raised deep concerns of too few protections against abuse.

The European proposal has not been greeted unanimously by EU members: significantly, Germany and the Netherlands have expressed strong reservations about the E-evidence proposal over the lack of sufficient privacy protections.

Citation: US, EU spar over sharing electronic evidence in investigations (2019, May 12) retrieved 10 May 2024 from https://phys.org/news/2019-05-eu-spar-electronic-evidence.html