TABLE OF CONTENTS

ARTICLE>> ........................................................................................................................................2

United States v. Microsoft Corporation: The Supreme Court Asked to Decide, and Asked Not to Decide, Applicability of Warrants for Foreign-Stored Communications .........................................................................................2

NEWS AND ANNOUNCEMENTS >> ..............................................................................................6

Stay Connected .................................................................................................................................6
ARTICLE>>

United States v. Microsoft Corporation: The Supreme Court Asked to Decide, and Asked Not to Decide, Applicability of Warrants for Foreign-Stored Communications

By Timothy P. Zintak

On February 27, 2018, the United States Supreme Court will hear oral argument in United States v. Microsoft Corporation, an appeal by the Department of Justice from the Second Circuit's decision, 829 F.3d 197 (2d Cir. 2016), reh. den. en banc, 2017 WL 362765 (2d Cir. Jan. 24, 2017) (available at https://scholar.google.com/scholar_case?case=187709056755717713).

The Supreme Court has certified the following question presented for review:

Whether a United States provider of email services must comply with a probable-cause based warrant issued under 18 U.S.C. 2703 by making disclosure in the United States of electronic communications within that provider's control, even if the provider has decided to store that material abroad.

The facts of the case are fairly threadbare because it solely involves an application from the U.S. government in the Southern District of New York for the issuance of a warrant under 18 U.S.C. § 2703, the “ Stored Communications Act” (“SCA”) for stored emails for a Hotmail email account. Microsoft, which owns Hotmail, was ordered to produce the communications in question under the SCA pursuant to its corporate headquarters location in Washington State.

Microsoft refused to comply with the warrant on the basis that the stored communications material sought was stored on a server owned by Microsoft in the Republic of Ireland. After the Southern District Magistrate and District Judge opinions held Microsoft in civil contempt for its failure to comply, Microsoft appealed to the Second Circuit. The panel opinion of the Second Circuit found in Microsoft’s favor, arguing that because the warrant issued required Microsoft to retrieve foreign-stored data, this constituted an extraterritorial application of law. Under the logic of Morrison v. National Australian Bank Ltd., 561 U.S. 247 (2010), and related cases explaining the presumption against extraterritoriality (when interpreting the laws of the United States, a court presumes that legislation of Congress is meant to apply only within the territorial jurisdiction of the United States, unless a contrary intent clearly appears), the Second Circuit found that this warrant constituted an extraterritorial application of the statute, which was facially not supported under the SCA.

In a 4-4 split decision, the U.S. request for rehearing en banc by the entire Second Circuit was denied, with each of the four dissenting judges writing an opinion explaining the grounds for dissent. Among other arguments, these judges cited the established case law relating to the collection of subpoenas where persons subject to U.S. jurisdiction who have access to the...

Notably, other courts have affirmatively found for the foreign applicability of these SCA warrants, in face of arguments based on the Second Circuit’s opinion. See In the Matter of the Search of Content that is Stored at Premises Controlled by Google, No. 16-mc-80263-LB, ECF No. 3 (N.D. Cal. Apr. 19, 2017) (available at https://dlbjbzgnk95t.cloudflare.net/0915000/915244/https-ecf-cand-uscourts-gov-doc1-035115371508.pdf).

Now, upon the government’s appeal to the Supreme Court in Microsoft, the argument presented is exceptionally well-developed, having been briefed, argued, and opined at the Magistrate Judge, District Judge, Circuit Panel, and Circuit en banc proceedings, with countless amicus curiae briefs submitted along the way.

And of course, for an issue of such import to come before the Supreme Court, the amicus curiae practice has likewise been thorough. However, a notable tack taken by multiple amici at this level has been to brief in favor of neither party, owing to the foreseeable and imminent outcomes that private electronic communications providers and foreign governments may take in response to the case. This, along with the possibility of impending legislative action, was also Microsoft’s argument against granting certiorari to the case, a fruitless argument.

In other words, the amici are asking the Supreme Court not to decide the case. One such notable amicus curiae brief is the “Brief of Former Law Enforcement, National Security, and Intelligence Officials as Amici Curiae in Support of Neither Party”, available at https://www.supremecourt.gov/DocketPDF/17/17-2/23633/20171213113332456_17-2%20Amicus%20Brief%20in%20Support%20of%20Neither%20Party.pdf. This amici brief, spearheaded by former Secretary of Homeland Security Michael Chertoff, currently of the Chertoff Group, has essentially put forward a list of serious consequences which may result in the Court opining on the current state of the SCA applied to extraterritorially-accessed data.

At the outset, the amici note that foreign governments may respond to the Supreme Court’s decision in a move towards more unilateralism in law enforcement access to data. Some governments step up the disclosure requirements in response to SCOTUS’ enabling U.S. law enforcement access to foreign data. Others may seek to legislate prohibitions which “reaffirm their sovereignty over the perceived incursion” and prohibit compliance with such a U.S.-issued SCA warrant. This problem of conflict of laws has, as the brief notes, the potential to actually force companies to close altogether rather than risk dual contempt-like judgments in two countries. For instance, Brazil is currently levying fines against Microsoft’s subsidiary there for failing to provide data to Brazilian law enforcement for fear of violating U.S. law.

Yahoo! likewise has been criminally charged in Belgium for failure to produce records for law enforcement. The brief notes one of the internal problems of the SCA (itself part of the larger Electronic Communications Privacy Act (ECPA)) is that U.S.-based providers, like Yahoo! in the Belgian case, have invoked the Act to argue why they should not be forced to provide data
over. In other words, the ECPA not only gives U.S. its current claimed authority to produce the overseas records, but simultaneously gives U.S. companies a reason not to comply with mirrored provisions in other countries.

Another risk for the Court’s action on this issue is the further movement towards what Jennifer Daskal called, in Law Enforcement Access to Data Across Borders: The Evolving Security and Rights Issues, 8 NAT’L SEC. L. & POL’Y 473, 473 (2016), a “Balkanized internet”, where countries become more unilateral rather than cooperative in requiring evidence. This could be coupled with data localization requirements, mandating “data originating within a country to be stored within the nation’s borders”. Not only does the brief note that data localization has been a tool of authoritarian governments to exercise power over citizens and block international competition, it can present barriers to access to data that would threaten to end the global nature of the internet altogether. Not only did the brief from amici describe the predictable data localization imposed by the Russian and Chinese regimes, data localization efforts by Germany and France have already begun to impact U.S. business decisions.

At its apex of risk, the brief argues that the potential for reductions in cooperation and political poisoning are serious security risks. Like the “going dark” phenomenon in the wake of the Snowden leaks, the cross-border nature need to collect electronic data will be hindered by a patchwork of laws that will hinder cooperation. As of right now, the U.S. receives more data requests from other countries than it makes itself, and a unilateral decision by the court risks jeopardizing cooperation between U.S. and foreign partners.

The brief proposes that the case in question is not the appropriate means by which to fix the failures of the SCA. The SCA, a 1986 act designed to deal with stored communications on outdated technology, is outdated and ineffective against today’s global communications system. The amici propose that Congress, and not the Courts, is the location where the fix needs to come from, especially because it involves balancing of international affairs. The amici point to bipartisan legislation pending before Congress, attempt to address the issue, as well as DOJ’s own draft legislation presented to Congress.

The amici, while expressing no favor for either side, present the parade of horribles from the Microsoft perspective: what will happen if the SCA is applied extraterritorially. But where the amici brief might have even been strengthened further would be to argue the foreseeable problems if the Court upholds the Second Circuit and finds the government cannot access these materials. Not only does this permit the flaunting of court-ordered process by means of storing communication abroad, it further incentivizes a race to the bottom. That some communications may be accessible by the government by means of Mutual Legal Assistance Treaties (MLATs) has been identified in many of the pleadings in support of Microsoft. But here, those supporters are inconsistent: they complain of the anachronism of the SCA compared to modern technology, but insist that the government work through a byzantine treaty process (or an even slower ancestor process to MLATs, letters rogatory) to gain evidence despite the instantaneous nature of cyber, terrorist, and criminal threats that current technology poses to homeland and national security.
The race to the bottom can continue further, with some service providers seeking to avoid government production by placing servers in jurisdictions who will not cooperate with U.S. law enforcement at all. The flags of convenience analogy is apt here: Google has purchased a barge on which it intends to store data. In this situation, as was discussed in the dissents from the Second Circuit’s order denying rehearing en banc, this could leave the communications at issue not only without government compelled process by the U.S., but could likewise leave the communications themselves outside of the privacy protections of the ECPA itself.

On the privacy front, it is worth noting that at no point in this litigation has the issue of the validity of the warrant as to substantiating information been at issue – probable cause supports the production of the stored communications, the issue here has been a fight over where the information has been stored. To find for Microsoft hurts law enforcement and personal privacy because it encourages a “going dark” where privacy of communications would remain at the whim of the foreign entity, and without recourse to the jurisdiction where the criminal conduct is occurring.

These problems are compounded exponentially when cloud data storage is considered – certain processes enable the storage of communications across a host of different jurisdictions. These smaller packets of information cannot constitute anything of evidentiary value absent the others. Without the ability to compel the production of the materials at the point of the user’s access, effectively no jurisdiction would have the ability to access the materials at all, regardless of the level of cause which can be shown.

In light of the dangers of a decision in either direction, policy making is truly the only means by which to alleviate this problem. On the domestic front, the proposed bills typically propose to satisfy the extraterritoriality requirement of the Morrison case law, but to only order production on the basis of the subject of the party or parties involved in the communication itself, rather than being preoccupied on the location of the service provider. Further, an effort is under way for a bilateral treaty framework between the United States and the United Kingdom to address this issue.

In sum, the SCA was an effective framework court processes governing how a prosecutor might access evidence from recording on a off-site voicemail taping service in the possession of a landline telephone provider. Against today’s global communications structure, the most complex and interconnected system ever devised by human beings, its limits have been laid bare. Regardless of the decision of the Supreme Court in light of Microsoft, the privacy and law enforcement implications of the issue of will continue to deteriorate absent legislative efforts, either at the national law or international treaty level.

Timothy P. Zintak is the Chair of the American Bar Association Young Lawyers Division Homeland and National Security Committee, a position he began in 2016. He works as the Assistant Special Prosecutor for the Republic of Palau.
NEWS AND ANNOUNCEMENTS >>

Stay Connected

The American Bar Association Young Lawyers Division Homeland and National Security Committee (ABA YLD HNSC) wants you to stay connected. Please visit these ABA organization’s webpages, join their committees, and subscribe to their email listservs, for all news, events, and topics on Homeland Security, National Security, Military Law, and Government:

ABA YLD HNSC Webpage:
https://www.americanbar.org/groups/young_lawyers/committees/homeland_security.html

ABA Standing Committee on Law & National Security Webpage:
https://www.americanbar.org/groups/public_services/law_national_security.html

ABA Section of International Law: National Security Committee Webpage:
http://apps.americanbar.org/dch/committee.cfm?com=IC905000

ABA YLD Air and Space Law Committee Webpage:
https://www.americanbar.org/groups/young_lawyers/committees/air_space.html

ABA YLD Criminal Justice Committee Webpage:
https://www.americanbar.org/groups/young_lawyers/committees/criminal_justice.html

ABA YLD Government, Military, and Public Sector Lawyers Committee Webpage:
https://www.americanbar.org/groups/young_lawyers/committees/government.html

ABA YLD International Law Committee Webpage:
https://www.americanbar.org/groups/young_lawyers/committees/international_law.html