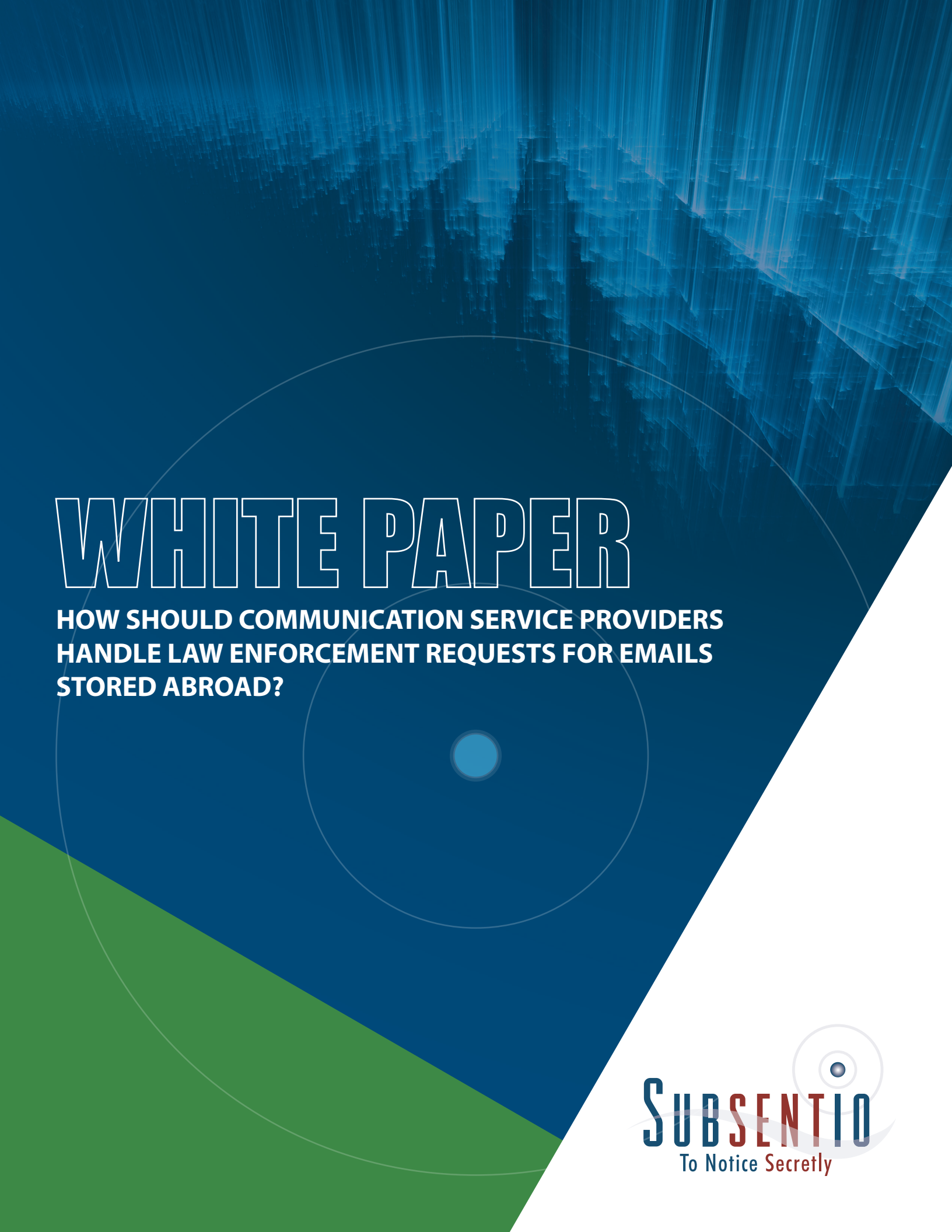

WHITE PAPER

HOW SHOULD COMMUNICATION SERVICE PROVIDERS HANDLE LAW ENFORCEMENT REQUESTS FOR EMAILS STORED ABROAD?

SUBSENTIO

To Notice Secretly

The judicial conflict over foreign-stored email is not some obscure legal debate of passing interest to the communications industry. The fight involves two giants of the US tech industry – Microsoft and Google – which together account for over a billion email users. It also impacts all other industry players that store emails and related end-user records. [1]

The following summarizes the two judicial rulings, explains how they impact the interested parties – email users, law enforcement agencies (LEAs) and communications service providers (CSPs) – and suggests how the dispute might be resolved.

The Stored Communications Act Permits LEAs to Collect Stored Email

In the US, the privacy of telephone calls, Internet sessions, email correspondence, and other electronic messages is protected by the 1986 Electronic Communications Privacy Act (ECPA). The section of ECPA that protects stored communications such as telephone billing records, voice mail, and email is the Stored Communications Act (SCA). These stored items are presumptively private, but certain exceptions permit the data to be disclosed. For example, a criminal court judge may sign a search warrant directing a CSP to deliver a suspect's emails to an LEA once the LEA has shown "probable cause" that the emails are probably indicative of a crime or terrorist plot.

The key provision of the SCA that entitles LEAs to collect suspect emails is Section 2703(a). 18 U.S.C. § 2703(a). Section 2703(a) states that:

> *A government entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication … only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction.*

Ever since the American public began exchanging emails, LEAs have served American CSPs with court-issued search warrants to collect the emails of individuals suspected of crime or terrorism. CSPs have routinely complied.

But the conventional SCA practice was disrupted in 2016 following litigation by Microsoft. As a result of the company's action, the Second Circuit Court of Appeals imbued Section 2703(a) with a new interpretation that significantly restricted its applicability.

The Second Circuit Ruling in the Microsoft Case Hindered LEAs from Collecting Emails Stored Abroad

Beginning in December 2013, Microsoft challenged the validity of an email warrant in a drug investigation. Microsoft argued that the targeted email had been stored in Ireland, and that Section 2703(a) did not give US judges "extraterritorial jurisdiction" to obtain such foreign-based communications content. After losing its case before two lower courts, Microsoft appealed again and won. In October 2016 the Second Circuit Court of Appeals agreed with Microsoft's jurisdictional point. Then, in January of this year the Second Circuit denied a request by the Department of Justice (DOJ) to rehear the case.

The Microsoft ruling forced CSPs to revise their warrant compliance procedures. When served with email warrants in the Second Circuit's jurisdiction, which spans New York, Connecticut and Vermont, CSPs could no longer decide whether to comply with such a warrant until they first determined whether the desired emails were stored domestically or abroad. The Microsoft precedent also left CSPs unsure how to respond when served with email warrants in other federal circuits.

Further confusion followed when another federal court – the Eastern District Court of Pennsylvania –delivered a ruling that refuted the Second Circuit decision. Once

303-794-6936 • info@subsentio.com • www.Subsentio.com

again, LEAs had attempted to access emails stored offshore. This time the objecting party was the world's largest Internet company: Google.

The District Ruling in the Google Case Preserved LEA Authority to Collect Emails Stored Abroad

On February 3, 2017, just 10 days after the Second Circuit declined to rehear the Microsoft case, its ruling was expressly contradicted by a decision in the Eastern District Court of Pennsylvania. The Eastern District case involved an investigation of criminal fraud, and the warrant sought emails from Google.

In the Google case, the Eastern District upheld the traditional interpretation of Section 2703(a). The Court stated that regardless of whether the targeted emails happened to be stored domestically or abroad, the warrant validly ordered a "search" (i.e. disclosure) of the data in the US, where Google's security staff would access the material and forward it to the LEA.

The Eastern District stands in the hierarchy of the Third Circuit Court of Appeals. The District covers Eastern Pennsylvania, Delaware, and New Jersey. As a result of the Google decision, a CSP must continue to implement email warrants without regard to location for purposes of all federal circuits except the Second Circuit, where compliance still depends on whether the requested email is housed on US soil.

The Second Circuit Court may be an outlier on the meaning of Section 2703(a), but its jurisdiction is undeniably important. The judicial ambit includes greater metropolitan New York City, a central hub of international communications ports for undersea fiber optic cables that transit traffic between the US and foreign destinations. Thus, the Court's opinion may have far-reaching consequences.

Let us now consider the impact of this ruling on end users, public safety and CSPs.

The Microsoft Ruling Offers Mixed Results for End Users

To communication subscribers, the Microsoft decision may seem arbitrary. Most email users do not control or monitor the CSP server locations where their emails are stored. They just want their messages kept private and secure. So the location factor does not appear relevant to a user's expectation of privacy.

The US does not regulate the location of CSP data repositories. Certainly no US law considers foreign-based servers any more private than domestic ones. The primary way US law protects the privacy of communications content from undue LEA infringement is to require LEAs to demonstrate probable cause to a judge. In the cases of Microsoft and Google, that standard was undisputedly met.

If an American citizen's emails are maintained in a foreign server they may actually receive less privacy protection than emails kept in the US because the criminal procedures of many foreign countries, including those in the European Union, lack the high due process standard of probable cause. They commonly require LEAs to show only that the targeted emails are "relevant" to a criminal or terrorist investigation. That means European LEAs may gain access to an American's EU-stored emails more readily than American LEAs, even those American LEAs acting outside the Second Circuit. Therefore, if multinational CSPs shift their email storage containers to offshore locations, they will generally reduce privacy protection for their American users.

Even if an American email user were to switch from an American CSP to a foreign CSP, where both competitors store emails in the US, the individual may lose a degree of privacy. Suppose a German government authority orders the German CSP, Deutsche Telekom AG, to contact its US wireless subsidiary, T-Mobile US, and retrieve an American suspect's emails stored in Seattle. That search could be conducted under Germany's low relevance standard of due process, not the high standard of probable cause. For this reason, major American CSPs commonly ask requesting foreign LEAs to obtain the needed evidence through the "mutual legal assistance treaty MLAT" process described below.

But not all subscribers think alike. Privacy-minded American email users may gladly accept the increased risk of access by European LEAs if their priority is to evade US LEAs. Those individuals could follow the example of the suspect in the Microsoft case by registering for email service from a European address.

The Microsoft ruling is also a win for persons residing outside the US. Many foreigners distrust the combined power of American law enforcement and American CSPs, especially after 2013, when National Security Agency contractor Ed Snowden exposed the global surveillance operations of that intelligence agency. In their view, the FBI has no business accessing a European user's emails in Ireland, regardless of whether the agents demonstrate probable cause to an American judge. They presumably want any disclosure of their emails to be conducted under their own governments' standards of privacy and due process. Hence, these consumers are likely glad to hear that American investigators acting in the Second Circuit are obstructed from collecting emails deposited in non-US servers.

The Microsoft Ruling May Threaten Public Safety

Until the Microsoft ruling, an American LEA could serve a search warrant on a CSP doing business in the US to obtain the emails of a suspect using the CSP's network, and the CSP would be required to disclose the targeted material, regardless of whether it was stored domestically or abroad. By comparison, if an LEA felt no urgency to read the email content, but only needed to know who sent and received the emails, along with the times and dates of the messages, the LEA could serve the CSP with a subpoena, and the CSP would be required to disclose the requested metadata, regardless of whether it was stored domestically or abroad. A subpoena may be issued under the low "relevance" standard of due process.

The Microsoft decision bars American LEAs in the Second Circuit from using search warrants to access foreign-stored email content. Significantly, the new restriction would block an investigation of such emails, even if the warrant is valid, the suspect is American, the victim is American, the crime takes place in America, and the email communications are sent and received in America. US law enforcement considers this ironic outcome a threat to public safety that was not contemplated by the SCA.

Another way of assessing the risk to public safety, one that highlights a different irony in the Second Circuit's approach, is to compare the use of warrants and subpoenas. Under the legal framework of the Second Circuit, if an LEA meets the high standard of probable cause for a warrant to obtain email content, it cannot obtain that type of evidence anywhere outside the US, but if the same LEA meets the low standard of relevance for a subpoena to obtain email metadata, the agents may obtain evidence everywhere in the world.

Yet another topsy-turvy outcome of the Second Circuit decision creates a disparity between American LEAs and foreign LEAs. In particular, an American LEA may be excluded from the foreign-stored emails of American suspects, even though the same emails may be readily viewed by foreign LEAs who lack any interest in the American crime.

The Second Circuit believes its decision will not harm public safety because LEAs have a work-around. Specifically, the US and many nations have signed mutual legal assistance treaties (MLATs) that provide LEAs a government-to-government channel to obtain stored communications such as emails. First, the US Department of Justice (DOJ) would submit a request for assistance to its counterpart agency in a foreign country such as France's Ministry of Justice. Then the French National Police would gather the emails under French

303-794-6936 • info@subsentio.com • www.Subsentio.com

standards of due process and privacy. Finally, the Ministry of Justice would forward the evidence to the DOJ. MLATs avoid cross-border conflicts of law where a request from Country A for evidence stored in Country B may otherwise violate the laws of Country B.

However, LEAs complain that relying on the MLAT process is no guarantee for obtaining evidence stored abroad. The US has not signed MLATs with many countries. Also, MLAT requests are not always approved by the receiving countries. Even where they are approved, the process takes a long time. Depending on the nature of the request and the closeness of the two countries, an LEA may have to wait several months or more to receive the needed evidence. By that time a criminal could literally get away with murder. For these reasons LEAs prefer to serve their due process requests directly on CSPs.

The digital storage policies of Internet giants like Microsoft and Google make MLATs even less reliable. In the above-described court proceedings, the industry leaders explained that their storage systems run on optimization algorithms that "fragment" emails into bits, store the bits in different server locations, and change the locations automatically from time to time. Google actually revealed that its own staff may not know the bit locations of an email identified in a warrant. Consequently, an LEA may not know which nation to approach with its MLAT request.

The Microsoft Ruling Offers Pros and Cons for CSPs

Most CSPs realize they are legally required to assist LEA investigations but also have responsibilities to protect subscriber privacy. Sometimes these obligations conflict. If a CSP refuses an order to retrieve emails from a foreign country, the service provider may be fined by the ordering court. Conversely, fulfilling the order may violate the foreign country's due process and privacy laws. The Second Circuit ruling resolves the conflict by prohibiting the foreign retrieval.

A CSP may try to avoid a similar conflict in another circuit by petitioning the court to quash the email warrant, as Microsoft did in the Second Circuit, or ask the LEA to use an MLAT. Either approach would score points with privacy-minded subscribers. Of course, not all CSPs can afford the specialized legal expertise needed to litigate such matters, especially if they do not consider the issue core to their business. Other competitors take a more LEA-friendly approach. They have developed reputations as good corporate citizens by demonstrating concern for public safety. There do not appear to be any industry-wide studies on the number of international email requests that have caused legal conflicts, or how often such standoffs have triggered CSP liability.

Given the Second Circuit precedent, international CSPs like Microsoft and Google may start retaining more communications content outside the US. The strategy may significantly raise their digital storage costs and hinder operations. But it would enable them to withhold more data from US LEAs. Silicon Valley players have increasingly defied US LEAs as a means of burnishing their privacy credentials among foreign customers, as in the EU, where many citizens demand strict privacy protection and distrust US LEAs.

A key downside of the Second Circuit ruling for CSPs is that it complicates the law enforcement assistance process. A CSP's security staff must remember that when a request for communications content originates from the Second Circuit, they must identify the email storage location before deciding whether to disclose the requested information. If they cannot find the email

location, it is unclear how they should proceed. CSPs dislike regulatory uncertainty. They prefer working environments that are uniform and stable.

A footnote in the Second Court decision shows another important consideration for CSPs. The note remarks that CSPs have the discretion to decide whether to assist LEAs in cases of emergency. Suppose an LEA based in the Second Circuit investigates a suspect who is apparently planning a murder. The LEA makes a phone call to an American wireless carrier with operations in the EU seeking copies of the suspect's EU-based emails over the past few weeks. In this situation the American CSP may disclose the information on a voluntary basis, even without receiving a warrant or subpoena. Alternatively, the CSP may hang up the phone.

Notice that CSPs in the foreign-content-emergency-request scenario may position themselves anywhere on the legal continuum from extremely pro-public safety to extremely pro-privacy, regardless of the federal circuit jurisdiction or the other above-described laws. This condition further complicates the CSP compliance task. Before establishing a corporate policy on foreign-LEA emergency requests, a CSP should consult an expert to help weigh the options.

The Conflict Between the Microsoft Ruling and the Google Ruling May be Difficult to Resolve

It is unclear whether the majority of US judges will: (a) gravitate toward the Second Circuit/Microsoft innovation of stricter privacy protection for foreign-stored communications content; or (b) maintain the preexisting balance of interests represented by the Eastern District/Google ruling. Much depends on whether the Google case is appealed to the Third Circuit Court of Appeals and whether similar issues arise in other federal circuits.

In the DOJ's view, the Second Circuit opinion should be overturned. The DOJ could pursue this goal in multiple ways. It could appeal the Second Circuit ruling to the Supreme Court. The risk of this option is that the high court's current eight-member panel may uphold the Second Circuit's logic or reach a four-four deadlock, which would leave the Second Circuit result intact.

A potentially more effective strategy would seek a congressional amendment of ECPA, including the SCA. Many congressmen of both major parties agree the old 1986 statute sorely needs updating. In 2015 two bills appeared on Capitol Hill to address the issue of LEA access to emails stored abroad. The first was the Law Enforcement Access to Data Stored Abroad Act (the LEADS Act), introduced in the Senate as S. 512 and in the House as HR 1174. The LEADS Act would establish that US LEAs may not use warrants to compel the disclosure of foreign-stored subscriber content unless the suspect is a US person.

At the email-gathering stage of an investigation, an LEA cannot always tell whether the suspect is a US person. Accordingly, Congress devised a more elaborate legislative formula in 2015 called the International Communications Privacy Act (the ICPA), unveiled in the Senate as S. 2986 and in the House as HR 5323. Essentially, the ICPA would permit the extraterritorial collection of suspect emails if the LEA has taken "all reasonable steps" to identify the subscriber's nationality and location and there are "reasonable grounds" to

303-794-6936 • info@subsentio.com • www.Subsentio.com

believe the suspect is a US person, a person located in the US, or a national of "a foreign country that has a law enforcement cooperation agreement" with the US. Neither the LEADS Act or the ICPA has made progress on the legislative assembly line.

If no other legal remedy is available, the DOJ may ask Congress for a simpler but more drastic fix called a "data localization law." Data localization laws vary widely, but they essentially require multinational corporations to host and/or process certain types of information within a nation's borders. The primary purpose of localization is to keep domestically-originated data within the nation's jurisdiction so government agencies may lawfully access it. From the suspect's point of view, the restriction ensures that an individual's personal data is disclosed pursuant to his or her own country's standards of due process, privacy, and security. Such laws have been passed in Russia, China, Australia, Indonesia, India, South Korea, Nigeria, and Brazil.

The communications industry opposes data localization because it frustrates the business of cloud computing. After all, the IT cloud is valuable precisely because it facilitates computer processing in remote locations, including foreign countries. And the cost of building and maintaining a data center in a foreign country can be prohibitive.

The Interests of Privacy, Public Safety, and Business Could be Reconciled Through Global Standardization

There is no easy answer to the problem of ensuring lawful LEA access to data in a globally digitized world. CSPs feel caught in a legal tug-of-war between LEAs who need evidence and customers who demand privacy.

But there is hope. Governments worldwide recognize the need for global standards to balance the interests of privacy, public safety, and business. They have already cooperated well in pursuit of these common goals.

The EU and US signed a "Safe Harbor" agreement to protect the privacy of EU personal data processed in the US, and that arrangement has since evolved into a "Privacy Shield." MLAT agreements formed bridges among many nations for the mutual sharing of investigative data. And free trade agreements have helped level the competitive playing field.

If international regulators would devote more attention to the cross-border email issue, they could establish better ground rules that take all the above interests into account. Then we could stop the madness of trying to solve the problem through ad hoc courtroom fights.

1 Eric Ravenscraft, "Webmail Showdown: Gmail vs. Outlook.com," (April 17, 2016), http://lifehacker.com/web-email-showdown-gmail-vs-outlook-com-1771473111.