Microsoft Corp. v. United States of America
829 F.3d 197 (2d Cir. 2016)

ARLETTE NOUJAIM*

BACKGROUND

Appellant, Microsoft Corporation ("Microsoft"), is a multinational technology company headquartered in Redmond, Washington that develops, supports, and sells computer hardware and software services. Among its most common services is its cloud-based email service, Outlook.com, available for use to the public, free of charge. Microsoft stores the contents of each user's emails, email traffic, and other non-content information at datacenters located near the physical location of the customer, as identified by the user upon signing up. Many of these datacenters are operated by the company's international subsidiaries and can be located outside of the United States, such as Dublin, Ireland.

The Stored Communications Act (SCA) provides privacy protection for users of electronic communication services, such as email communication and cell phones, as well as remote computing services, such as computer storage or processing services. The SCA imposes obligations of non-disclosure on service providers such as Microsoft. Section 2703 of the SCA facilitates the process by which the government can obtain other non-content records by a court order issued only upon a statement of "specific and articulable facts showing . . . reasonable grounds to believe that the contents or records . . . are relevant and material to an ongoing criminal investigation".[1] To obtain other user content that is less than one hundred eighty (180) days old, a warrant is required; for older content, a warrant is also required unless the government is willing to provide notice to the customer.

In December 2013, federal law enforcement was piloting a criminal narcotics investigation and sought a search warrant under § 2703. Through this warrant, the government appropriated all contents of an email account belonging to a Microsoft customer without notification to the customer.

The same month the investigation began, a magistrate judge of the U.S. District Court for the Southern District of New York issued the

---

*Ms. Noujaim is a 2017 J.D. candidate at the University of San Francisco School of Law. Her interests lie in the areas of technology, privacy and intellectual property law.

1. 18 U.S.C. § 2703(c)(2), (d) (2012).

government a warrant. However, because the information sought was stored in the Dublin datacenter, Microsoft maintained that the SCA did not apply to customer content held outside the United States. Thus, Microsoft disclosed all the relevant information that was stored in the United States, but moved to quash the warrant with regard to the content stored in Dublin.

In denying Microsoft's motion, the judge reasoned that probable cause, regarding the account's use in furtherance of narcotics trafficking, existed. The judge noted that under the SCA, Congress intended that a warrant served on a service-provider should be executed like a subpoena, meaning information should be produced regardless of its location.

Microsoft unsuccessfully appealed the magistrate judge's decision to a judge of the District Court for the Southern District of New York. After being held in civil contempt for refusing to fully comply with the warrant, Microsoft timely notified its appeal of the district court's decision to the Second Circuit Court of Appeals.

ISSUES

The Second Circuit Court of Appeals was faced with determining whether § 2703(a) of the SCA applied extraterritorially to the provision under which the government, pursuant to a warrant, was permitted to compel service providers to produce the content of certain stored communications. Then, if the initial inquiry was that section 2703(a) does not apply, the court had to determine whether the case at hand involved such a prohibited application.

DECISION

The Second Circuit Court of Appeals determined that the SCA did not authorize a U.S. court to issue and enforce a warrant against a U.S.-based service provider for the contents of a customer's electronic communications stored on servers outside of the United States. Accordingly, Microsoft may not be compelled to produce the contents of a customer's email account stored entirely in Ireland. The court reversed the district court's denial of Microsoft's motion to quash, vacated the finding of civil contempt, and remanded the case to the district court with new instructions.

REASONING

The court of appeals set the tone for its decision to reverse and remand the district court's ruling by asserting that when Congress passed the SCA, its aim was to protect user privacy in the context of developing technology that increased a user's interaction with a service provider. The court noted that today international lines are crossed

much more regularly and service providers rely on such worldwide networks of hardware, including datacenters, to satisfy customers' growing expectations of privacy. Accordingly, Congress' focus in passing the SCA was to provide privacy safeguards for local users. With this tone in mind, the court focused its attention on analysis of the SCA and the Supreme Court's decision of *Morrison v. Nat'l Australia Bank Ltd.*[2]

The court looked to *Morrison* to see if Congress intended the warrant provisions of the SCA to reach beyond the United States.[3] The approach set forth in *Morrison* indicated that in order to determine whether the reach of a statutory provision was limited to the United States,[4] the court must first determine whether extraterritorial application is contemplated by the provision, as indicated by the language and legislative history of the statute.[5] If it is not, the court then considers whether the government's questioned application was extraterritorial; and therefore, outside the statutory limits.[6]

As to the first inquiry, the court concluded that the warrant provisions of the SCA did not contemplate or permit extraterritorial application. The provisions in the SCA, and even those in the Electronic Communications Privacy Act (ECPA), which is the SCA's bigger statutory framework, did not mention any extraterritorial application, either explicitly or implicitly.[7] The court confidently stated that if Congress intended a law to apply outside of the United States, it would have given an affirmative individuation of its intent, just as it had in other statutes.[8] The government asserted that nothing in the SCA's text, purpose, or legislative history indicated that compelled production of records was limited to those stored in the United States. However, the court noted that this claim was directly contradictory to the presumption in *Morrison,* indicating that U.S. laws were presumed to only apply domestically, unless otherwise stated or implied.

Furthermore, the term "warrant" as used in § 2703 of the SCA, was one used in the Constitution as connected to privacy concepts applied within the territory of the United States. The court indicated that the SCA's legislative history supported the use of the term "warrant" in the SCA with all of its traditional, domestic inferences.

The court rejected the government and district court's approach regarding the treatment of a warrant under the SCA as akin to a subpoena. Nothing in the provision suggested that the terms should be used interchangeably; and thus, they remained legally distinct. As a

2. *See generally* 561 U.S. 247 (2010).
3. *Id.* at 255.
4. *Id.*
5. *See* Microsoft Corp. v. United States, 829 F.3d 197, 210 (2016).
6. *Id.*
7. *Id.* at 211.
8. *Id.*

result, the court concluded that Congress did not intend the SCA's warrant provisions to apply outside of the United States.

As to the second inquiry set forth by *Morrison*, whether the case at issue involved such prohibited extraterritorial application, the court was faced with determining whether the execution of the government's warrant 'was contradictory to the SCA's primary focus. If so, the warrant would constitute an unlawful extraterritorial application of the SCA. In making its decision, the court considered the text and plain meaning of the statute, its legislative history, and its framework.

The court noted that the SCA's language focused on the privacy of stored communications. This conclusion was supported by the title language of the SCA's parent Act, the Electronic Communications *Privacy* Act of 1986. Furthermore, other aspects of the statute, such as the prohibition on any alteration or blocking of access to stored communications, protected the integrity of communications; and thus, protected the privacy interests of users from intrusion by unauthorized parties.[9]

Finally, the court concluded that the SCA's legislative history focused on privacy, as Congress noted that the acts of private parties were unfettered when it came to the privacy of their stored communications. In addressing the government's access, Congress sought to ensure that the protections afforded by the Fourth Amendment extended to electronic mediums through the SCA.[10] Thus, having determined that the SCA focused on user privacy, the court concluded that the execution of the warrant, insofar as it directed Microsoft to seize the contents of its customer's communications stored in Ireland, would constitute an unlawful extraterritorial application of the SCA.

9. *Id.* at 217.
10. *Id.* at 219.