Connecticut Debate Association

March 12, 2016

Farmington, Guilford and Pomperaug High Schools

Resolved: Apple should cooperate with the FBI to unlock Farook's iPhone.

U.S. and Apple Dig In for Court Fight Over Encryption

The Wall Street Journal, By DEVLIN BARRETT and DAISUKE WAKABAYASHI, Feb. 17, 2016

Company refuses to retrieve data from phone of one of San Bernardino killers

Washington and Silicon Valley geared up for a high-stakes legal battle over a phone used by one of the San Bernardino, Calif., terrorists, a contest each side views as a must-win in their long fight over security versus privacy.

A White House spokesman framed the brewing court fight as relating to a single phone—that of Syed Rizwan Farook, who opened fire with his wife at an office party late last year, killing 14 and injuring 22. Apple Inc. Chief Executive Tim Cook and the company's defenders said the fight is really about the privacy and security of millions of customers.

The furor stemmed from a judge's order this week requiring Apple to help the Federal Bureau of Investigation circumvent a passcode protection system on the phone used by Mr. Farook. Apple has said it will fight the order, setting the stage for what both sides expect will be a precedent-setting case in an era of ubiquitous smartphones.

Both sides are bracing for the legal fight ultimately to reach the Supreme Court, and the possibility that the case could prompt Congress to act. The order from Judge Sheri Pym gives Apple five days to challenge her order, which the company has already pledged to do. Whichever side loses is likely to appeal.

"We now have the conditions for the first punch to be landed,'' said Ron Hosko, a former senior FBI official. "But this is just Round One." Mr. Hosko said the FBI has been looking for some time for the right case to make a broader point about the dangers of phone encryption.

In the San Bernardino case, federal law enforcement officials say they have a compelling argument, after a deadly high-profile terror attack, to force open a phone and ensure they haven't missed additional suspects or evidence.

Sen. Tom Cotton (R., Ark.) said on Wednesday that "Apple chose to protect a dead [Islamic State] terrorist's privacy over the security of the American people.''

Apple CEO Tim Cook said the company will oppose a federal judge's order to help the Justice Department unlock a phone used by a suspect in the San Bernardino attack, which killed 14 people. Photo: AP

Detectives and prosecutors said encrypted smartphones are a growing problem for them. The Manhattan district attorney's office said that since September 2014, the technology has kept it from executing about 155 search warrants for devices running Apple's iOS 8 operating system, in cases that include homicide, attempted murder, sexual abuse of a child, sex trafficking, assault and robbery.

Apple and privacy advocates who support the company's stance responded on Wednesday that if the Justice Department wins, the data of every phone user in the U.S. and world-wide will be more vulnerable to hackers and government spying.

"It's not really a question of security versus privacy. It's security versus security,'' said Bruce Schneier, a fellow at Harvard University's Berkman Center for Internet and Society. "Saying that all of these devices must be insecure so the FBI can have access would be a security disaster for us as a society."

Sundar Pichai, CEO of Alphabet Inc.'s Google, voiced support for Apple. In a string of tweets, he said that "requiring companies to enable hacking of customer devices" and data could present "a troubling precedent." Software from Apple and Google run nearly all of the world's smartphones.

As the fight between federal officials and tech companies over encryption has intensified in recent years, talks between the two sides have produced few results, while Congress has struggled to craft legislation on the issue.

FBI leaders had been scanning for a case that would make a compelling argument about the dangers of encryption. In the San Bernardino phone, they found what some law-enforcement officials privately describe as a nearly perfect test case.

Mr. Farook and his wife opened fire at a Dec. 2 holiday party for workers of San Bernardino County, which employed Mr. Farook, before they both died in a police shootout.

The phone in question was used by Mr. Farook but owned by the county, which gave investigators permission to look at it. County officials don't know the passcode Mr. Farook used, according to a Justice Department court filing.

Mr. Farook backed up his data to cloud storage until about a month and a half before the attack. Apple has turned over that data. But investigators suspect there may be crucial evidence that can only be found on the phone itself.

The FBI wants Apple to help it disable a feature that would erase the phone after 10 unsuccessful password attempts. That would give investigators the ability to make numerous tries to find the password.

Apple said that to comply with law enforcement's wishes, it would have to create a separate operating system for the phone, without the security measures, to run in parallel with the existing software. But once that operating system is created, Apple said, criminals and foreign governments could circumvent the security of any phone simply by typing in the device's ID number.

A person familiar with Apple's thinking said the government's suggested techniques for unlocking the iPhone in question would work on even newer iPhones, which have upgraded security systems walled off from the phone's main systems.

A Justice Department spokeswoman on Wednesday said it was "unfortunate that Apple continues to refuse to assist the department in obtaining access to the phone of one of the terrorists involved in a major terror attack on U.S. soil." She added, "The judge's order and our request in this case do not require Apple to redesign its products, to disable encryption or to open content on the phone. In addition, the judge's order and our request were narrowly tailored to this particular phone.''

The government's action presents Apple with a daunting public relations dilemma. In defying the FBI, the company risks alienating consumers concerned about terrorism and being blamed for a future attack. On the other hand, because many customers and Internet activists care deeply about privacy, Apple risks a backlash if it complies.

In China, Apple's largest overseas market, the company faces particular pressure from human-rights activists not to provide technological "back doors" that could enable the government to spy on citizens.

Many within Apple say they view the issue as a moral one, and Mr. Cook's outspoken stand marks a watershed moment in his tenure as CEO. Unlike his predecessor, the late Steve Jobs, who avoided weighing in on political issues, Mr. Cook has demonstrated a willingness to speak out, and he has said in the past that Apple sees privacy as a fundamental human right and one of its core values.

Within the Justice Department, some view the case as a must-win, because it deals with one of the less-complicated problems raised by encrypted technology—how to unlock a suspect's phone after a crime has occurred. Experts call that retrieving "data at rest,'' because it is simply a question of extracting data from a device in investigators' possession. If the government can't win on that issue, officials fear, it will likely be impossible to get courts to allow them access to "data in motion"—messaging apps, texts and other means of communicating that are hard to monitor in real time to detect plots.

In preparation for what is expected to be a long legal fight, activists and politicians on both sides rushed to weigh in. The case attracted the attention of former National Security Agency contractor Edward Snowden, whose disclosures of government spying sparked much of the distrust between the government and the tech industry.

Now a fugitive from U.S. charges living in Russia, Mr. Snowden tweeted that the iPhone case "is the most important tech case in a decade.''

Mr. Cotton said the case suggests the only solution may be for Congress to force tech companies to give law enforcement access to data.

And Republican presidential candidate Donald Trump blasted Apple during an interview on Fox News, saying, "Who do they think they are? … Certainly, we should be able to get into the phone, and we should find out what happened, why it happened, and maybe there's other people involved."

Apple's Rotten Core

The Wall Street Journal, By L. GORDON CROVITZ, Feb. 28, 2016

CEO Tim Cook's case for not aiding the FBI's antiterror effort looks worse than ever.

By refusing to help the FBI unlock the iPhone used by a dead terrorist, Apple succeeded in shifting the debate over privacy and security—but not the way it intended. Apple's recalcitrance makes it likely technology companies will no longer be allowed to ignore court orders or design devices to evade reasonable searches. The question is whether Congress or the courts will set the new rules.

CEO Tim Cook's test case for Apple is rotten to the core. He claimed it was too "burdensome" for Apple to help unlock the iPhone of Islamic terrorist Syed Rizwan Farook, who with his wife killed 14 people and wounded 22 in San Bernardino, Calif., in December. The FBI needs Apple to disarm the feature that erases the content of iPhones on the

10th wrong password so that agents can gain access to the phone to learn if there are other sleeper cells or plots.

When Apple refused the court order, Apple defenders claimed it was impossible to unlock the phone. In court papers filed last week, Apple admits that's not true, but still claims an "unreasonable burden."

The company told the court it would take six to 10 staffers two to four weeks to develop the necessary software. That's less than the annual cost of one engineer, perhaps $200,000. For the world's most valuable company, with annual revenues above $200 billion, it's a trivial cost—and the U.S. government is offering to reimburse Apple's expenses anyway.

National-security lawyer Stewart Baker suggested in the Washington Post that Apple disclose how much Beijing made the company spend on special customer-monitoring software "for the convenience of the Chinese security apparatus."

Apple at first claimed that this work would affect millions of customers. Now its engineers admit code can apply to a specific iPhone.

Apple says cooperating with the government would hurt its marketing, which emphasizes privacy. In another court case, in New York, Apple said compliance would "substantially tarnish the Apple brand," as if branding were above the law. Apple's new litigators, Ted Olson and Ted Boutrous, last week added the better argument that separation of powers requires Congress to decide the issue, not courts.

There's a way out of the impasse: Apple could agree to help unlock Farook's iPhone and focus its legal arguments on the New York case, which is less urgent because the defendant, a drug dealer, already pleaded guilty.

Apple's refusal to help investigate terrorism has rekindled interest in legislation. Congress holds hearings this week, with most Americans saying Apple should comply with the court order, according to a Pew Research Center poll. Microsoft's Bill Gates last week observed that the issue in the Apple case is "no different than 'Should anybody ever have been able to tell the phone company to get information? Should anybody be able to get at bank records?' " Phone companies and banks must ensure that their equipment makes it possible to comply with court orders, and if AT&T and Citibank can't promise customers privacy by evading court orders, why should Apple be able to?

There's a tendency in this era of rapid digital innovation to assume that our technologies raise unique issues. But mobile phones are best considered the latest evolution in the communications revolution that began with the telegraph and continued with the telephone.

Providers of those earlier technologies were eventually required to cooperate with reasonable searches under the Fourth Amendment. In 1928 Justice Oliver Wendell Holmes called wiretapping a "dirty business" and argued that it should be forbidden to law enforcement. As electronic communications became widespread, Congress and the courts established rules for legal wiretaps.

"Criminals, spies and saboteurs," Attorney General Robert Jackson told Congress in 1941, "have one great method of communication which they may use without fear of leaving incriminating trails—the telephone and telegraph. If a criminal writes a letter he runs the risk that it will fall into the hands of the law. If he transacts his illegal business in person, he may be overheard by an eavesdropper. If he sends a confederate to act for him, the confederate may betray him. . . . But so long as he uses the telephone or telegraph, he is sheltered."

Jackson, who was later appointed to the Supreme Court, added: "Experience has shown that monitoring of telephone communications is essential in connection with investigations of foreign spy rings."

Court-ordered wiretaps are now routine, but the law lags by focusing on old-fashioned phones. Technology evolves, yet the Constitution is steadfast in requiring compliance with reasonable searches—even by Apple.

Why Apple Is Right to Challenge an Order to Help the F.B.I.

The New York Times, By THE EDITORIAL BOARDFEB. 18, 2016

It is understandable that federal investigators want to unlock an iPhone used by one of the attackers who killed 14 people in San Bernardino, Calif., in December. And it's understandable that the government would turn to Apple for help. But Apple is doing the right thing in challenging the federal court ruling requiring that it comply.

In an order issued on Tuesday, Magistrate Judge Sheri Pym says Apple must create new software that would bypass security features on the iPhone used by the terrorist, Syed Rizwan Farook. That would allow the Federal Bureau of Investigation to unlock the device and retrieve the pictures, messages and other data on it. Her ruling was based on the All Writs Act of 1789, which is used to require people or businesses not involved in a case to execute court orders. Another federal magistrate judge in New York is considering a similar request to unlock an iPhone in a narcotics case.

Law enforcement agencies have a legitimate need for evidence, which is all the more pressing in terrorism cases. But the Constitution and the nation's laws limit how investigators and prosecutors can collect evidence. In a 1977 case involving the New York Telephone Company, the Supreme Court said the government could not compel a third party that is not involved in a crime to assist law enforcement if doing so would place “unreasonable burdens” on it. Judge Pym’s order requiring Apple to create software to subvert the security features of an iPhone places just such a burden on the company.

Apple has already given the F.B.I. data from the phone that was backed up and stored on its iCloud service; the last backup was made about a month before the attacks. But the company’s chief executive, Timothy Cook, has said that requiring it to create software to bypass a feature that causes the phone to erase its data if 10 incorrect passwords are entered would set a dangerous precedent and could undermine the security of its devices. The Department of Justice has argued that the software would be used on that phone only and notes that Apple has previously helped law enforcement unlock phones. The company changed how it encrypts phones after the surveillance revelations by Edward Snowden.

But writing new code would have an effect beyond unlocking one phone. If Apple is required to help the F.B.I. in this case, courts could require it to use this software in future investigations or order it to create new software to fit new needs. It is also theoretically possible that hackers could steal the software from the company’s servers.-

There are certainly other ways for law enforcement agencies to collect evidence. They already have the power to get data stored on online services like iCloud and Google’s Gmail through search warrants. And they can get records of phone calls and text messages from companies like Verizon and AT&T. A recent study published by Harvard’s Berkman Center for Internet and Society concluded that the proliferation of Internet-connected sensors, cameras and other devices provides the government ever-expanding opportunities to collect information about people.

Even if the government prevails in forcing Apple to help, that will hardly be the end of the story. Experts widely believe that technology companies will eventually build devices that cannot be unlocked by company engineers and programmers without the permission of users. Newer smartphones already have much stronger security features than the iPhone 5c Mr. Farook used.

Some officials have proposed that phone and computer makers be required to maintain access or a “back door” to encrypted data on electronic devices. In October, the Obama administration said it would not seek such legislation, but the next president could have a different position.

Congress would do great harm by requiring such back doors. Criminals and domestic and foreign intelligence agencies could exploit such features to conduct mass surveillance and steal national and trade secrets. There’s a very good chance that such a law, intended to ease the job of law enforcement, would make private citizens, businesses and the government itself far less secure.

Tim Cook’s Bad Apple

L. Gordon Crovitz, The Wall Street Journal, Updated Feb. 21, 2016 7:20 p.m. ET

Refusing to cooperate with the FBI is about protecting the brand, not iPhone users.

The dispute between Apple and terrorism investigators comes down to whether Apple can refuse a court order because it fears complying would be bad for business.

Contrary to CEO Tim Cook’s claim that the FBI’s request is “chilling” and would benefit “sophisticated hackers and cybercriminals,” Apple hasn’t been asked to make iPhones less secure. Instead, last week the company rejected a court order to do minimal work to help the FBI unlock a single phone used by successful terrorists.

This case is a forceful reminder why the Constitution empowers courts to order reasonable searches. A federal magistrate told Apple to help with the iPhone used by Syed Rizwan Farook, who with his wife killed 14 people and wounded 22 in San Bernardino, Calif., two months ago. The FBI hasn’t been able to unlock it to learn whom the terrorists contacted and if there are other plots.

Apple was asked to adjust its software that wipes iPhones clean after 10 failed passwords, to enable the FBI to find the password. Prosecutors want this only for Farook’s phone, to “mitigate any perceived risk to Apple iOS software as to any other Apple device.” The local agency that employed Farook owns the phone and wants Apple’s help. “The user was made aware of his lack of privacy in the work phone while alive,” prosecutors note.

There’s no risk to encryption and the dead terrorist has no privacy rights. So what is Apple trying to protect?

The answer, according to the Justice Department, is a “business model and public brand marketing strategy.” Apple admitted as much last year in explaining to a federal court in Brooklyn, N.Y., why it refused to unlock the iPhone of a methamphetamine dealer. The company had unlocked some 70 iPhones in criminal cases since 2008, so the judge was surprised by its sudden refusal.

Apple’s lawyers explained that customers are so concerned about government access to data that compliance with court orders would “substantially tarnish the Apple brand.” They added: “The reputational harm could have a longer term economic impact beyond the mere cost of performing the single extraction at issue.”

Faced with defending its “brand” against the FBI’s urgent need to gain access to a terrorist’s phone in its biggest investigation since 9/11, Apple has brought in powerhouse lawyers—former Solicitor General Ted Olson and First Amendment expert Ted Boutrous—to find less self-serving arguments.

But what the company said in Brooklyn was genuine. “In the wake of [Edward] Snowden, a kind of anti-government publicity arms race has emerged in Silicon Valley,” Susan Hennessey of the Brookings Institution wrote on the Lawfare blog. “Companies have rushed to disavow any perception of cooperation with law enforcement, and to adopt a position overtly contrary to any kind of surveillance.”

She asked why Apple can “assert reputational harm as a shield from complying with the same laws from which it derives benefits.”

Gus Hurwitz of the American Enterprise Institute says the issue is whether companies can “develop their products knowingly and intentionally in a way that will lead to the routine destruction of evidence.” In 2014 Apple bragged that for its new iPhones, “it’s not technically feasible for us to respond to government warrants.”

Refusing to help a terrorism investigation and crowing about escaping the reach of the law could get iPhones treated the same as earlier phones. The Supreme Court in 1977 enforced a judge’s writ requiring the phone company to install a dialed-number recorder, or pen register, to monitor (but not listen in on) suspected criminals. Two years later the justices held that a pen register didn’t even require a warrant. Federal law now requires telecommunications companies design their equipment to ensure they can comply with court orders.

The head of AT&T, Randall Stephenson, disagrees with Apple’s position. “I understand Tim Cook’s decision, but I don’t think it’s his decision to make,” he told the Journal. “This is an issue that should be decided by the American people and Congress, not by companies.” (Apple’s complying with U.S. law would in no way weaken its position in Russia or China, where surveillance is already far more intrusive.)

Internet companies worry one bad Apple would spoil the bunch by boosting the government’s case for a new law requiring companies make devices accessible under court orders. The problem is that there is no consensus yet on the best way to retain records while still providing strong encryption.

Legislation may be premature, but Mr. Cook’s poor judgment in blocking access to the terrorist’s iPhone tells Americans they can no longer trust technology companies to make these decisions on their own.

Billions at stake in Apple encryption case

CNN, By Peter Bergen, CNN National Security Analyst, February 20, 2016

Peter Bergen is CNN's national security analyst, a vice president at New America and a professor of practice at Arizona State University. He is the author of the new book "United States of Jihad: Investigating America's Homegrown Terrorists."

(CNN)It's a dispute that pits two important principles against each other. It's about the right of the U.S. government to investigate thoroughly the most deadly terrorist attack on American soil since 9/11 versus the right of the most valuable (and iconic) American company to go about its business without the same U.S. government undercutting the key promise it makes consumers -- that their most private communications are kept safely under lock and key.

It's also a dispute that sets the stage for what promises to be one of the great commercial battles of the next years, between the U.S. government and the tech companies that are the most important engine of the booming American economy.

The FBI has argued for years that it faces a "going dark" problem, that its investigations of everything from child pornographers to terrorists are hampered, or even completely undercut, by the fact that so much Internet communication is now encrypted to a level that the U.S. government can't break.

As a result, the FBI wants a "backdoor" into the encrypted communications platforms engineered by American tech companies.

The tech companies reject this demand on the basis that such a backdoor defeats the whole purpose of encrypted communications since if a backdoor exists, not only can the FBI use it, but also so can others.

The companies argue -- quite properly -- that when you build a fence around your house to keep out intruders you don't leave a big hole in the fence for the easy access of police in the event that a crime might take place inside the house, because others can also exploit that big hole.

In addition, the firms argue that if it is known they have given the U.S. government such a backdoor, then consumers around the world will be leery of using Apple and Google and other U.S. technology products. Many tens of billions of dollars are therefore at stake.

The new occasion of this long-simmering dispute is Apple's rejection Wednesday of a federal judge's order to help the

FBI hack into the encrypted iPhone of Syed Rizwan Farook, who in December, together with his wife, killed 14 of his co-workers at a holiday party in San Bernardino, California.

The couple carried out the attack on behalf of ISIS, although there is no evidence they did so at the direction of the group.

On the face of it, Apple's rejection of the judge's order seems quite wrongheaded. After all, the San Bernardino attack was the most lethal since 9/11.

Apple's position, however, is that helping the FBI to decrypt Farook's iPhone would give the government access to all other similar iPhones and would also lead to an unfortunate precedent in which the government could eventually access encrypted communications on any American tech platform. Google has publicly supported Apple's position.

So who is right here? The revelations by National Security Agency leaker Edward Snowden in 2013 about just how much U.S. tech companies had been playing footsie with the U.S. government had an effect on the firms' bottom lines around the globe.

A 2014 paper by my colleagues at the New America think tank estimated that the Snowden revelations cost U.S. tech companies billions of dollars.

Since Snowden went public, companies such as Apple and Google -- two of the world's most valuable companies -- have incorporated much greater encryption into their products and have also been at pains to show that they will not go along with U.S. government demands to access their encrypted products.

What might be learned from Farook's iPhone? Of course, we don't know, but it's likely that it wouldn't be much beyond what we already know from the couple's Facebook postings, their Verizon phone account, their computers seized by police, the evidence found at their apartment complex and the fulsome confession of their friend Enrique Marquez, who allegedly provided them with the rifles used in their massacre and also allegedly knew of their plans to commit a terrorist attack as early as 2012.

No evidence has emerged that Farook and his wife had any formal connection to a terrorist organization, and the plot involved only the couple and the alleged connivance of Marquez. What might be found on Farook's iPhone therefore is more than likely simply only some additional details to buttress the overall account of what we know already.

Balanced against that is what the tech companies lose if they are seen to be doing the bidding of the FBI -- tens of billions of dollars and also the strong possibility of losing market share to other non-American tech companies, particularly software and cloud computing firms, around the world.

A further wrinkle in the story is provided by Daily Beast reporter (and my New America colleague) Shane Harris who reported that Apple has decrypted iPhones for U.S. law enforcement authorities 70 times in the past several years and as recently as 2015. At the same time, Harris reports the government has successfully decrypted at least one version of the iPhone.

These revelations suggest the possibility that the facts of this particular case aren't as important as the larger principles at stake and that both Apple and the U.S. government are using the San Bernardino case as something of a test of the question: Should tech companies give the FBI any kind of permanent backdoor?

The San Bernardino test case will likely set up a legal fight that could go to the Supreme Court. It also may prompt Congress to intervene to pass legislation on the matter.

Although the fight between American tech companies and the FBI hunting terrorists is undeniably important, to some degree it may also be increasingly moot.

ISIS' key social media-encrypted platform is Telegram, which is engineered by a Berlin-based tech company that can simply ignore the rulings of American federal judges as well as legislation passed by the U.S. Congress.

ISIS also advocates to its followers to use the "dark Web" Tor browser, which disguises users' IP addresses and is not controlled by any American tech company.

In other words, once again, technology is outrunning the ability of both law enforcement and legislation to keep pace with it.

Amid Apple-FBI Fight, China Looms

The Wall Street Journal, By LI YUAN, March 2, 2016

Battle on iPhone could reverberate if company faces similar demands abroad

Apple’s refusal of the Federal Bureau of Investigation’s request to help unlock a shooter’s iPhone has been a hot topic not only in its home country but in its biggest foreign market: China. Some Chinese have questioned whether the move is a marketing stunt, but others have supported Apple for standing up to the government—something unimaginable for

Chinese companies. Some also have asked: What if the Chinese government asked Apple to do the same thing? Could Apple say no?

That question points to a significant issue for the company in the current standoff: Complying with the FBI in the San Bernardino, Calif., iPhone case could make it much harder for Apple to rebuff the demands of repressive governments in China and elsewhere abroad for access to the phones of, say, democracy activists or other dissidents. It's an especially important concern for Apple, which gets most of its revenue from outside the U.S. The company derives roughly 25% of its revenue from the greater China region, which includes the mainland, Hong Kong, Macau and Taiwan.

Apple has alluded to this issue, without naming China. In its filing to a federal court in California last week, Apple warned about the dangers of building a backdoor into the iPhone. "Once developed for our government, it is only a matter of time before foreign governments demand the same tool," the filing says.

Benjamin Qiu, a partner in law firm Loeb & Loeb's Beijing office, says if Apple were to lose the battle with the FBI, China's government would have every reason to make similar requests.

"Compared to the Chinese government, FBI is a pushover," he says.

China's State Internet Information Office, which regulates the Internet, didn't respond to requests for comment.

On its privacy Web page, Apple says it "has never worked with any government agency from any country to create a 'backdoor' in any of our products or services."

Chinese technology companies are used to accommodating their government's demands. Executives say they have to surrender whatever user information the government requests, and abide by frequent updates on content to be censored.

Says an executive at one Chinese Internet company, "When government says, 'Jump,' we're expected to ask, 'How high?' "

Increasingly, Beijing is trying to regulate Western tech companies in a similar fashion. A new Internet regulation, effective next week, bars foreign companies from publishing online content in China without prior approval. A draft Cyber Security Law, under review, would require Internet network operators to provide authorities with technological support and assistance for national security and criminal investigations—which Amnesty International, a rights group, says could make it easier to involve companies in censorship and surveillance.

"Since China emphasizes national security more than personal-data protection, tech companies may well be required to follow the authorities' orders," says Yun Zhao, a law professor at the University of Hong Kong.

Western tech companies used to be better able to fend off Chinese government requests by citing legal constraints and political repercussions back home. But Edward Snowden's revelations that the U.S. government tapped into electronics gear overseas to spy on other governments have fed fears about foreign technology in China. As a result, many U.S. tech companies have lost market share in a critical market.

Apple's business has been a rare bright spot among multinational tech companies in China. In fiscal 2015, its revenue in China soared 84% to $58.7 billion. In the rest of the world, it grew 16%.

But Apple, like others, faces increasing scrutiny and pressure from China's government and state-run media. In 2014, after state television called the iPhone a "national security risk," Apple moved Chinese customers' data from overseas into a domestic facility operated by state-run China Telecom. Some critics said the move could make Apple products less secure.

At the time, Apple said the move would improve performance for its Chinese customers, adding that the data are encrypted and not accessible by China Telecom. Jonathan Zdziarski, who researches Apple's software security, posted on Twitter that Apple stores iCloud data on China Telecom with the encryption keys outside the country. "This makes sense and reduces risk of data breach," he wrote.

Still, Chinese authorities have appeared eager to make Apple seem cooperative.

In an English-language post on its Twitter account in January 2015, People's Daily, the Communist Party newspaper, wrote "#Apple has agreed to accept China's security checks, 1st foreign firm to agree to rules of Cyberspace Admin of China." The post was accompanied by a photo of Apple Chief Executive Tim Cook shaking hands with Lu Wei, head of the State Internet Information Office.

All telecommunications manufacturers need to submit their products for government security testing in China, as in other countries, says a person close to Apple.

Apple already fields many requests for information from authorities in China—as in other countries. Its latest transparency report says it received 1,129 device requests in China in the first half of 2015, providing data for 74% of those. In the U.S., it provided data in response to 81% of 3,824 such requests.

Apple doesn't specify the nature of the requests in either country, but says the vast majority globally are from agencies working to retrieve stolen devices. When it comes to law enforcement asking for account information—generally related to iCloud—Apple provided data on 29% of 24 requests in China, compared with 81% of 971 requests in the U.S.

Any U.S. tech company must fear being put in the position Yahoo was with the Shi Tao case. In 2004, at the request of the Chinese government, the company provided information from Mr. Shi's Yahoo email account that Chinese authorities used to convict the Chinese journalist of disclosing a secret government order to an overseas website. Mr. Shi was sentenced to 10 years in prison. At a 2007 congressional hearing on the case, one representative castigated Yahoo executives as moral "pygmies." Yahoo officials apologized.

Apple Wins in Brooklyn Battle Over Unlocking iPhone

Bloomberg News, Christie Smythe and Tiffany Kary, February 29, 2016

Apple Inc. won a pivotal clash with the U.S. over privacy rights, with a Brooklyn judge ruling that the company doesn't have to help unlock a drug dealer's iPhone.

For months, Apple has rebuffed U.S. requests that it assist investigators seeking to crack into encrypted iPhones. The battle burst into public after a California judge this month ordered the company to aid prosecutors seeking access a terrorist's phone, but by then Apple had spent months in a Brooklyn court fighting over the drug dealer's device.

On Monday, Magistrate Judge James Orenstein said the government's demands on Apple were impractical and excessive.

"It would be absurd to posit that the authority the government sought was anything other than obnoxious to the law," Orenstein said in a 50-page opinion.

After helping prosecutors unlock at least 70 iPhones, Apple last year stopped cooperating and said the company would no longer serve as the government's helper. Apple Chief Executive Officer Tim Cook said this month that U.S. demands for iPhone access are a chilling attack on privacy. The government disagreed, saying Apple is more concerned about its marketing and brand identity than about the safety of the public.

Embolden Apple: Monday's decision comes on the eve of Congressional testimony from Apple General Counsel Bruce Sewell and is certain to embolden Apple, which has fought its case in the courts of law and public opinion. At a minimum, it offers the Cupertino, California-based company a legal basis for defying the government. Should the issue reach the Supreme Court, as is likely with the California case regarding the phone used by the gunman who killed 14 people in San Bernardino in December, Orenstein's opinion may inform the high court's decision.

FBI Director James Comey and Manhattan District Attorney Cyrus R. Vance Jr. are also due to appear before the House Judiciary Committee to advocate for the government's push to get more access to encrypted smartphones to help with investigations. While the FBI has stressed that the California case is about only the one phone, Vance has said that Apple's stance has stymied numerous other investigations.

Lasting Impact: With Apple and other companies building even more robust encryption, the outcome of the Brooklyn and California cases could have lasting impact on personal privacy, national security, law enforcement and the technology industry. Orenstein is the first judge to thoroughly explore what the government can and cannot access. The government will appeal.

"This phone may contain evidence that will assist us in an active criminal investigation and we will continue to use the judicial system in our attempt to obtain it," Justice Department spokeswoman Emily Pierce said in an e-mailed statement.

The ruling should help in the California case because Orenstein fully supported Apple's arguments, a company executive said in a call with reporters after the ruling.

In refusing to uphold the warrant, Orenstein focused on the government's use of the All Writs Act, a more than 200-year-old law that prosecutors used to demand that Apple help access data on locked phones.

Orenstein said the government's demands are too "burdensome" because prosecutors have begun demanding repeatedly that Apple unlock other iPhones.

Ask Congress: Echoing comments earlier this month from Cook, Orenstein said that the government should go to Congress for authority to access encrypted phones.

How best to balance privacy and security "is a matter of critical importance to our society, and the need for an answer becomes more pressing daily, as the tide of technological advance flows ever farther past the boundaries of what seemed possible even a few decades ago," Orenstein said.

Legislators, not judges, are best "equipped to consider the technological and cultural realities of a world their predecessors could not begin to conceive," he said.

The Brooklyn case is one of at least dozen across the country in which Apple has recently refused to help investigators access an iPhone. Prosecutors there are seeking help accessing an older operating system, iOS 7, by bypassing the user's pass code and downloading the data.

Pass Code: The phone in California uses a newer operating system, with tighter encryption standards that make it virtually impossible to access content of a phone without a pass code. U.S. investigators can still attempt to get the data through a "brute force" tactic of entering unlimited numbers, but extra protections may erase all data on a phone if the wrong code is entered more than 10 times.

The government said its only concern in California is getting Apple to disable that feature in that one iPhone. Apple called the U.S. demand "dangerous" in a Feb. 25 legal brief because it would force the company to create an entirely new operating system vulnerable to "hackers, identity thieves, hostile foreign agents and unwarranted government surveillance."

Months before the San Bernardino attack, both Apple and the government recognized that the legal dispute was so fundamental that they pressed Orenstein for a ruling even though the defendant in the crystal meth conspiracy case had pleaded guilty. The legal principles courts establish may be controlling regardless of a phone's degree of encryption.

Cook's Letter: Since Cook published a Feb. 16 letter declaring that Apple would challenge the California magistrate's order, law enforcement officials across the country have rallied behind the Justice Department.

Apple's stand puts "profit over safety," said Jonathan Thompson, executive director of the National Sheriffs' Association.

"This has nothing to do with privacy," Thompson said. "It's all about money and their brand."

Tech Sector: Big names in the tech sector came to Apple's defense after the California order. Microsoft Corp. said it would file a legal brief in support of Apple. Google Chief Executive Officer Sundar Pichai said the government's request could spur "a troubling precedent." WhatsApp co-founder Jan Koum said on his Facebook page, "We must not allow this dangerous precedent to be set. Today our freedom and our liberty is at stake."

The Brooklyn decision will have no direct bearing on the California case, where Magistrate Judge Sheri Pym issued an order even before giving Apple an opportunity to weigh in. The company has now filed its legal briefs, and Pym will consider the case further and may consider Orenstein's decision even if not bound by it.

The case is Order requiring Apple, Inc. to assist in the execution of a search warrant issued by the court et al, 1:15-mc-1902, U.S. District Court, Eastern District of New York (Brooklyn).

The iPhone Fight Is Already Over

The Wall Street Journal, By HOLMAN W. JENKINS, JR., Feb. 19, 2016

Law enforcement will win this bout but lose the larger battle over access to encrypted data.

The government will win its fight with Apple.

If Apple can provide a means to gain access to encrypted data on the iPhone of Syed Rizwan Farook, one of the San Bernardino shooters, the company can expect courts to force it to do so. Just as any company in a position to provide useful information to a criminal investigation can expect to be compelled to cooperate. What's more, data on Farook's iPhone isn't "secure." If Apple can defeat the purpose of encryption on its device, somebody else can.

In the meantime, Apple nonetheless reasonably defends its commercial reputation by declining to cooperate until legally compelled to do so. The legal system's job is to make sure Apple swiftly complies. And don't believe the guff that Apple can't submit without endangering all iPhone users.

Down the road, of course, the bigger problem is that Apple—or Google, Facebook, WhatsApp or anybody—is perfectly capable of designing devices and apps unbreakable even by their creators. And down the road is apparently now: Farook's iPhone 5c model is said to be susceptible to Apple-created software to get around a key safeguard, but later iPhone models supposedly lack some of the vulnerabilities the FBI is asking Apple's help in exploiting.

For good reason, however, Congress is unlikely to solve this problem by requiring the creation of so-called backdoor keys exploitable by law enforcement. So a government victory in the current Apple fight may not have the far-reaching implications that Apple CEO Tim Cook's rhetoric implies.

For all the histrionics, the precedent could be a big yawn. Apple will have served itself with its conspicuously noisy defense of customer privacy. Apple's fight has turned into a branding moment. And when the company is finally forced to yield, it will declare victory anyway and emphasize how current iPhone models are designed to be impenetrable even with Apple's coerced assistance.

To the FBI and other police agencies, the outcome will be less than ideal. They can expect to be increasingly frustrated by the inaccessibility of encrypted information on late-model devices. Law enforcement and the public, rightly, will not take comfort in the argument (made by some) that, oh well, such electronic information didn't exist a decade ago and law enforcement survived without it. If the information exists, government understandably will want to exploit it for national security and law enforcement purposes.

Life, though, is full of trade-offs. Even if Silicon Valley were to become maximally cooperative, compliance would likely only make the market more inviting for apps and devices beyond the reach of U.S. mandates. One reason Congress resists "backdoor" legislation is fear of undermining Silicon Valley's global pre-eminence in software. Any benefit to the U.S. government would be short-lived if criminals switched to foreign-designed and -maintained platforms. And devalued would be the considerable expertise already accumulated by U.S. agencies in how to track, spoof and disrupt criminal users of popular U.S. devices and messaging apps.

Criminals face trade-offs too. Law enforcement may find it difficult or impossible to decrypt specific messages, but criminal and terrorist reliance on digital devices still generates plenty of information that law enforcement can exploit. Ask any late terrorist who unwittingly gave away his location electronically and was visited by an armed surveillance drone. Even masterminds like the hacker "Sabu" and the online drug kingpin "Dread Pirate Roberts," to name two recent examples, despite paying expert attention to concealing their online identities, were unable to scrub the clues that allowed the FBI to nab them.

But optimal is not the same as perfect, and it seems obvious that an optimal solution now won't include backdoors. Even if such openings for law enforcement weren't liable to be exploited by criminals and hackers, customers apparently won't stand for them. What the Apple case teaches is mainly a lesson for device makers: As long as a company leaves itself a means to get access to user data, it can expect the law to come knocking.

And even this lesson is anachronistic: Apple's iPhone 5 was released in September 2012, months before the Edward Snowden betrayal brought attention to the NSA's surveillance activities, setting off a commercial race by Apple, Google, Facebook and the rest to distance themselves from U.S. security efforts. Whatever the optimal balance before Mr. Snowden's action, the need to keep faith with global consumers has now left less room to accommodate legitimate law enforcement. We'll just have to learn to live with the result.

The FBI vs. Apple

The Wall Street Journal, Editorial Board Member Joe Rago, Feb. 19, 2016

The White House should have avoided this legal and security showdown.

The encryption cold war that for two years has pitted Silicon Valley against law enforcement finally turned hot this week, as a California judge ordered Apple to unlock an iPhone used by the San Bernardino terrorists. Perhaps public safety and modern digital security methods were bound to collide, but the danger as always in such conflicts is that both sides end up annihilated….

One question is whether the San Bernardino terror case should be an exception to Mr. Cook's strong argument against backdoors. In this case Apple is not being ordered to create a universal backdoor for all phones, and some digital security experts believe it is technologically possible to assist the FBI in the San Bernardino investigation with a unique iOS to brute-force this single device.

"Apple does not dispute that it has, in prior instances, complied with data extraction demands that have been contained in the body of search warrants or, less often, All Writs Act orders," Apple conceded in a New York court filing last year. The government is citing this to show that its request is reasonable.

But in those cases the company's engineers have never been conscripted to create a new architecture to defeat their own security measures. Apple believes that if it caves even once, every prosecutor in America will be lining up for forensic help with misdemeanors. A supposedly one-time emergency fix in an antiterror case could well become a de facto backdoor in practice over time.

There's also the question of whether the government currently has the legal authority to force Apple to become the government's agent. Safe manufacturers are not obligated to crack their own locks when the FBI calls. Apple contends the All Writs Act has never been used to compel what the government now wants from Apple, and the question is far from clear-cut. The litigation to settle this could take months or years.

It's an understatement to say that Apple is taking a risk by challenging the Administration in a high-profile domestic terror incident with unpredictable politics. "Apple chose to protect a dead ISIS terrorist's privacy over the security of the American people," said Arkansas Republican Tom Cotton, and Donald Trump has been no more subtle.

But for the same reason, the Administration ought to have resolved the situation confidentially before it reached legal and political Defcon One. Terror cases by their nature are different from run-of-the-mill law enforcement, and San Bernardino requires more than the government's typical show of incompetence…