ICIT | Institute for Critical Infrastructure Technology

The Cybersecurity Think Tank

ICIT Analysis: The CLOUD Act

Immediate Passage of the CLOUD Act Ensures Unambiguous Protection of Privacy and National Security

March 2018

Authored by:

James Scott, Senior Fellow, Institute for Critical Infrastructure Technology

ICIT Analysis: The Cloud Act

Immediate Passage of the CLOUD Act Ensures Unambiguous Protection of Privacy and National Security

March 2018

Authored by: James Scott, Sr. Fellow, ICIT

Support ICIT

Information should be liberated, not commoditized.

This powerful philosophy is the bedrock of the Institute for Critical Infrastructure Technology (ICIT), a nonprofit, nonpartisan 501(c)(3) cybersecurity think tank located in Washington, D.C. Through objective research, publications and educational initiatives, ICIT is cultivating a global cybersecurity renaissance by arming public and private sector leaders with the raw, unfiltered insights needed to defend our critical infrastructures from advanced persistent threats, including cyber criminals, nation states, and cyber terrorists.

Financial capital from generous individual and corporate donors is the lifeblood of the institute and a force multiplier to our efforts. With your support, ICIT can continue to empower policy makers, technology executives, and citizens with bleeding-edge research and lift the veil from hyper-evolving adversaries who operate in the dark. Together, we will make quantum leaps in the resiliency of our critical infrastructures, the strength of our national security, and the protection of our personal information.

http://icitech.org/support-icit/

Upcoming Event

Contents

Introduction

On February 27, 2018, the Supreme Court began consideration of the long-debated case Microsoft v. the United States, otherwise known as Microsoft-Ireland. The case focuses on whether the 30-year-old, Stored Communications Act (SCA) applies extraterritorially. In other words, the Court will decide whether U.S. warrant authority is restricted by the physical location of the server upon which data are stored. A win for either Microsoft or the U.S. government results in long-term adverse outcomes for the private sector, law enforcement, and privacy and security communities. Despite the case being lampooned into notoriety by privacy advocacy groups, Microsoft, U.S. law enforcement, and the court all agree that it is not a privacy case and the issue under contest has nothing to do with privacy. The entire case hinges on the intent behind the exact words and phrases used in a 30-year old piece of legislation that did not anticipate the Internet or the digital age. The case is about whether the SCA applies to U.S.-based companies operating in other countries. Under the current system, Microsoft would still relinquish email and other data stored in the United States without contest if presented with the appropriate warrant based on probable cause and sufficient evidence.

Microsoft-Ireland is not an issue of privacy; it is entirely an issue of semantics. According to many views, Microsoft had little choice but to pursue an expensive legal battle because they felt they could not legally fulfill the request for information without infringing on the sovereignty of the foreign nations in which they operate. Meanwhile, the United States government has spent thousands or millions of taxpayer dollars pursuing the case because their only alternative was to set a precedent by dropping the case and attempting forever to access data stored abroad through the dysfunctional Mutual Legal Assistance Treaty (MLAT) process. Complications with the MLAT process is a more significant and pressing issue than the faux-privacy debate surrounding the case; however, due to the convolution of the interwoven treaties, it received disproportionately little coverage compared to the alleged privacy aspects of the case.

To put in perspective why the problems with the MLAT system daunt the misapplied privacy complaints, consider the following example under the current MLAT system. A significant portion of the evidence in a wide variety of cases is now digital. If German authorities were investigating a domestic abuse incident in which threats were communicated over Facebook messenger, and proof of those threats were pivotal to the case (and essential for a restraining order, protective custody, etc.) then they would have to leverage an MLAT with the United States to file a request with U.S. law enforcement. U.S. law enforcement would eventually receive and process that request (after dealing with similar claims from every MLAT-partnered nation), and they would then file an application for the information to Facebook on behalf of German law enforcement. When Facebook eventually evaluates and processes the request,

they would decide whether or not the support for the case (and the warrant) proves sufficient to access the data (stored on servers abroad, possibly even in Germany) under the antiquated Stored Communications Act (which was written before the Internet was ubiquitous). In all, the process to complete a time-sensitive request could take months or over a year. Consider that the same process may be the only legal course of action if authorities in the UK are investigating individuals suspected of plotting an act of terrorism.

For reasons discussed at length below, neither outcome of the Microsoft-Ireland case is desirable nor diminishes the complexity or bureaucracy surrounding the MLAT process. Instead, a bipartisan coalition of senators proposes passage of the CLOUD Act as an alternative solution that would bypass the MLAT process, moot the Microsoft-Ireland case (and reduce the ongoing legal fees to Microsoft and taxpayers), and mitigate both undesirable outcomes and the ensuing negative cascading impacts. The CLOUD Act would empower U.S. law enforcement and authorities in countries that enter into agreements with the government, to quickly access essential evidence stored in servers owned by companies that are based in the United States, provided that there is probable cause and warrant to access that information. The CLOUD Act has the support of Microsoft, Apple, and other technology leaders. The CLOUD Act is the only solution proffered to the dispute that saves lives, has the support of both sides, preserves international relations, empowers law enforcement, and ensures justice for citizens.

The CLOUD Act Dispels the Drama of Microsoft-Ireland

On February 27, 2018, the Supreme Court began hearing arguments pertaining to the notorious Microsoft-Ireland case, focused on the issue of United States law enforcement's ability to reach data stored across national borders. The case presents the court with two unfavorable options, based on the interpretation of the 30-year-old, antiquated Stored Communications Act (SCA). Either U.S. warrant authority is limited to data physically held within the United States, or it reaches all data held by a U.S. company, regardless of location [2]. The CLOUD Act alleviates the tension in this debate by offering a solution that is favorable to both technology companies and the government, that is flexible in its execution, and that better ensures the long-term privacy rights of U.S. citizens.

The Microsoft-Ireland case hinges on the question of whether Section 2703(a) of the SCA, the provision under which the government sought and received a search warrant for an email account, applies extraterritorially. In December 2013, federal law enforcement was conducting a criminal narcotics investigation. During its investigation, the government sought a search warrant, pursuant to Section 2703(a) of the SCA, to seize the contents of a Microsoft email account belonging to a customer. According to the court proceedings, Microsoft stores the contents of its users' emails on 100 discrete data centers worldwide. Each user's data is stored

based largely on the user's unverifiable "country code," which is allegedly, but not always, geographically proximate to that user's actual location. Once transferred abroad, the data, for the most part, is deleted from U.S. servers. Microsoft retains the capability to retrieve the data from systems in its U.S. offices; however, it is unclear whether it is obligated to do so or if complying with such a request would violate the sovereign data privacy laws of the country where the information is stored. Microsoft complied with the warrant to an extent, turning over any account information that was being stored in the United States. The actual emails and their contents were stored overseas in Dublin, Ireland, however. Microsoft did not overturn the content, and the district court held the corporation in civil contempt for its failure to comply with the warrant. Three years later, the Second Circuit reversed the previous decision, holding that "§ 2703 of the Stored Communications Act does not authorize courts to issue and enforce against U.S.-based service providers' warrants for the seizure of customer e-mail content that is stored exclusively on foreign servers" [1].

The Stored Communications Act, enacted as Title II of the Electronic Communications Privacy Act (ECPA), is at the center of the debate. Passed in 1986, the ECPA was envisioned to update the Federal Wiretap Act of 1968 to include computer communications. The SCA itself was not designed with the digital age in mind and is therefore insufficient for deterministic governance of data quandaries that could jeopardize lives, personal privacy rights, or national security. The purpose of the SCA, as emphasized throughout the Second Circuit's opinion on the Microsoft-Ireland ruling, was to "extend electronic records' privacy protections analogous to those provided by the Fourth Amendment." The act was implemented to protect users of electronic communication services or remote computing services and provided general obligations of non-disclosure on service providers. The SCA also created exceptions to those obligations, including the current warrant provision, under which the government may require a service provider to disclose the contents of stored communications. The warrant provision allows that any warrant obtained under the SCA must be issued using the procedures described in the Federal Rules of Criminal Procedure. The crux of Microsoft v. the United States is whether the SCA's warrant provision applies extraterritorially. The government contends that when the SCA used the word "warrant," the statute was actually referring not to a traditional warrant, but to a legal process or "compelled disclosure" more akin to a subpoena. A warrant, according to the Second Circuit and conceded by the government, has domestic boundaries. According to the court, the purpose of the Fourth Amendment was to restrict searches and seizures conducted in the U.S. on domestic matters. Conversely, subpoenas, can require the production of communications stored overseas and are restrained by fewer territorial restrictions [1].

The Second Circuit did not agree with the government's interpretation, and the case has since transcended to a final decision under the Supreme Court. Citing the presumption against extraterritoriality, the court examined whether the SCA's warrant provision contemplated

extraterritorial application. The plain meaning of the SCA has no indications that Congress envisioned an extraterritorial use of the statute. Given a long history of warrants and subpoenas being entirely distinct legal instruments, the court found no reason to infer that Congress used "warrant" to mean "subpoena." Instead, the court ruled that Congress used the term "warrant" to provide a higher level of protection to users. Furthermore, the Second Circuit was not swayed by the government's attempt to import law developed in the subpoena context into the SCA's warrant provision. A previous decision that a grand jury subpoena issued in a tax evasion investigation could reach an overseas Swiss business was not applicable in the current case, where Microsoft was only a data custodian. Likewise, the court discounted the government's argument that banks have been required to comply with subpoenas, citing the Supreme Court's decision that bank depositors have no protectable privacy interests in a bank's records regarding their accounts [1].

After concluding that Congress did not intend the SCA's warrant provisions to apply extraterritorially, the court refocused on the SCA's warrant provisions. Relying heavily on Morrison v. National Australian Bank Ltd., the court looked at whether the domestic contacts were secondary to the statutory focus, thereby precluding an extraterritorial application of the warrant provision. To do so, the court reverted to common tools of statutory interpretation, including the plain meaning of the statute, as well as its legislative history. The court ruled that the primary focus of the SCA was to protect user content. Providing methods for law enforcement to access that content remained a secondary objective – thereby excluding an extraterritorial application. The court also addressed several secondary concerns. The government had argued that the actual conduct in question occurs in the U.S.; to comply with the warrant, the service provider only must act within the United States. The court found, however, that the conduct actually falls outside the U.S., given that the subject of the warrant is located in and would be seized from Dublin [1].

The court acknowledged the government’s position that a ruling for Microsoft would place a substantial burden on the government by requiring it to go through the cumbersome Mutual Legal Assistance Treaty (MLAT) process to conduct searches abroad. The Second Circuit expressed that despite the great need for a modernized framework with a focus on the current digital landscape, however, it cannot ignore the exact text of the SCA and its intent is only to reach data stored within the United States [1].

Despite popular interpretation, Judge Gerard Lynch emphasized that United States v. Microsoft is not about the privacy or Fourth Amendment rights of citizens. In the case, Microsoft does not dispute that the SCA’s warrant provision would be adequate to obtain emails stored on a server within the United States: “Microsoft’s argument is not that the government does not have sufficiently solid information, and sufficiently important interests, to justify invading the privacy

of the customer whose emails are sought and acquiring records of the contents of those emails." In this case, according to the concurrence, a user's privacy is at the mercy of a private corporation, which at any time can send the data back to the U.S. The case is solely about whether or not the exact words written in the SCA apply extraterritorially [1]. Even if decided at the Supreme Court, the case will not ensure additional privacy and is not centered on privacy protections, and either outcome could result in diminished privacy rights in the future. The bipartisan CLOUD Act, which has bipartisan and multi-stakeholder support at every level, resolves the SCA conflict by providing the language necessary to empower law enforcement, protect private corporations, and enhance privacy rights.

Even if the case is decided in favor of Microsoft, there is a distinct possibility that the Supreme Court, like the lower courts, will say that a legal assertion of how or if American law applies overseas is dependent on Congress. Despite the suggestion of numerous privacy authorities, neither privacy nor Fourth Amendment rights are the focus in the case. The entire dispute is yet another result of the government's inability to modernize and adapt to the digital landscape. The drafters of the SCA did not contemplate the extraterritorial application of their statue, primarily because the statute was enacted in the 1980s when the idea of cloud storage was unfathomable. Eventually, Congress will need to weigh the costs and benefits of applying one statute to overseas conduct and update the antiquated law. In other words, after years of considerable expenses to Microsoft and taxpayers, the final verdict could still require Congressional intervention. Implementing the CLOUD Act would mitigate the necessity of an expensive and drawn-out Supreme Court case that could have severe unintentional cascading implications on the legal landscape, privacy rights, and national security. The CLOUD Act, which is endorsed with bipartisan support at every level of government and by Microsoft and other major tech leaders, would preempt the Supreme Court decision and wholly prevent future disputes that result from reliance on outdated laws.

Neither Microsoft-Ireland outcome is beneficial to the privacy community, law enforcement, or national security, and both findings will result in drastic cascading impacts, the least of which will be the extreme actions the losing side takes to mitigate what they see as a devastating outcome. One of the main problems with the case is that both possible outcomes are absolutes with implications that far exceed the scope of the case [2].

The U.S. tech community fears that they will lose foreign customers if the government wins, and as a result, prior to the proposal of the CLOUD Act, most major firms expressed or signaled support for Microsoft in the case. Major firms, including Microsoft, have shown significant support for the passage of the CLOUD Act. Nevertheless, if the Act is not passed, a win for the government in the Supreme Court case will be viewed around the world as the United States asserting access to all data held by U.S. companies anywhere, without regard to the

countervailing considerations of foreign states or the outdated mutual legal assistance treaties that govern international relations. Federal law enforcement considers the conflict of laws when deciding whether to seek a warrant. This is done as a matter of policy, not law, however, and is not applicable to state prosecutors that can also issue such warrants. Internal executive branch policy constraints are insufficient to counter the apprehensions of foreign customers worried about the reach of U.S. surveillance authorities. Worse, a decision in favor of the government position sets a dangerous precedent that makes it harder for the United States to insist that foreign governments respect U.S. law when seeking the U.S.-held communications content of a U.S. citizen or resident [2].

If the Supreme Court decides against Microsoft, one possible cascading outcome could be that the United States begins to issue requests for data stored abroad and foreign governments emulate the framework implemented and requests made based on the U.S. precedent. Consequently, U.S. firms would either comply and risk jeopardizing the privacy of U.S. citizens; combat the requests via legal channels and incur significant expenses; or ignore the requests and risk financial, legal, and operational ramifications. Current law prohibits direct access of U.S.-held communications content. Foreign governments must make a diplomatic request for the data, rather than going directly to the company that holds it. Data are only disclosed if U.S. law enforcement deems the request worthy and obtains a warrant based on probable cause on behalf of the foreign government. This process leverages MLATs and existing agreements and can take months to conclude [2].

If the court decides with the U.S. government, there is the risk that foreign governments will increasingly try to bypass these restrictions if the United States is seen as directly demanding access to their nationals' data. Alternately, without a framework like that of the CLOUD Act, they might demand equal access to digitally stored information. The broad prospect of nations compelling access to the data of anyone everywhere, without baseline substantive and procedural protections in place, threatens the privacy rights of every citizen of every nation and the continued operation of businesses across the world [2].

A win for Microsoft excessively diminishes law enforcement's ability to investigate crimes based on where vital data is stored at the moment of request. The cost-effectiveness of cloud solutions and the prevalence of storing data abroad, because of server costs and fiscal incentives, are objectively fluid parameters that have nothing to do with the equities of a case but could prove deterministic of the outcome because of nothing more than happenstance, logistics, and operational efficiencies necessary to compete in the global market.

The possible ruling would utterly cripple law enforcement by unequivocally restricting its ability to access or obtain critical evidence-based solely on the decision of a third-party provider of where to hold it. Such a rule also incentivizes data localization mandates, pursuant to which

data is required to be held locally, as a means of ensuring access. As discussed in an October 2017 hearing before the House Energy and Commerce Subcommittee on Digital Commerce and Consumer Protection, the possibility would significantly increase the costs for any company that wants to compete internationally and profoundly damages the future of the Internet and U.S. business interests [2]. Further, in an attempt to comply with law enforcement and continue operations abroad, firms might generate multiple copies of vital data stores, thereby significantly increasing storage costs and expanding the threat landscape surrounding sensitive data.

This profoundly unsatisfactory choice is an apparent ethical and geopolitical dilemma that highlights the need for Congressional action to mitigate two dangerous extreme outcomes with the introduction of a compromise that protects privacy, ensures national security, reduces international operation costs, and institutes a geopolitical framework that both complements and assists in the modernization of the existing and outdated MLAT system. Two Second Circuit judges and numerous other legal authorities agree that immediate Congressional action is the best possible outcome to the Microsoft-Ireland case. The bipartisan CLOUD Act offers a compelling compromise between the tech community and law enforcement. The CLOUD Act has bipartisan support in Congress: 35 state Attorneys General recently endorsed it, it has received significant praise from the legal community, and Microsoft, Apple, Oath (a Verizon subsidiary), and other major tech firms have endorsed it [A5]. British Prime Minister Theresa May and other leaders have likewise expressed support for the bill.

Congress needs to act as soon as possible to pass the CLOUD Act, because its passage will efficiently moot the Microsoft-Ireland case and mitigate undesirable, unpredictable, and un-retractable cascading outcomes. From February 27, 2018, forward, every day that lawmakers delay is a day that taxpayers and Microsoft will pay for continued and increasingly more contentious deliberations of the case. Access to information, based solely on storage location or the practices of third-party data custodians, is not an ideal basis for a ruling that could reshape numerous sectors. Even in the best-case scenarios, either U.S. law enforcement will be perceived around the world as claiming the right to access data anywhere, without regard to the countervailing sovereign interests, or tech companies will be seen as obstructionists opposed to aiding investigations that affect people's lives. In either case, foreign entities will likely mimic the precedent.

The CLOUD Act includes provisions to accommodate foreign interests and thereby mitigates competing data access models. The comity process included provides a mechanism for companies to deny requests for information out of concerns for privacy or the sovereign laws of foreign entities. International comity gives service providers a possible excuse for their failure to comply with a U.S. disclosure order on the grounds that the order conflicts with foreign law.

Under this common law doctrine, providers can and should raise comity concerns if the United States seeks, according to its warrant authority, data of a foreigner located outside the United States and the disclosure order conflicts with foreign laws. There is no guarantee that the final ruling in the United States v. Microsoft case will include a provision ensuring international comity.

The CLOUD Act recognizes the reality of the digital landscape and the needs of the international community. It sets out a statutory mechanism for providers to raise comity claims, albeit in limited situations. It also explicitly notes, via a savings clause, the possibility of common law comity claims with respect to instances of compulsory process issues under section 2703 [3].

The CLOUD Act is a Solution to an Otherwise Unavoidable Dilemma

On February 6, 2018, a bipartisan group of senators, including Senators Graham, Hatch, Coons, and Whitehouse, proposed the Clarifying Lawful Overseas Use of Data (CLOUD) Act of 2018. On the same day, Representative Collins introduced a companion bill in the House of Representatives. The CLOUD Act was negotiated with and draws support from technology companies, including Microsoft, and U.S. law enforcement, including the Department of Justice.

The CLOUD Act appeals to US law enforcement by clarifying that all data that is in the "possession, custody, or control" of American "communications service" (data) providers, wherever that data is stored, is reachable by SCA warrants, subject to principles of international comity. Additionally, it would require participating countries to remove legal restrictions that prevent compliance with data requests from U.S. law enforcement. Oppositely, American service providers gain a transparent process for complying with and challenging government requests for data stored abroad, such as the statutory right to challenge warrants for data regarding foreign nationals based on comity concerns, as well as a process by which to notify certain foreign governments of requests regarding foreign nationals. The CLOUD Act offers benefits for allied foreign governments seeking to protect their citizens' information and also provides a mechanism for assistance from U.S. companies during international law enforcement investigations, provided the foreign governments meet prerequisite criteria. Under the act, foreign governments can enter into bilateral agreements with the U.S. government. Countries that do so would then be permitted to challenge U.S. law enforcement requests deemed inappropriate. The bill authorizes foreign governments to request content regarding foreign nationals directly from American providers under executive agreements if the country meets a set of requirements. These requirements include (1) robust substantive and procedural protections for privacy and civil liberties and (2) appropriate procedures to minimize the acquisition, retention, and dissemination of information.

After being introduced, the Senate's CLOUD Act was referred to the Senate Committee on the Judiciary for review. Its companion in the House was referred to the House Committee on Rules and the House Committee on the Judiciary. If it becomes law, the CLOUD Act will join the Department of Justice's Computer Crime and Intellectual Property Section, Criminal Division December 2017 guidance advising prosecutors seeking enterprise customer data stored "in the cloud" to attempt to collect responsive information from the enterprise first, instead of serving information requests directly on the enterprise's cloud data service provider.

Conclusion

Despite the consternation of overly opinionated privacy advocates, the CLOUD Act is the compromise that law enforcement and leading technology firms believe necessary to the long-term protection of national security, personal privacy, and business interests abroad. As the adage goes, "the hallmark of an effective compromise is that no party is 100 percent happy with the result." Issues of privacy and security are often a tug of war, and progress does not come by leaps and bounds. Advancements are gradual and every inch gained is more valuable than the hypothetical foot that is never realized. The CLOUD Act offers the optimal compromise to every stakeholder. It has bipartisan support at every level of government and the support of tech leaders. Every day that Congress delays passing the CLOUD Act is an expense to taxpayers and an increase in the risk that a less advantageous decision will have to be made. There are no reasons and no more time to delay passing the CLOUD Act.

ICIT Contact Information

Phone: 202-600-7250

E-mail: http://icitech.org/contactus/

ICIT Websites & Social Media

www.icitech.org

https://twitter.com/ICITorg

https://www.linkedin.com/company/institute-for-critical-infrastructure-technology-icit-

https://www.facebook.com/ICITorg

Sources

[1] Lawfare. (2018). The Microsoft Ireland Case: A Brief Summary. [online] Available at: https://www.lawfareblog.com/microsoft-ireland-case-brief-summary [Accessed 23 Feb. 2018].

[2] Daskal, J. (2017). *Where is Congress? The Supreme Court's Cert in Microsoft Ireland Case Should Spur Lawmakers to Act*. [online] Just Security. Available at: https://www.justsecurity.org/46075/congress-supreme-courts-cert-microsoft-ireland-case-spur-congress-act/ [Accessed 23 Feb. 2018].

[3] Daskal, J. (2018). Symposium Recap: We Need the Cloud Act To Save Us & What Bill Dodge Got Right. [online] Just Security. Available at: https://www.justsecurity.org/52879/symposium-recap-cloud-act-save-bill-dodge/ [Accessed 23 Feb. 2018].