1050 17th Street, N.W.
Suite 1150
Washington, DC 20036
202.525.5717

Free Markets. Real Solutions.
www.rstreet.org

Statement for the Record

Before: Reps. Ted Poe, Pete Olson and Blake Farenthold

April 11, 2016
Baker Institute, Rice University

Mike Godwin
Director of Innovation Policy and General Counsel
R Street Institute

Encryption: Balancing the Needs of Law Enforcement and the Fourth Amendment

My name is Mike Godwin and I'm director of innovation policy and general counsel for the R Street Institute, a free-market public-policy think tank based in Washington. I'm also a native Houstonian, and I like to think my commitment to liberty on the internet has grown out of my strong Texas roots. I want to thank the Congressmen for giving me the opportunity to come back to Houston to talk about encryption and the Constitution.

As we all know, encryption and digital-security measures have been in the news a lot lately, thanks to the recent disagreements between the FBI and Apple I want to stress at the outset that, for the most part, neither Apple nor anybody else who disagreed with the FBI's insistence that Apple help hack their own digital security in the San Bernardino terrorist case believes that particular case represents a Fourth Amendment issue. The owner of the iPhone in that case was not the suspect, but the suspect's employer. That employer gave consent for the phone's search. So there's no Fourth Amendment issue with regard to that particular phone.

But the larger issues raised by the case do implicate the Fourth Amendment. Speaking as a constitutional lawyer, I naturally want to talk about what those implications are. Please forgive me in advance—I may talk about other amendments today as well, but we're here to talk about the Fourth Amendment:

> *The right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.*

These days, I often hear the argument that the Fourth Amendment is just about warrants and the requirement that they be particular, and not so-called "general warrants." But let's diagram the Fourth Amendment, as my Houston Independent School District teachers required me to do with a lot of sentences when I grew up here. The Fourth Amendment turns out to be two independent provisions. The first provision, which is about security and reasonableness, is arguably more important than the second, which is just about warrants.

Given the breadth of the first part of the Fourth Amendment—which uses words like "secure" and "unreasonable" that are meant to be understood broadly – we can reasonably guess that what the FBI wants now is something the Fourth Amendment's authors never contemplated.

Should our government mandate the kind of profound, extensive backdoor access to every aspect of our personal lives that would be made possible when companies are compelled to hack our security for the FBI? Should we give our police secret keys that unlock everything we might say or do on our smartphones?

And here, I'm not just talking about Apple, Facebook and Google,

but also about smaller companies that provide us with a range of digital-security tools we may use with our devices. These companies may not have the muscle to challenge an insistent FBI, even when they think they're in the right to provide citizens with real digital security.

But the FBI, and other government agencies at the state and federal level, have argued in court—and likely will continue to argue in court—that the need to investigate crime or thwart terrorism requires us to give the government guaranteed access to the backdoors of our digital lives. What's more, they are asking Congress to step in and establish those rights as a matter of statutory law. This is what the anti-encryption draft legislation introduced last week by Sens. Richard Burr and Dianne Feinstein would do.

We at the R Street Institute believe Congress should act now, as it has before, to secure our rights against government demands to access our every secret thought. As intimately connected as we are to our smartphones today, it's likely that we'll be even more intimately connected to whatever technologies help us in our daily lives in the future. There are people in this room today who will live to see digital technologies in their very bodies, helping them recover from injuries or illnesses. Do we really think the FBI or a federal magistrate should have the power to enable government to hack these digital devices inside us?

The FBI and some other law-enforcement agencies seem to believe the Fourth Amendment grants the government a fundamental right to succeed in every investigation on which it embarks. This is wrongheaded; the amendment is supposed to operate as a limit on government power, not to grant a right to investigatory success

Remember, the amendment protects:

> *The right of the people to be secure in their persons,*

houses, papers and effects

It's a right "of the people," not a right belonging to the FBI, the IRS, the Securities and Exchange Commission or to local or state police. It's not a right that disappears when there's a big, important case or investigation going on.

Should Congress mandate that our digital devices be made hackable and snoop-able by every government entity in this country? One reason they shouldn't is that doing so would effectively empower every other government entity in the world that might have jurisdiction over Apple, Google, Microsoft, etc. to compel the same intrusion. Why should any of us ever trust digital tools and digital commerce if our government insists that any company we buy from must be able to create burglar tools for the FBI? In the digital age, when we keep our whole lives on our computers and phones, this mandate meets every definition of "unreasonable."

Now, please note: I'd mention briefly that other Bill of Rights protections are raised by the question of whether government should be able to compel companies to provide backdoors into the digital-security technologies that all of us use.

Obviously, the First Amendment is important when it comes to encryption, because it's well-established that the freedoms of speech and association sometimes require privacy in order for each of us to exercise them.

And I would argue the Second Amendment is relevant too, since both the right to keep and bear arms and the common-law right of self-defense suggest that government can't and shouldn't be able to hobble our ability to keep our digital lives and internet homesteads secure.

Not many people talk about the Third Amendment—it prohibits

the forcing citizens to provide quarters in their homes for soldiers in peacetime. But maybe that's relevant too—if Apple has to build its own forensics lab in California for the purpose of giving government agents a place to get access to encrypted data—that starts looking quite a bit like quartering of soldiers, or at least quartering of policemen. And giving government agents a backdoor to our digital lives, looks a bit too much like the mandatory quartering of soldiers in our homes.

Finally, although I could mention other constitutional rights and legal doctrines, I want to stress that Apple and others have argued that Fifth Amendment due-process requirements and prohibitions against compelled testimony apply, as well. No person or company should face a categorical mandate to declare to the world of devices that this particular software—the FBiOS that the government may want—is a trusted update, when its actual purpose is not to protect us but to reveal our secrets.

Now, the argument from government has always been that the warrant requirements and due-process requirements in court ought to be satisfy us—that we shouldn't rely on unbreakable security technologies to make our digital data, and our digital lives, secure. But their assumption here is that the primary way we vindicate our constitutional rights is to go to court and assert them, or to rely on a judge to assert them for us.

But that's not the American tradition—we believe in our citizens' right to protect themselves. As the poet Robert Frost put it, "good fences make good neighbors." We're all better off if we're allowed to use good fences rather than rely on the sheriffs and judges to be the first and only way we make sure we have good neighbors.