BRACEWELL

BLOG POST

The Pit and the Pendulum

October 21, 2014

There's a fight going on right now between companies and the government, and it goes something like this:

Government: "We want to make you more safe!"

Company: "No way. We'd like to put our customers at risk. Thanks!"

Wait. That doesn't sound right. Maybe's it's more like this:

Government: "We'd like to invade your privacy."

Company: "No way. We'd like to protect our customers from government spying. Thanks!"

That doesn't really sound right, either, does it? But that's basically the tension that we are seeing right now: the classic standoff between privacy and security.

Economists like to call it a zero-sum game, where one side's gain directly correlates to the other side's loss. But economists are weird people and always want to assume things that aren't necessarily there, so I'm going my own way. (Three economists went hunting and came across a deer. The first economist fired and missed by one foot to the left. The second economist fired and missed by a foot to the right. The third economist didn't shoot but shouted, "We got it!")

I like to think of this tension as a pendulum, with liberty on one side and privacy on the other. When the pendulum swings towards security, then more and more privacy interests are sacrificed for security. And vice versa.

In mid-September, ***Apple issued an open letter*** about its commitment to privacy. One of the company's key points was that the encryption of its new mobile operating system, iOS 8, prevents anyone but the end users to access the content of their iPhones or iPads that are running the system. The takeaway point? Well, ***let's just ask Apple itself***: "On devices running iOS 8, your personal data such as photos, messages (including attachments), email, contacts, call history, iTunes content, notes, and reminders is placed under the protection of your passcode. Unlike our competitors, Apple cannot bypass your passcode and therefore cannot access this data. So it's not technically feasible for us to respond to government warrants for the extraction of this data from devices in their possession running iOS 8."

Google's newest Android operating system ***is going to offer encryption as well***. Google previously offered encryption as an option, but will now apply it by default. (Q: Why did the Stormtrooper choose an iPhone? A: Because he couldn't find the 'Droid he was looking for.)

There's a lot to, well, decrypt, here. First, ummm, wow? Can you imagine what the reaction would have been like if a company had done this the day after the 9/11 attacks? Because that was really when the pendulum had taken the hardest swing to the security side, resulting in the passage of the Patriot Act just six weeks after the attacks. No company would have wanted to be perceived as shielding potentially vital information from the government. Now though, with most people far less fearful of terrorist attacks, Apple is able to use the shielding of information from the government as a marketing ploy – and Google immediately matches.

Second, much of the focus on privacy and governmental requests for information comes from the NSA spying revelations of Edward Snowden, which has the ***general tenor of public opinion decrying government surveillance programs*** while creating a cottage industry of Snowden- and PRISM-related stories. But while the broad-based approach of the NSA has fueled the public sentiment, ***the real impact of encryption*** will be felt by the police officers and federal agents who are investigating non-terrorism cases and who have historically relied on Constitutionally-permissible searches based on a warrant that is obtained by making a showing of probable cause to a judge.

How would this impact investigations? ***Many real-life examples***. Here's a hypothetical: A Starbucks employee calls the police after two independent customers have complained that a man in the coffee shop is viewing what is clearly child pornography on an iPad. When detectives arrive and ask to see the iPad, which runs iOS 8, the device it turned on but requires a password for access. The man declines to provide a password and asks for an attorney.

Now what? Since Apple encrypted its devices, what can the detectives do? And what if the man is part of a child pornography ring – aren't linkages that would otherwise appear on the iPad now lost? Apple's take – and Google's take – is that the privacy concern is paramount.

What's your take?

This kind of situation is why ***the Attorney General*** and ***the FBI is adamantly against*** what Apple and Google have done. It's why people like John J. Escalante, chief of detectives for Chicago's police department, say, "***Apple will become the phone of choice for the pedophile***. The average pedophile at this point is probably thinking, I've got to get an Apple phone."

Is there a happy medium? Most everyone agrees that building a law enforcement back door into iOS 8 or Android is a bad idea, and one that will lend itself to exploitation by determined hackers. ***The Washington Post's Editorial Board***, which calls for a balance between security and privacy interests, offers that, "with all their wizardry, perhaps Apple and Google could invent a kind of secure golden key they would retain and use only when a court has approved a search warrant."

A magical golden key. Riding on the back of a unicorn? C'mon. Be serious.

There really is no good answer here. Security and privacy do not coexist well together. And on either side of the pendulum, there is a deep, dark, and perilous pit.