wiley

NEWSLETTER

Microsoft and Dahda: The Supreme Court Agrees to Hear Two New Cases Balancing Security and Data Privacy

November 2017

On October 16, 2017, the Supreme Court of the United States granted certiorari to review two surveillance cases that implicate territorial jurisdiction, international data transfers, and forced data localization. These cases could dramatically shape how the lower courts construe the contours of Title III of the Omnibus Crime and Safe Streets Act of 1968 (Title III) and the Stored Communications Act (SCA). More broadly, the cases will allow the Supreme Court to weigh in on the proper balance between data privacy and criminal investigations in the information age.

Practice Areas

Privacy, Cyber & Data Governance

The Cases

United States v. Microsoft Corp., No. 17-2

In *Microsoft*, the Court will address whether an email services provider must comply with a warrant supported by probable cause under the SCA when the email records are stored outside of the United States.

In 2013, a federal judge granted the government's warrant request that required Microsoft to disclose information about an email account that law enforcement believed was being used for drug trafficking. The government obtained the warrant pursuant to the SCA, which authorizes the government to obtain email records when it has a warrant supported by probable cause to believe a crime is being committed. The warrant was served on Microsoft at its headquarters in Redmond, Washington. Microsoft refused to comply, arguing that the SCA did not apply because the emails were stored in Ireland.

The trial court ordered Microsoft to turn over the information, but the U.S. Court of Appeals for the Second Circuit reversed and refused to enforce the warrant. The court held that the term "warrant" in the SCA neither explicitly nor implicitly envisions the application of its warrant provisions overseas. According to the court, the government's interpretation of "warrant" would require courts to disregard the "strong and binding" presumption against extraterritoriality recently emphasized by the Supreme Court. In light of what it interpreted as the SCA's plain meaning and other statutory characteristics, the court held that in passing the SCA, Congress was focused on protecting users' privacy and did not intend for the SCA's warrant provisions to apply extraterritorially.

Notably, the Supreme Court granted certiorari even though there does not appear to be a circuit split on the issue. The Court has not yet scheduled oral argument.

Dahda v. United States, No. 17-43

In *Dahda*, the Court will determine whether Title III requires courts to suppress evidence obtained pursuant to wiretap orders that are facially insufficient because they exceed a court's territorial jurisdiction.

Twin brothers were charged with conspiracy to distribute illegal drugs. The government obtained evidence by wiretapping several cell phones pursuant to nine wiretap orders issued by the U.S. District Court for the District of Kansas. Under Title III, a judge can issue a wiretap order to intercept communications within the territorial jurisdiction of the court on which the judge sits, but courts can suppress evidence if the order is insufficient on its face. The wiretap orders authorized the use of a stationary listening post in a neighboring state. The defendants argued that the order was insufficient on its face because it allowed the government to intercept communications even when the wiretapped phones were outside of Kansas. The trial court admitted the evidence, and the defendants were found guilty.

The defendants appealed to the U.S. Court of Appeals for the Tenth Circuit. The Tenth Circuit held that the wiretap orders were insufficient on their face because under Title III "interception" occurs both at the tapped phones' locations and where law enforcement positions its listening posts. Because the orders did not geographically restrict the phones' or listening posts' locations, the orders allowed the government to intercept communications outside of the court's territorial jurisdiction.

The court nonetheless held that the wiretap evidence was admissible because the territorial defect did not affect Title III's chief underlying concerns – privacy and uniformity. The territorial limitation appears in neither the congressional examples of the Act's privacy protections nor in the Act's legislative history. The court reasoned that the territorial requirement would also undermine the goal of uniformity by requiring prosecutors in multiple jurisdictions to coordinate their electronic surveillance use. Thus, even though the wiretap orders were insufficient on their face, violation of the territorial requirement did not require evidence suppression.

Justice Neil Gorsuch, who was scheduled to sit on the Tenth Circuit panel that heard oral arguments on the brothers' case, has recused himself. The Court has not yet scheduled oral argument.

Why These Cases Matter

Microsoft and *Dahda* add two important cases to this term's Supreme Court docket, which is shaping up to be one of the most consequential in the Court's history when it comes to balancing data privacy and security interests. Already, the Court will decide in *Carpenter v. United States* whether the Fourth Amendment permits the warrantless seizure and search of historical cell phone records revealing a person's location and movement over a period of 127 days.

Microsoft could be particularly consequential. Since the Second Circuit's ruling, the government has argued that the decision is causing "immediate, grave, and ongoing harm to public safety, national security, and the enforcement of our laws." The government fears that the ruling might chill cooperation between law enforcement and companies that store consumer data. Indeed, it argues this has already begun, claiming that "[t]he major domestic Internet providers aren't treating the [decision] as just a decision from one circuit. They have all decided to treat the decision as the law in effect everywhere." Law enforcement claims that if more companies use *Microsoft* to justify noncompliance with warrants, investigations into matters such as terrorism, child exploitation, drug trafficking, tax fraud, and sex trafficking will be stifled.

In response, Microsoft has argued that "[t]he current laws were written for the era of the floppy disk, not the world of the cloud." Microsoft President and Chief Legal Officer Brad Smith would like Congress to respond by enacting new legislation. Microsoft has voiced support for the International Communications Privacy Act of 2017, a bill introduced in July that would provide "sensible ways for cross-border data access." State law enforcement officials have strongly supported the federal government's position, with 33 states urging Supreme Court review.

Disputes between leading technology companies and the U.S. Justice Department centered on the balance between privacy and security have become increasingly common. Last year's high-profile dispute between Apple and the FBI over whether Apple had to help law enforcement hack into an encrypted iPhone threatened to push the issue to the forefront. The debate was stalled when the FBI withdrew its request after claiming that a third party assisted in unlocking the phone. Along with *Carpenter*, *Microsoft* and *Dahda* will give the Court an opportunity to finally weigh in on how to balance companies' desire to protect collected data and law enforcement's mandate to investigate crimes in an increasingly data-driven world.

Shawn M. Donovan is a law clerk in Wiley Rein's Telecom, Media & Technology Practice.