# The United States vs. Apple and Microsoft: The Makings of a Perfect Storm

Jeffrey Blatt
Of Counsel
jeffrey.b@tilleke.com

Last month, a U.S. court in California issued an order to Apple that was metaphorically equivalent to a magnitude 9 earthquake cutting through the Silicon Valley. The order shook the tech world to its core, requiring Apple to write code to bypass a security feature of its product to allow a brute force password attack by the FBI to unlock an iPhone used by one of the terrorists killed by police after the San Bernardino attack in December 2015. That order, and the subsequent filings by the U.S. Department of Justice (DOJ), Apple, and amicus curiae (friend of the court) briefs by tech giants including Microsoft and Google, have resulted in the merits of the case being debated around the world, both for and against the DOJ and Apple. In a surprise move, on March 28, the DOJ requested the court to withdraw the order saying that it had successfully accessed the data on the iPhone and no longer needed Apple's assistance.

Although the San Bernardino case will not proceed, the issues are far from resolved. Apple has said it will take steps to enhance the security of its products and plug the security vulnerabilities the FBI may have used to access the locked iPhone. The battle will now move to the next level. In the absence of technical alternatives, the U.S. government will continue to attempt to compel Apple and other tech companies to provide access to the digital devices we rely on to store our most sensitive personal and business data, including phones, tablets, and laptops. Without new legislation, the DOJ would be compelled to again argue that the court has the authority to require a tech company to assist the government under the "All Writs Act" (a U.S. law on the books since 1789).

Notably, in the San Bernardino case, Apple had already provided the FBI with the phone data that was stored on the iCloud, and Verizon has released the call details and location tower data (i.e., data pointing to where the phone was). Apple could provide data stored on the iCloud because Apple holds the encryption keys for data stored in their cloud. What the government sought was *any other* data that may only reside in the phone and was not backed up to the iCloud.

While the Apple case received a lot of press, there is another case pending that is, in many ways, just as important. The combination of these two cases and the U.S. government positions that they reflect may create a "perfect storm" defining how tech companies must walk a tightrope between protecting digital privacy and cooperating with governments around the world that demand access to our data.

That "other" case has the rather long title of "In the Matter of Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation" (we just call it the "Microsoft" case), and it is currently on appeal to the U.S. Court of Appeals for the Second Circuit. The DOJ

is seeking, through a search warrant issued to Microsoft U.S.A., e-mails stored on a cloud server at a Microsoft subsidiary in Ireland. This compelled disclosure to the DOJ would violate Irish law, and would not follow the established procedures required in an existing law enforcement assistance treaty between the two countries.

The DOJ argues that a U.S. search warrant issued to a U.S. cloud provider covers emails no matter where it is stored on the planet. Microsoft is refusing to comply, arguing that a U.S. warrant is only valid in the United States. If the DOJ wants data stored in Ireland, Microsoft contends, it needs to follow established international procedures. The DOJ apparently does not want to jump through those hoops.

If the DOJ prevails, the U.S. government can reach anyone's emails and documents stored on any cloud provider that the United States can assert jurisdiction over. So as strange as this sounds, a Thai company, using a cloud service provider for its corporate email handling based in Singapore, may find that its emails are divulged to the U.S. government without going through any legal process in Singapore (perhaps in violation of Singapore law) if the cloud provider has a sufficient presence in the United States. If the United States can get away with this, then why not China, the United Kingdom, or any other government that can assert jurisdiction? A decision in favor of the DOJ would change the risk profile for businesses around the world when deciding whether to use the cloud.

The tech community has rallied behind Microsoft and filed dozens of friend of the court briefs, including Apple, Amazon, and the Government of Ireland. As of this writing, the U.S. Second Circuit Court of Appeal has not issued a decision.

Just as ocean waves interact with each other with some becoming bigger, smaller, or cancelling themselves out, the potential combination of outcomes, in terms of the escalating battle between the U.S. government and Apple and the decision in the Microsoft case, can form a perfect storm in terms of both best and worse outcomes depending on one's view.

A "perfect" outcome for the DOJ would be for Microsoft to lose and be forced to compel its Irish subsidiary to divulge its customer's e-mail, and for either Congress to mandate that a "back door" be built into encrypted products or for a court to again order a tech company to write code to compromise its own product (and for that order to be upheld on appeal). This perfect storm scenario for the United States would dramatically affect our expectations of privacy for data in our portable devices and in the cloud. Other governments would take similar actions to compel the disclosure of data on devices and in the cloud of those they choose to investigate.

However, if Apple and Microsoft ultimately prevail in their positions, we would feel more confident that our data is more secure. Business models for tech companies would evolve accordingly, but that outcome would most assuredly tempt Congress and governments around the world to consider specific legislation.

A "win" by Apple or Microsoft, and a "loss" by the other, would have other ramifications. If encrypted data on a phone is safe from government access, but governments can reach data in the cloud regardless of where in the world the data is located, a security-conscious company may well opt to store their sensitive data locally and not on the cloud. Governments may then be tempted to compel cloud backups for portable devices and require cloud-service providers to hold the encryption keys. Other outcomes will result if Microsoft prevails but Apple loses in its battle to keep its products secure from others including government agents.

The waves are still in motion. For legal advisors and business executives, the current situation presents serious challenges in making decisions regarding business and legal risk management. Some government access to our data is a fact of life, but to make conscious decisions we need

to understand where the limits are. The only certainty is that the outcomes of these cases will affect our personal and business decisions in how we protect our data for years to come.


Supalai Grand Tower, 26th Floor, 1011 Rama 3 Road, Chongnonsi, Yannawa, Bangkok 10120, Thailand
T: +66 2653 5555 F: +66 2653 5678 E: bangkok@tilleke.com