Reasons not to help FBI crack iPhones

**By Hiawatha Bray** GLOBE COLUMNIST

America is in a populist frame of mind this election year, making it a lousy time to root for Apple Inc.’s chief executive, Tim Cook. He’s a millionaire a few hundred times over, a Silicon Valley liberal whose company has parked about $200 billion in profits outside the United States to avoid paying taxes on them. In short, Cook’s the sort of guy that Republicans and Democrats alike can merrily despise.

Worse yet, Cook is the sort of guy who says no to the FBI, as it investigates last year’s brutal terrorist attack in San Bernardino, Calif. His refusal to allow investigators to look at the data locked in the cellphone of a terrorist could undermine the security of Apple’s flagship product, the iPhone, but it also could deprive the FBI of vital evidence.

It’s the latest in a series of showdowns between the feds and the tech industry over when and how the government should get access to data we don’t want anyone to see. By taking a stand now, when it hurts, Cook could go a long way toward protecting Americans’ privacy for a long time to come.

On Tuesday, a federal magistrate judge in California ordered Apple to help the FBI break into an iPhone 5C used by Syed Rizwan Farook, who along with his wife murdered 14 people in San Bernardino in December. The massacre was reminiscent of the far bloodier November 2015 Paris rampage, carried out by supporters of the radical group Islamic State. But so far, there’s no evidence of a connection to the Islamic State or any other terrorist group.

Still, the FBI wants to make sure by reviewing passcode-protected data locked in Farook’s iPhone. Investigators might find e-mails, photos, maps — a horde of documents that might reveal direct links to other bad guys, here or abroad.

The iPhone 5C, released in 2013, originally featured a version of Apple’s iOS operating system that was relatively easy to hack. But since 2014, Apple has released two upgrades, iOS 8 and iOS9. These programs encrypt all data stored on the phone and on newer models, using a system so tough it’s supposed to be unbreakable — even by Apple itself.

The second piece of Apple’s security is the passcode. The operating system has a feature that limits the number of incorrect numerical codes that can be entered. Punch five incorrect codes into your iPhone, and you’ll have to wait one minute before trying again. As an even tougher option, users can set a self-destruct feature. At 10 misses, all files are deleted. (The FBI has no way of knowing whether Farook turned on this option.)

In October, in response to a similar demand filed by FBI agents in a New York drug investigation, Apple said that it couldn’t possibly comply. “For devices running iOS 8 or higher, Apple would not have the technical ability to do what the government requests,’’ according to a document filed by Apple’s legal team.

The California court order suggests this wasn’t quite true, or that the government has recently uncovered a weak spot in the iPhone’s defenses. Magistrate Judge Sheri Pym’s order indicates that she believes Apple can crack its own phones, and it lays out a plan of attack.

Pym wants Apple to create a customized version of its operating system, designed to run on Farook’s phone and no other. This software will be somehow injected into the phone without interfering with any other data stored on it. It will then deactivate the feature that limits the number of incorrect passwords that can be entered.

The judge also wants Apple to add software that lets the FBI rapidly feed multiple passwords into the phone. Apple would retain a fig leaf of credibility, because the company wouldn’t actually crack the iPhone’s encryption, which scrambles data so that it can’t be read by hackers. Instead, it would lower the phone’s passcode defense, so the FBI could launch a “brute force’’ attack — trying millions of possible passwords until something clicks.

In an open letter published on Apple’s website Wednesday, vowing to appeal the court order, Cook never denies that Apple is capable of doing what the court demands; he merely warns that such a program is “something we consider too dangerous to create.’’

And Cook is right.

Does anybody believe that this tool will be used just this once? The USA Patriot Act, created to fight terrorism, was deployed against all manner of common criminals. Create an iPhone hacking tool, and every police force in America will want a copy. Why would any judge refuse?

For years, US technology companies have resisted demands from thuggish nations like China that want backdoor access to their products, so they can spy on subversive citizens. If companies give in over here, expect similar pressure from over there.

If Pym’s order stands, every US tech company is one court order away from sacrificing its customers’ privacy. American firms could lose billions in sales as consumers worldwide seek out alternative products from companies that US courts can’t touch. The popular secret-message program Telegram, for example, comes from Germany; the file encryption software maker Silent Circle is based in Switzerland. Good luck with those subpoenas.

The files on Farook’s phone may or may not contain valuable evidence. But the phone has already told investigators who Farook called and when, as well as the Internet sites he visited. That data, which could identify other terrorists, is on file, unencrypted, at the phone company, available to any police officer with a court order.

The Apple-FBI clash looks like the biggest pitched battle yet in a decades-old conflict between tech innovators and police. In the 1990s, the Clinton administration tried to outlaw encryption altogether, giving up only when it saw that such a ban wasn’t enforceable. More recently, the FBI has begged Congress for laws requiring “back doors’’ in encryption software, to let the agency monitor suspicious communications that would otherwise be indecipherable.

But the techies rightly reply that back doors swing both ways. They’re open to police, but also to vandals, criminals, even terrorists. A court order forcing Apple to crack open its system would make iPhones less secure. And legally, it could set a precedent from which our digital privacy may never fully recover.

So much for populism. This time, I’m rooting for the rich guy.

*Hiawatha Bray can be reached at hiawatha.bray@globe.com. Follow him on Twitter @GlobeTechLab.*