APRIL 2016 • WWW.SCMAGAZINE.COM

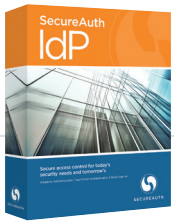
SC MAGAZINE

FOR IT SECURITY PROFESSIONALS

REVIEWED IN OUR GROUP TEST

Datablink P41
Strong authentication, easy to use and fits well in a banking setting.

SecureAuth P44
Well-conceived front-end for all of your assets and locations.



Vasco P45
Authentication that addresses code injection and screen scraping.

FEATURES:

READY TO RUMBLE

Apple vs. FBI: Privacy and security hang in the balance, says privacy expert Lisa Sotto. P18

States take the lead

Expect more activity at state legislatures on cybersecurity and privacy. P24

Devalue data, deter cybercriminals

Methods exist to render enterprise data more difficult for intruders to access. P26

READY TO RUMBLE

Apple vs. FBI: Privacy and security hang in the balance, says privacy expert Lisa Sotto. Teri Robinson reports.

Let's get ready to ruuuummbbbble! In this corner, we have the Justice Department, the prosecutorial arm of the U.S. government and, in its own words, defender of the people. And, in the other corner, we have the darling of Silicon Valley, a self-billed "true American company," Apple.

In what promises to be a battle of epic proportions (think Godzilla vs. King Kong, Muhammad Ali vs. Joe Frazier, The Rock vs. Hulk Hogan) the two giants are squaring off over the fate of an iPhone 5c. To the winner goes the spoils! But, of course, in this case, the spoils are much more than the iPhone at the heart of this legendary showdown.

The outcome of this fight – one that observers expect will make its way to the biggest ring of them all, the Supreme Court of the United States – will have long-lasting influence on privacy and more clearly define the boundaries of governmental reach.

It may also finally prompt a sluggish Congress to break its gridlock and craft overarching encryption and surveillance legislation.

"It should never have escalated to this, privacy should have been addressed," says Lisa Sotto, managing partner in the New York office of Hunton & Williams, who focuses on privacy and cybersecurity issues. The government, she says, should have "worked with tech companies to craft policies and processes."

But escalated it has into what Justin Harvey, chief security officer for Fidelis Cybersecurity, calls "a landmark case," noting that he is "aware of people getting compelled to unlock a phone, but I've never heard of a manufacturer being ordered to decrypt something by court order."

Why the government and Apple squared off over this particular case is puzzling to more than a few observers – with some curious as to why Apple drew a firm line after years of compliance with similar government requests and others equally curious as to why the FBI is pushing against that line. Hard.

But most believe the time is simply right, with many pointing to a confluence of events and undercurrents that have brought Apple and the FBI to an inevitable confrontation: A terrorist attack on U.S. soil by husband/wife team Syed Rizwan Farook and Tasheen Malik that followed close on the heels of the horrifying attacks in Paris has lent a sense of urgency to pending investigations. An FBI worried about the rise of homegrown terrorists adept at using technology to communicate and "going dark" to evade detection and relying on a law, the *All Writs Act* (*AWA*), that's more than 225 years old, as broad authority to demand tech companies provide access to data locked in iPhones and other smart devices. A post-Snowden world that finds companies once perceived as working too closely with government, now trying to rehabilitate their images with consumers. The rise of smart devices as the "footlockers" (according to the Supreme Court) of their owners' personal lives.

In the years since Edward Snowden unleashed documents pilfered from the National Security Agency (NSA) that revealed the extent of NSA surveillance of U.S. citizens and a certain complicity between government investigators and Silicon Valley companies, Apple, Google, Twitter, AT&T and the like have spent a lot of time and effort distancing themselves from those ignominious revelations and shining light – through transparency reports and other initiatives – on government data requests.

Those companies have tried to extricate themselves from the surveillance business by putting more control over the contents of smartphones and other devices squarely in the hands of users by adding encryption, passcodes, biometrics and an auto-erase feature – like the one activated on Farook's phone that wipes the device clean after a certain number of unsuccessful passcode attempts (in this case, 10).

Add to that a gridlocked Congress unable to produce definitive legislation – and you have the cliché commonly referred to as a perfect storm. Whatever the circumstances that led to the tense standoff, the FBI/Apple conflict in San Bernardino likely will become a test case for the FBI as to how far it can push tech companies to do its bidding. Or, it could become known as the time Apple spurned the advances of federal prosecutors and struck a blow for digital rights.

Put up your dukes

The first punches in the conflict were thrown in December 2015 when the FBI seized the iPhone 5c issued to Farook by his employer, San Bernardino County, during its investigation of a violent attack at the Inland Regional Center in San Bernardino, Calif. in which Farook and Malik killed 14 people. When the FBI seized the phone, it instructed San Bernardino County to reset the iCloud password, a request that may have contributed to the feds' inability to access data on the phone going forward.

Apple was asked to unlock the phone, but refused, ostensibly because doing so would require creating ingress into its products. Once Apple spurned its advances, federal

Lisa Sotto, partner, Hunton & Williams

Photo by Danny Ghitis

prosecutors petitioned a federal court in California to compel the iPhone-maker to hand over the tools the authorities need to crack the phone's encryption.

Sheri Pym, a U.S. Magistrate Judge for the Central District of California, ordered the tech company to provide "reasonable technical assistance" to help law enforcement access encrypted data on the iPhone 5c. Included in that reasonable assistance was Apple's use of its exclusive expertise to bypass the auto-erase function on the phone so that FBI investigators could input an unlimited number of passcodes as they attempted to unlock the iPhone of the killers.

"Apple has the exclusive technical means which would assist the government in completing its search, but has declined to provide that assistance voluntarily," according to the Justice Department's initial filing, which U.S. Attorney Eileen M. Decker, the chief federal law enforcement officer in the Central District of California.

Apple's reaction was swift. That same evening, CEO Tim Cook penned a letter to customers and posted it to the company's website, saying that "the U.S. government has asked us for something we simply do not have, and something we consider too dangerous to create."

Let the trash talk begin

By the time Farook carried out his violent plans against his workmates, Apple had already helped the feds break into a number of iPhones, as Loretta Lynch, the Attorney General of the U.S., reminded attendees at the RSA Conference in San Francisco in a March keynote.

"This is a very different position for Apple," Lynch told the RSA audience discussing the company's stance in the San Bernardino case, and urged the company to comply with the law as it has done in the past.

"Apple has attempted to design and market its products to allow technology, rather than the law, to control access to data which has been found by this Court to be warranted for an important investigation," Justice said in court documents.

In his letter to customers, Cook points out that "when the FBI has requested data that's in our possession, we have provided it." Apple, he stresses, indeed "complies with valid subpoenas and search warrants, as we have in the San Bernardino case," adding that the company has "also made Apple engineers available to advise the FBI, and we've offered our best ideas on a number of investigative options at their disposal."

And Snowden himself decried the FBI's claim that it needed Apple's expertise, saying the agency most certainly has the ability to crack the phone.

But this case is different

In its formal response to the FBI's order, Apple accused the government of overreaching its authority,. The company and its supporters say that the San Bernardino request that prompted Pym's order threatens to violate a handful of Constitutional amendments. At RSA, Lynch dismissed arguments of Fifth Amendment violations since Apple is not the subject of the Justice Department's investigation. "Apple is not a target…[and] is not accused of doing anything wrong," Lynch explains. "They're a third party," so there is "no self-incrimination" involved.

As for contentions that the First Amendment applies to code, Lynch says it bears discussion but is "not germane to this case."

But "nobody quite knows" how those amendments might apply, says Sotto. "It doesn't fit [neatly] into any legal regime."

The attorney general furthered the government's argument that its request is a one-off, a less convincing claim considering how many similar requests are pending for numerous iPhones around the country, and, says Kevin Bankston, director of the Open Technology Institute (OTI), given that "the FBI has already spent the last year arguing for backdoors in front of Congress and at the White House." Indeed FBI Director James Comey has been back and forth to Capitol Hill arguing the agency's case and appearing before the Senate Select Committee on Intelligence (SSCI) to contend that the FBI's investigation has been hampered by the inability to crack the iPhone.

And Apple attorney Marc Zwillinger

COMPETITIVE: Disadvantage

The Justice Department has slammed Apple's public repudiation of the California court order, stating it "appears to be based on its concern for its business model and public brand marketing strategy."

The company, it said in court documents, "has attempted to design and market its products to allow technology, rather than the law, to control access to data which has been found by this Court to be warranted for an important investigation."

While the company has declared its main motivation in challenging the government is to protect the privacy and security of its customers, it has stressed in court documents that it is, in fact, concerned what the outcome of the case might have on its reputation. If compelled by the court to break the security of its own products, the damage to its brand will be irreparable, it says.

Indeed, Apple is already feeling the heat from potential customers for spurning the FBI's entreaties to open the San Bernardino iPhone. Maricopa County Attorney Bill Montgomery said in a February statement that he was banning iPhones for the county's more than 900 employees. Of the 564 smartphones used throughout the prosecutor's office, 366 are iPhones and the ban currently applies to replacement and upgrade phones. "Apple's refusal to cooperate with a legitimate law enforcement investigation to unlock a phone used by terrorists puts Apple on the side of terrorists instead of on the side of public safety," Montgomery said in a statement, calling Apple's refusal to bend to federal prosecutors a "corporate PR stunt."

writes in a letter in federal court of nine cases in which federal prosecutors are pressuring the company.

Lynch's words at RSA perhaps are the most telling, hinting at the government's larger goal. While calling the request a one-off, in nearly the same breath she said that the "inability to access information that could actually save lives" is dangerous. Industry and government working together is critical in successfully combating violent extremism and the rise of the homegrown terrorist requires the collaboration of government and private industry, she said in a plea to the tech innovators in the room, noting that going dark is a "very real threat" that tech must help thwart by preventing terrorists and criminals from finding the "safe harbor they seek within dark corners" of the internet.

"I think the issue of going dark has been a huge bugaboo for law enforcement for years," says Sotto.

If Apple is made to provide access, there are a number of prosecutors across the country lying in wait to press the country into service. Cy Vance Jr., the District Attorney of New York County, has made it clear that he would petition Apple to open the nearly 200 phones he has in evidence for various investigations.

John Gunn, VASCO Data Security

> "This is a very different position for Apple."
>
> – Loretta Lynch, Attorney General of the U.S.

Privacy and security on the ropes

"The future of digital privacy also hangs in the balance," Alex Abdo, staff attorney with the ACLU Speech, Privacy and Technology Project, says of the Apple case. "If the government can force companies to weaken the security of their products, then we all lose."

Indeed, Apple's Cook writes, "Specifically, the FBI wants us to make a new version of the iPhone operating system, circumventing several important security features, and install it on an iPhone recovered during the investigation," the letter says, warning that "in the wrong hands, this software – which does not exist today – would have the potential to unlock any iPhone in someone's physical possession."

The California court order, then, Cook says, "has implications far beyond the legal case at hand."

Privacy advocates agree, with the likes of the ACLU, Electronic Frontier Foundation (EFF) and Center for Democracy and Technology (CDT) throwing their support behind Apple with court filings and a stepped up awareness campaign to keep a dialog going with the public and lawmakers.

"We are supporting Apple here because the government is doing more than simply asking for Apple's assistance," the EFF writes in a blog post penned by Kurt Opsahl, deputy executive director and general counsel. "For the first time, the government is requesting Apple write brand new code that eliminates key features of iPhone security – security features that protect us all."

A number of privacy advocates agree. "Governments have been frothing at the mouth hoping for an opportunity to pressure companies like Apple into building backdoors into their products to enable more sweeping surveillance," Evan Greer, campaign director for digital rights group Fight for the Future, says. "It's shameful that they're exploiting the tragedy in San Bernardino to push that agenda."

The government's request, EFF's Opsahl notes, is akin to demanding Apple create a master key that can open a single phone that it would likely demand to use in other cases. "We're certain that our government will ask for it again and again, for other phones, and turn this power against any software or device that has the audacity to offer strong security," he says.

Once a company would "create that mechanism," says Sotto, "it's out there in the wild and it can't go back in the bottle." As a result, it "becomes a tool available for oppressive governments to use," she says.

At the end of the day, privacy advocates believe that the order undermines users' rights to safeguard and handle their own data. "The Constitution does not permit the government to force companies to hack into their customers' devices," said Abdo at the ACLU. "Apple is free to offer a phone that stores information securely, and it must remain so if consumers are to retain any control over their private data."

Chris Eng, vice president of research at Veracode, says a "broader discussion around whether generic backdoors should be provided by technology providers to law enforcement is completely different, and the continued backlash against this is fully warranted" because it can't safely be done "without endangering users."

Collateral damage

DoJ's efforts drew immediate fire from many security pros as well. "The DoJ is accusing Apple of exploiting the issue of backdoors as a marketing strategy while they simultaneously promote the idea that every surveille action is necessary to stop the next terrorist attack," says John Gunn, vice president of communications at VASCO Data Security. "The history of mass surveillance programs doesn't support this and consumers endorse Apple's decision to not build-in a known security vulnerability."

How the Apple case plays out could have an impact on the U.S.'s ability to uphold the Privacy Shield pact reached with the EU in February. "One of its major points is to create 'clear safeguards and transparency obligations on U.S. government access,'" says Csaba Krasznay, product manager at Balabit. "Although this demand seems to be an internal issue in the United States at the first sight, this is a bad message for EU and its citizens."

There's a fundamental difference in the way Europe and the U.S. view privacy. "We think about privacy as a consumer issue where in Europe, privacy is a fundamental right," says Sotto.

Justin Harvey, CSO, Fidelis Cybersecurity

Krasznay contends that "from the technology perspective, there shouldn't be a 'magic key' to open any encryption on a vendor's device. If there is such a key, the trust level in the vendor will fail dramatically. This is a true Catch-22."

Abdo told reporters recently that the flood of data requests would force technology companies to create compliance departments consisting of their best technologists. Those departments, he says, would eventually become targets of cybercriminals, who would quickly divine where a company's security secrets were kept.

But not everyone in the industry is in agreement with Apple's position, with some casting the company as a drama queen and acknowledging the challenges the FBI faces in tracking down terrorists and criminals.

Eng at Veracode, for one, takes issue with calling law enforcement's request a backdoor. "They're asking for a software update (which could be designed to work only on that one particular phone) which would then allow the FBI to attempt to crack the passcode and decrypt the data," Eng says. "Such a solution would be useless if applied to any other phone."

Pointing to Apple's past compliance with "requests to, for example, bypass lock screens in aid of criminal investigations," he notes that "it's only in recent years that they've taken an ideological stance on consumer privacy." That leads Eng to "believe Apple is taking this position less as a moral high ground and more as a competitive differentiator, betting that Google won't do the same."

The San Bernardino County District Attorney Michael Ramos has thrown in his two cents, claiming in court filings that the Farooks could possibly have used the iPhone 5c as a weapon to introduce a dormant cyber pathogen into the county's infrastructure. Let that sink in for a moment. A dormant cyber pathogen. That's a fancy way of saying that shooter Syed Rizwan Farook may have used his county-issued iPhone to infect the government's networks with malware.

And if the Cupertino, Calif.-based company's concerns over potential "unauthorized access to an encryption key" is its true motivation, says Maricopa County Attorney Bill Montgomery, who recently banned iPhones among county employees, then the problem should be defined and worked on as such. "Otherwise, Apple is proving indifferent to the need for evidence to hold people accountable who have harmed or intend to harm fellow citizens."

Philip Lieberman, president and chief executive officer of Lieberman Software, says he doesn't "get" Apple's position. "Everyone knows they know how to open it up," he says. "The backdoor has always been there." The case, he says, "is all about the root certificate. Whoever gets to control the root certificate controls the code."

Apple could ensure its assistance in the San Bernardino case is a one-off by taking a page out of the government's book in its dealing with the Iraq centrifuge case. "You invalidate the certificate after the thing is done and it can't be used any more," says Lieberman.

Who'll throw the knockout punch?

It is hard to tell how the legal wind is going to blow. While Apple is powerful and armed with a team of lawyers and resources, "it's still no match for a motivated federal government," says Jeff Hill, channel marketing manager at STEALTHbits.

But Sotto says the FBI "may have gone a step too far" in pushing a court battle over the San Bernardino phone and may very well "get nailed" for its ambition. "They used to keep it under the radar," she says of the FBI's liberal use of the *AWA* to get at data encrypted on smart devices. "But now they've revealed [it] and the whole program is going to be rolled back."

Apple did score a victory in another case under close scrutiny when a federal magistrate in New York ruled on Feb. 29 that the company did not have to comply with an FBI request to crack open an iPhone at the center of a drug case. Judge James Orenstein, known as a Fourth Amendment advocate, agreed. In a 50-page ruling he knocked the government for assigning itself broad authority under the *AWA*.

"Under the circumstances of this case, the government has failed to establish either that the *AWA* permits the relief it seeks or that, even if such an order is authorized, the discretionary factors I must consider weigh in favor of granting the motion," Orenstein writes.

It was Orenstein who first raised questions over prosecutors' request that the court order Apple to unlock an iPhone 5s that the Drug Enforcement Agency (DEA) had seized in a drug investigation. In an October memo, Orenstein took aim at the government's expansive use of the *AWA* and asked

Apple to respond, Abdo said in a conference call with the press in late February, praising the judge's decision.

"This is a victory for privacy, security and common sense," Abdo says. "The government should not be able to run to court to get the surveillance power that Congress has deliberately kept from it."

Orenstein's ruling does not have legal standing with cases pending outside of New York, though it could wield some influence in California and elsewhere.

And the Justice Department's Lynch made good on her promise at RSA in March to resubmit the fed's request, asking for a district court judge to overturn Orenstein's ruling.

Congressional heavyweights

Apple and the FBI have been left to duke it out in the courts in large part because Congress, as has become its modus operandi, has stayed silent ringside. Locked in its own internal struggles, the lawmaking body has failed to produce one meaningful piece of legislation around encryption or set parameters for prosecutorial reach.

It has become increasingly apparent that the FBI has stretched the *AWA* well beyond its bounds – at least when it comes to the cybersecurity and collecting encrypted data from smart devices. "The established rules for interpreting a statute's text constrain me to reject the government's interpretation that the *AWA* empowers a court to grant any relief not outright prohibited by law," Orenstein wrote in his decision.

Rep. Ted Lieu (D-Calif.)

As the Apple/FBI case dominates the national dialog, even finding its way to the presidential debate stage, many say Congress needs to step in and, more than referee the fight, actually lay down the ground rules of engagement.

> **"The backdoor has always been there."**
>
> **– Philip Lieberman, CEO, Lieberman Software**

"The courts can't keep doing it on a piecemeal basis," says Sotto, who explains that Orenstein's decision is not binding. "It requires Congressional intervention."

But, poking the sleeping giant may have paid off – some rumblings of legislation can be heard on the Hill. A day after Comey testified before the Senate Intelligence Committee, a bipartisan set of Democratic and Republican members of Congress, including Reps. Ted Lieu (D-Calif.) and Blake Farenthold (R-Texas) unleashed a bill, the *Ensuring National Constitutional Rights for Your Private Telecommunications Act of 2016*, that would preempt states' data security vulnerability mandates and decryption requirements.

"A patchwork of 50 different encryption standards is a recipe for disaster that would create new security vulnerabilities, threaten individual privacy and undermine the competitiveness of American innovators," Lieu says. "It is bad for law enforcement, bad for technology users and bad for American technology companies."

The chairman of the Senate Intelligence Committee, Sen. Richard Burr (R-N.C.), is considering encryption legislation though he backed away from his earlier claims that he would include criminal penalties in his legislative proposals.

And Rep. Michael McCaul (R-Texas) used the stage at RSA Conference 2016 to stump for a bill he introduced with Sen. Mark Warner (D-Va.) that would create a panel of technology and legal experts that would work together to solve security issues. McCaul calls the idea of having vendors install backdoors that would allow law enforcement to enter devices used in a crime as an ineffective tactic, saying any criminal, terrorist or nation-state actor would simply move away from using such a device in order protect itself.

The ongoing battle between Apple and the FBI, McCaul implies, is a pivot point to push for the adoption of his bill to create the National Commission on Security and Technology Challenges. He says the argument is driving a wedge between law enforcement and the public sector – which is not good for the nation.

And the White House has cast its hat in the ring regarding the issue of encryption. In February President Obama introduced a bold Cybersecurity National Action Plan (CNAP) that not only included a significant dollar commitment to cyber in the fiscal 2017 budget, but under two executive orders called for the creation of a Commission on Enhancing National Cybersecurity and a Federal Privacy Council.

And Mark Weatherford, chief cybersecurity strategist at vArmour, also applauded Obama's actions. "Security needs to be a team sport where innovation meets policy, and where the technology community and Washington D.C. collaborate to address the nation's cybersecurity challenges."

Whether Apple can convince the public and the courts to support its efforts remains to be seen, but it promises to be one helluva fight between two undisputed heavyweights. ■

A more extensive version of this article is available on our website.


As seen in
SC
MAGAZINE
FOR IT SECURITY PROFESSIONALS