



POLITICS

Competing Interests on Encryption Divide Top Obama Officials

By **MICHAEL D. SHEAR** and **DAVID E. SANGER** MARCH 5, 2016

WASHINGTON — The intensifying legal battle over encryption between Apple and the Justice Department has all but obscured another more subtle division, the one inside the Obama administration itself.

Driven by competing and sometimes clashing interests about privacy, national security and the economy, some of the president's most senior aides are staking out a variety of positions on the issue.

The White House denies there is disagreement over the effort to force Apple to break into the phone used by one of the terrorists in the San Bernardino, Calif., shootings, but the differences on how to deal with the broader questions raised by encryption have become increasingly apparent.

The Federal Bureau of Investigation wants the ability to break into smartphones and computers for investigations. The Pentagon and intelligence officials worry that the same techniques could be used by foreign powers or hackers to drain data from phones used by the United States government, and that countries like China will demand the same access provided to American law enforcement officials.

The conflicting positions were on display last week. On Tuesday, James B.

Comey Jr., the director of the F.B.I., testified in Congress about the need for some kind of government action — he avoided the word “legislation” because the White House has specifically said it is not seeking that now — that would guarantee access to law enforcement, no matter how encryption technology evolves.

Less than a day later, Defense Secretary Ashton B. Carter, talking to technologists at an annual computer security conference in San Francisco, struck a very different tone. “Data security, including encryption, is absolutely essential” to the Pentagon, he said. “None of our stuff works unless it’s connected.” He also warned against a legislative solution.

A law “written in an atmosphere of anger or grief,” he said, is “not likely to be the right answer.” Later he drove home the point, saying “it would be better to work this out rather than have a law written.” And throughout his talk, Mr. Carter made it clear that he is more interested in securing data than prying into it.

Administration officials insist the comments do not reflect serious internal disagreements about policy. They say, for example, that the Justice Department and F.B.I. also support strong encryption — with limits — while the heads of the intelligence agencies, responsible for securing government communications, understand the stresses on those investigating serious crimes.

In a statement, the White House said on Friday that “our policy on encryption is clear.” But the policy it described delineated the differing positions rather than resolving them.

“The United States government firmly supports the development and robust adoption of strong encryption, which is a key tool to secure commerce and trade, safeguard private information, promote free expression and association,” it said. “At the same time, encryption poses a grave challenge for our national security and law enforcement professionals.”

But officials from the National Security Agency, the Department of Homeland Security and the Pentagon describe meetings in the White House Situation Room that go over the same territory, and in the end cannot find a middle ground.

The arguments were touched off two and a half years ago, with the revelations by Edward J. Snowden, the N.S.A. contractor, that the agency had gone to some lengths to undercut encryption.

There was evidence — none confirmed, or discussed by the Obama administration — that the N.S.A. had gained access to the unencrypted communications of servers around the world owned by Google and others to tap into foreign communications. There were suggestions that it had also tampered with the products of a foreign manufacturer of SIM cards, which go into every mobile telephone, to make it easier to intercept calls and emails.

The issues were taken up by a presidential commission that included legal scholars and intelligence experts, like Michael J. Morell, the former deputy director of the C.I.A., and Richard A. Clarke, a former senior national security official in the Clinton and Bush administrations who now works in cybersecurity. Their conclusion was unambiguous in opposing the building of so-called back doors for encrypted devices.

The commission told President Obama that the United States government should “not in any way subvert, undermine, weaken or make vulnerable generally available commercial software,” and it urged more companies to adapt such systems.

Last month, Admiral Michael S. Rogers, commander of the United States Cyber Command — the Pentagon’s digital arm, which both protects the Defense Department’s networks and conducts offensive action — as well as director of the N.S.A., echoed that view in remarks to the Atlantic Council.

The view of Admiral Rogers, many experts say, may be affected by the fact

that his agency has the best code-cracking capabilities in the world, and he does not need to make public what systems he is already inside. Because he cracks the codes of foreign adversaries (and more than a few allies), he does not need a warrant, as Mr. Comey does. And his agency's less publicized job is securing the government's most vital secrets.

With more and more government communications relying on mobile devices, including a so-called hardened version of the iPhone and the iPad, the N.S.A. is also not interested in advertising to the world ways in which those devices can be defeated.

So far Mr. Obama has fully backed legal efforts by the F.B.I. to force Apple to help authorities unlock the iPhone of the San Bernardino terrorist, who was killed in the attack. But he has rarely spoken about the broader questions, and when asked recently, a senior administration official said the White House still does not favor legislation to solve the issue.

The encryption issue seems particularly acute at the State Department and the Commerce Department, both of which have their own sets of concerns.

One of Hillary Clinton's favorite pilot programs as secretary of state, accelerated during the 2011 Arab Spring crisis, was to equip dissidents and activists around the world with the "Internet in a suitcase," devices to help communicate and evade censorship.

But the system relies on encrypted conversations, to keep them away from Chinese state security or Egypt's brutal internal police. Any effort to force Apple to break that encryption, several American officials said — insisting on anonymity because the administration is still debating these issues — would be replicated from Beijing to Cairo.

Commerce Department officials have made the point that if Congress ultimately mandates that all encrypted products must be accessible to investigators, it will be a boon to foreign producers of encryption hardware

and software. And there are a lot of them.

Bruce Schneier, a cybersecurity expert, published a study recently that said there were “at least 865 hardware or software products incorporating encryption from 55 different countries.” After the United States, Germany tops the list with 112. Most products, Mr. Schneier said recently, “are as good as what you would find in the United States.”

But so far users are not flocking to them in mass numbers for a simple reason: For novices, they can be hard to use.

Apple’s design is of particular concern to the F.B.I. because the encryption is automatic; users do not have to do a thing to make it work. As a recent Harvard study about the problem of “going dark” — when law enforcement can no longer get access to evidence because of technological advances — pointed out, the more times users have to manipulate the programs, the greater the opportunity for error.

Which is exactly what the F.B.I. is hoping for.

A version of this article appears in print on March 6, 2016, on page A1 of the New York edition with the headline: Apple Battle Bares Fissure in U.S. Policy.