"figure out a way to square that circle"
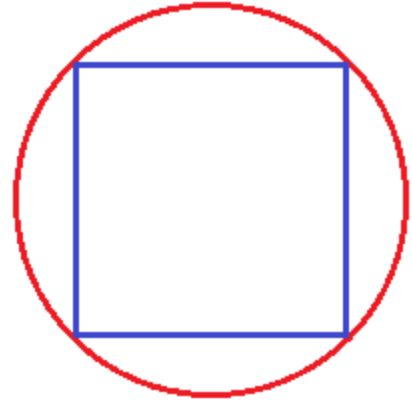
By Joe Chiarella

July 25, 2018

On July 19, 2018 NBC News' Lester Holt interviewed FBI Director Chris Wray at the Aspen Security Forum. If you watch this video (time segment 34:32 through 37:41) you can see for yourself how Wray addresses the topic of law enforcement having access to encrypted data. You can also read the transcript here (see page 13).

I like Wray and share his desire to protect our citizens. I'll even go so far as to say that I wish there was a way to guarantee lawful access to encrypted data, while also not allowing unlawful access. But Wray is slightly misguided. This is not about technology. Cryptography is about math and math can be pretty absolute. In fact, his comment that we have to "figure out a way to square that circle," ironically a math reference in itself, testifies to the irrationality of the approach.

A hole in the math, is a hole. The math cannot tell the difference between a lawful request and an unlawful one. And if it could, an unlawful actor need only fool the math to believe it is a lawful actor and... So, everyone ends up going through the hole. Wray's position, as with others in our government (again, I'm convinced are well intentioned) is puzzling.

Still, if we accept Wray's assertion that it is a solvable problem, then that brings me to the question I am writing about today.

Why is the government positioning Silicon Valley as the group to solve this problem (and why are we allowing them to frame it that way?)? The best and largest collection of cryptographic math minds in the solar system reside near Ft. Meade, Maryland at the NSA (and perhaps some at NIST as well). Why don't the FBI, DOJ, DOD, DIA, CIA and all the other TLA organizations ask their fellow national security colleagues at the NSA (or NIST) to solve the problem? If it is solvable - they are our best chance to solve it. And if they can't, can we stop trying to "square a circle"?