Reevaluating China - Is it time to ban all Chinese tech over privacy, security and moral concerns?

August 20, 2020 - Over the past couple of years or so, the White House has been busy banning certain Chinese technology companies from doing business in the United States. You may think that the administration's moves are unwarranted or, at the very least, inconvenient. But there really are some things that everyone should consider before going anywhere near Chinese tech.

Tweet

(function() {
var s = document.createElement('SCRIPT'), s1 = document.getElementsByTagName('SCRIPT')[0];
s.type = 'text/javascript';
s.src = 'http://widgets.digg.com/buttons.js';
s1.parentNode.insertBefore(s, s1);
})();

(function() {
var po = document.createElement('script'); po.type = 'text/javascript'; po.async = true;
po.src = 'https://apis.google.com/js/plusone.js';
var s = document.getElementsByTagName('script')[0]; s.parentNode.insertBefore(po, s);
})();

The Trump administration's push against these companies really started with the telecommunications giant Huawei. That particular company is a leader in 5G technology, as well as telephone handsets. Unfortunately, because they are located in China they are also a national security concern. That's because Chinese law requires all corporations to cooperate with the Chinese government - meaning the Chinese Communist Party (CCP).

And whether or not you think of it that way, the US telephone network you use every day, is a strategic American asset - especially during military conflicts - which the US Government will do pretty much anything to protect. Allowing a Chinese company to embed technology in that network - no matter how good (or cheap) that technology may be - would be foolhardy for any government that wants to protect that particular asset. Hence the ban on Huawei.

Just think about what travels over that phone network. All internet communications run through it. That means billions of financial transactions daily would be at risk. The military uses it for everything from the mundane to strategic information transfer. Banks, other government agencies, defense contractors, etc... Virtually every aspect of modern daily life in the United States merges with the telephone network here on a daily basis; either through voice calls or data transfers. If Chinese tech is a part of that picture, it's an open invitation to China to collect data on Americans and American business.

But Huawei is far from the only Chinese tech company doing business in the United States. Some of the most popular cell phone apps available come from China. These include TikTok and WeChat. Maybe Huawei builds telecommunications infrastructure, but if you can put a Chinese app on your otherwise non-Chinese phone, China may be able to accomplish pretty much the same thing. After all, app makers can collect a lot of data on the people using their apps. And tens of millions of Americans are using both TikTok and WeChat, as well as others.

That hasn't gone unnoticed. The White House has given the parent company of TikTok a timeline to sell their American operations or close down. And they have now given notice to WeChat that they need to halt operations in the United

States by September 20th.

If you think this is overblown, then consider this. A Chinese company by the name of DJI has more than 70% of the US market share for personal and commercial drones. Yesterday, the Heritage Foundation published a report on DJI which highlighted findings made by researchers at Synacktiv; a French cybersecurity firm. They reverse engineered DJI's phone app for controlling drones in flight and found that the app was collecting huge amounts of information and then transmitting it back to China. The information included location details as well as everything necessary to clone the phones which the app is installed on. None of that information is relevant to flying their drones.

None of this should really be a surprise. The US Government has banned the use of several Chinese apps, as well as the use of drones manufactured in China over security concerns. There is a legitimate fear that this technology will be used to provide the CCP with details and location information on American critical infrastructure projects. If the DJI application is any indication, that fear is actually a reality that is already going on.

The truth is that the federal government should probably ban all technology built in China including phone apps. Just think about it. There is a great deal of photographic equipment made there, and much of that comes with phone apps. If you have one of those apps on your phone, it's reasonable to assume that someone in China has the ability to look at any pictures you take. Moreover, they will know where you were, when you were there and there is an excellent chance that they may be able to find out who you were with at the time. That may not be important if you are taking a picture of the Grand Canyon. But what if you are taking a picture of a document with all of your personal information on it? Or what if the phone is being used by a government agency and has access to data that isn't in the public domain?

If none of this convinces you, then consider one last thing. Purchasing products made in China supports some things that are very bad from pretty much any perspective. Suppression of political expression in Hong Kong. Prison camps for the Uighur people - there are reportedly 4 million people in these so-called "re-education" facilities. Forced labor to manufacture goods cheaply. Live organ harvesting from political dissidents - including taking the hearts of people who are still alive - for transplantation. Buying Chinese is supporting genocide. In 1945, the world said, "Never again!" Well, here we are again.

Nobody needs TikTok, WeChat or Huawei. Nobody really needs a cheap TV or phone. It's time for Americans to start reading labels again. While we'd like to see more of them that read "Made in the USA," right about now we'll settle for "Made anywhere but China."
by Jim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.

Follow ACCESS