

Microsoft Corp. v. United States: Jeff Sessions Wants Open Borders, But Only for Police

On October 16, Morgan Chalfant of *The Hill* reports, “the US Supreme Court agreed to hear the Justice Department’s appeal in *Microsoft Corp. v. United States*.” The question before the court: Are search warrants issued by American courts valid abroad?

In 2013, Microsoft refused to turn information from a customer’s email account over to law enforcement pursuant to a warrant in a narcotics investigation. The information, Microsoft noted, was stored on a server in Ireland. Ireland, as you may have learned in elementary school, is neither one of the fifty states nor a US territory. It’s a sovereign state with its own laws. US search warrants carry no weight there.

A three-judge panel of the US Court of Appeals for the Second Circuit sided with Microsoft, and the full court denied the government’s request for a rehearing. Apparently they learned geography as youngsters, too.

US Attorney General Jeff Sessions, maybe not so much. But he does seem to have a perpetual burr under his fur about “national sovereignty.” Sessions is on record criticizing both “illegal immigration” (under the US Constitution there’s no such thing) and the Trans-Pacific Partnership trade agreement as attacks on US sovereignty. So why is the Justice Department he leads seeking a declaration from the US Supreme Court that US search warrants override the sovereignty of Ireland? American exceptionalism much?

Hopefully the court will uphold the Second Circuit’s decision and make it clear to Sessions that the whole border/sovereignty thing goes in both directions.

But the tech sector and individuals who value their privacy shouldn’t just sit still and hope for the best. What we need is a the continued erosion of “national” borders and the perfection of individual borders that are, as a practical workaday matter, mostly impenetrable to people like Jeff Sessions. While the former may take some time yet, the latter are already partially available and the unavailable part represents opportunity for reasonably entrepreneurial “sovereign states.”

The available part, as you might guess, consists of strong encryption. The sooner Microsoft and other email and data storage providers implement well-crafted end-to-end encryption for their users — encryption the providers do not hold the keys to — the sooner the data in question will become useless to the Jeff Sessionses of the world. “Oh, you have a warrant? OK, fine, here’s what you asked for. Good luck reading it.”

The unavailable part consists of (hopefully more than one) “data haven” states: Countries

whose governments are willing to write strong data privacy and freedom protections into their laws, believably commit to sticking with those protections, then stand back and watch as Microsoft, Google, Facebook, et al. build huge data centers and perhaps even decide to re-domicile themselves (presumably paying lots and lots of taxes in both cases).

Sometimes the Supreme Court gets things right, but it's definitely an imperfect and untrustworthy vessel to entrust with the protection of our privacy and our rights. Better to take those rights into our own hands with encryption, and decentralize their protection across friendly sovereignties.