Apple vs. the FBI: Where Did It Come From? What Is It? Where Is It Going?

Riana Pfefferkorn

Lunchtime talk delivered at Berkeley Law, March 7, 2016

Hosted by the Berkeley Information Privacy Law Association

Hi everyone. Thanks for coming out to the talk that you all thought was the least boring option out of the lunch talks that are serving free food today.

You've just heard who I am, now let's find out who you are.

- How many people here are from the I-School?
- How many from the Law School?
- Anyone here from neither category?

And you're all here *hopefully* not just for the free food, but because you share my interest in privacy and the law.

Like some of you, I went to law school because I wanted to work at the intersection of technology law and civil liberties. That interest came from two things I did in my last year in college: first, I spent my summer volunteering at the EFF. (Mind blown.) And second, in the fall semester, I audited a class on the First Amendment.

The Dance of the First Amendment and Technology

In that class, we learned about cases that involved books, flyers, trucks with PA systems mounted on them, radio, and the 7 naughty words you can't say on TV.

And what I noticed as a common theme across all these cases was that the law was in a never-ending tension with technology. Anytime a new technology came along that could possibly be used to express yourself, somebody would put it to that use, inevitably in a really obnoxious way. Whether it was a truck with a PA rigged up, or the Internet.

And invariably, the police or other government officials wouldn't like it and they'd bring the hammer down, to stop the speech. And it would take a court case to roll back those restrictions, because they went too far in infringing on our right to freedom of expression.

But that right is not absolute, so the courts have had to figure out how to strike the correct balance between that right and competing interests to which it sometimes gives way. Such as, not exposing little kids to a really blue George Carlin routine.

Before the 20th century, though, First Amendment jurisprudence basically didn't exist. And it's absolutely no coincidence that that changed, in a major way, in the

same century that the accelerating pace of technological innovation transformed the world we live in.

But we didn't get here merely because someone invented those new technologies. It takes making a technology widely accessible to lay people, not just the military or universities or a handful of businesses granted permission from the King, before any speech-enabling technology – whether it's the printing press or the Internet – starts looking dangerous enough to the people in charge to wind up in court.

And that's why we have Apple vs. the FBI.

Access for Me, But Not for Thee

Apple vs. the FBI, as the order to Apple in the San Bernardino shooter case has come to be known, is happening because that same discomfort with popular access applies not only to speech-enhancing technologies, but to privacy-enhancing technologies as well.

The police are used to accessibility being *their* thing, not *your* thing. They're accustomed to being able to keep tabs on your communications and your data, from letters to phone calls, from wall safes to PCs. And they're used to most people being unable to effectively keep them out.

But remember, their "*customary*" access isn't something the government is entitled to by some natural law or God-given dictate. They're starting from a position of constrained, limited power, subject to the Bill of Rights. And just as the police have gone too far quashing constitutional *speech* rights and needed the courts to dial it back, the same has happened with *privacy* rights. So it took the Sixth Circuit's *Warshak* decision in 2010 to make law enforcement start getting a warrant for email, and it took the Supreme Court's *Riley v. California* decision in 2014 to make them consistently get a warrant to search mobile phones.

Neither of those decisions, though, dealt with the police's *ability* to access information. They just told police what *procedural hoops* they have to jump through to get it. That it was *possible* to get it was taken as a given.

The '90s Crypto Wars

That's what encryption threatens. Law enforcement is used to being *able to access* information, with the right court process. So in the early 1990s, as personal computers became commonplace, the "Crypto Wars" began when the privacy-enhancing technology of encryption started to be developed in the private sector for commercial use—and the law enforcement and intelligence communities *freaked out*.

For decades, crypto had been the near-exclusive province of the spooks and the military. Making crypto commercially available to the general public was scary because it threatened law enforcement's *underlying ability* to access information even with the appropriate legal authorization. If commercial encryption was coming, like it or not, then the government wanted to at least get out in front of the 8-ball. It tried this both externally and domestically, but without long-term success.

Cryptography was classified as a munition until 1996 and was subject to strict export controls. As commercial crypto came into being in the '90s, the government imposed key-length limits on it for export, which made it easier to crack. So companies would typically offer two versions of their product, one for the US, a weaker one for the rest of the world. These export restrictions were gradually eased over the course of the '90s, though the NSA fought every inch, due to economic pressures to keep America competitive on the global market, legal challenges, and the simple reality that you can't put the genie back in the bottle.

Domestically, the NSA developed the ill-fated Clipper Chip in 1993. The Clipper Chip was an encryption device intended for inclusion in telephones. It had a built-in backdoor based on a key escrow scheme. The NSA's hope was that its seal of approval would drive the chip's adoption and these backdoored phones would be in common use. But the Clipper Chip was never adopted by industry and met its demise within a few years, due to privacy-minded backlash and the demonstration of critical vulnerabilities by well-known cryptographers.

CALEA

It was during this period, in the early '90s, that we started hearing law enforcement first sound the alarm about the perceived threat of criminals shielding their activities from detection through technological means including encryption.

The FBI in particular took this concern all the way to Congress, which in 1994 passed CALEA, the Communications Assistance for Law Enforcement Act. CALEA requires telecommunications carriers to make their networks and equipment technically capable of being wiretapped and having a pen register or trap-and-trace device installed, so that law enforcement is guaranteed to be able to implement a court order for those surveillance devices.

But there were **3** important limitations to CALEA when it was passed:

1) it doesn't allow law enforcement to dictate or prohibit specific designs for carriers' equipment, facilities, services, or features,

2) as originally written, it exempted the Internet ("information services"), and

3) it says carriers "shall not be responsible for decrypting, or ensuring the government's ability to decrypt, any communication encrypted by a subscriber or customer, unless the encryption was provided by the carrier and the carrier possesses the information necessary to decrypt the communication."

[47 U.S.C. § 1002(b).] These limitations came about as a result of a tooth-and-nail fight over the language and scope of CALEA between law enforcement, security experts, and civil liberties groups. CALEA reflects a **balance** that the members of Congress, who were accountable to the public, struck among competing interests including public order, security, and privacy, informed by mountains of evidence and expert testimony. The outcome was something that to law enforcement was a preservation of their *status quo*, but that die-hard civlib types believed gave up too much ground despite the carve-outs.

But the fight wasn't over. A decade after CALEA was passed, the FBI used an FCC rulemaking to get the law expanded in the digital-telephony age to cover Internet broadband providers, like ISPs, and certain VoIP providers. There was a legal fight, but the D.C. Circuit upheld it. (Law students: this is why Admin Law matters.)

In 2010, the FBI, citing what they called the "going dark" problem in an age of ubiquitous Internet-based services, pushed Congress to force *all* communications systems (like Gmail or Facebook), including all encryption software, to include backdoors for law enforcement access. The proposed bill died after an uproar. In 2013, the FBI again urged Congress, in vain, to extend CALEA to all communications services, so that companies with messaging services would have to backdoor their products and decrypt all encrypted messages.

These are the episodes that connect the '90s Crypto Wars to the present one. Effectively, these proposals would have undone two of the three exemptions that had been laboriously carved out from CALEA in 1994: the Internet carve-out and the encryption carve-out. The FBI had already taken a bite out of the former through the FCC, and in 2010 and 2013, it tried to finish the job. Yet in its PR efforts, the FBI painted these campaigns to extend CALEA as merely an attempt to preserve the *status quo* of access to your communications, not as an expansion of law enforcement powers.

Apple Introduces iOS 8

That was the mindset the law enforcement community still had in the fall of 2014, when the new crypto war started in earnest. The Supreme Court had just told the police in *Riley* that they had to get a warrant for mobile phone searches, so they were adjusting to that. And then, Apple added insult to *Riley*'s injury. The company announced iOS 8 for the iPhone, which would provide default encryption for iPhones that not even Apple could bypass for law enforcement.

In prior iOS versions 4-7, Apple could bypass the user's passcode and extract certain categories of data pursuant to a court order. In iOS 8, the files on the device are protected by an encryption key that commingles the user's passcode, which Apple doesn't know, with the device's unique ID, which Apple also does not know.

In short: Even if law enforcement did as the *Riley* Court said and got a warrant, Apple couldn't unlock iPhones anymore.

Law enforcement was *furious.* My law school classmates who became prosecutors all flipped out on Facebook about how terrible Apple was. FBI Director James Comey went to the press and to Congress, again threatening, as the FBI had done with its attempts to extend CALEA, that terrorists and pedophiles and murderers would "go dark." And Apple, he said, was helping these scum. It was downright un-patriotic.

The rhetoric was the '90s Crypto Wars all over again. But this time, it wasn't only data in transit that the FBI was worried about (though they're certainly worried about that too, given the prevalence of encrypted messaging tools including iMessage). With iOS 8, the issue was encryption for data at rest on our now-ubiquitous smartphones.

Just like in the '90s, law enforcement's attitude towards iOS 8 was that they were being *deprived* of something to which they had a *right* under the *status quo* which guaranteed them access to these devices. But that wasn't so. This source of evidence didn't exist due to a God-given edict or the natural order of things. Apple voluntarily started making iPhones in 2007, and they quickly became a treasure chest of information all collected in one pocket-sized place.

Law enforcement loved that. Inventing iPhones was a beautiful gift to law enforcement. It made their jobs so easy. But they only had access to the data on iPhones because Apple decided to build them that way. And now, with iOS 8, Apple had decided not to do that anymore. They would continue to comply with lawful process to the extent they could, but couldn't bypass their own advanced encryption. Apple had shown those treasure chests to law enforcement, and now it was yanking them away.

And if iPhones weren't so popular, it wouldn't have mattered so much to Comey and his colleagues. Like I said, what scared law enforcement about crypto in the '90s was that it was going to become readily available in commercial, off-the-shelf products. Law enforcement is used to having access to your information; they're not used to you having easy access to ways of protecting that information.

But the sky didn't fall after the '90s, even with the relaxation of crypto export controls and the CALEA carve-out for encryption. While commercially-available encryption became widely used to secure Internet traffic, e-commerce, banking transactions, and the like, it wasn't all *that* commonly used by Joe Average Consumer for laptops or mobile devices or browsing the web. You had to find a tool that would work on your setup and then you had to learn how to install it, configure it, and use it correctly. Encryption products have long been *infamously, notoriously, persistently, shamefully* user-**un**friendly in design. There are plenty of reasons for that, but the upshot is that Joe Average wasn't using PGP and Tor.

But what is Apple known for? Beautiful, clean design and an intuitive, easy-to-use user interface. Now, after the Snowden revelations in 2013, Apple had turned those core competencies to device encryption for the insanely popular iPhone.

Suddenly *millions* of people were going to have dead-easy access to strong encryption for data at rest, using just a passcode a few characters long. (Not only that, but for data in transit, Apple's iMessage uses end-to-end encryption, and it has competition from free apps such as Signal.)

That's what freaks out Jim Comey. He knows, and he's acknowledged, that determined, sophisticated criminals and terrorists will always find a way to encrypt their doings, no matter what U.S. law says or Apple does. But when a million Joe Averages deal weed or get in a brawl in a parking lot or get stopped by the cops just for the color of their skin, now not only can police not just rummage around their phones without a warrant, they may be unable to get into those phones at all. *Default* encryption on *consumer* devices in *widespread* use is a game-changer.

And it was perfectly legal. Apple was free to design iOS as it pleased. There was no law saying Apple couldn't design its phones to have strong encryption, or requiring Apple to put in only weak, backdoored encryption, or otherwise ensure access for law enforcement. This was the legacy of the '90s come to fruition. Apple was at liberty to make a smartphone it couldn't open for the police, even with a warrant.

iOS 8 turned the tables on the old "access for me, but not for thee" *status quo*. The lid was closing on the treasure chest. Law enforcement had gotten addicted enough that they'd convinced themselves that they had some immutable entitlement to the gift Apple had temporarily given them. What was Jim Comey to do?

Well, if making iOS 8 wasn't illegal, he'd make it so. He and his colleagues proposed to change the law to *force* the *status quo* back to where Apple had set it *voluntarily* pre-iOS 8. Comey and other officials called for legislation to require phone manufacturers, on pain of criminal fines, to build backdoors in device encryption which authorities could use to access encrypted data, but which couldn't possibly be exploited by bad guys. In essence, it was a CALEA II for mobile devices, but the exemptions – no design mandate, no application to Internet services, no duty to decrypt – would be filled.

The law enforcement officials calling for this legislation didn't offer any specific technical details of what this magical rainbow unicorn backdoor might look like. They left that up to the wizard-nerds in Silicon Valley. But even with the hand-waving as to specifics, the idea sounded like Clipper Chip 2.0, and it was just as roundly denounced by cryptographers as the first one. Law enforcement tried to paint Silicon Valley companies as being stubborn and unwilling to come up with a solution that could totally be invented if they would only nerd harder. Cryptographers responded that what law enforcement wanted was just plain

impossible. A backdoor can't be limited just to the good guys. It can and will be used by bad guys too.

Comey's idea didn't gain traction. Congress didn't seem interested in legislation, and the White House wasn't coming down one way or the other. Comey conceded in congressional testimony in early October 2015 that the administration had decided not to pursue a "legislative solution". Instead, he said, law enforcement would have conversations with tech companies to try to persuade them to voluntarily decide to backdoor their products. Instead of an open legislative process—which the FBI had already ducked in 2004 when they got CALEA extended through an FCC rulemaking rather than an act of Congress signed by the President—they'd put on pressure in meetings behind closed doors.

The All Writs Act

Even as Comey told a congressional committee about this supposed shift, the FBI and the DOJ were still going to federal court to get orders to bypass the passcode on pre-iOS 8 iPhones for which they had a warrant. The government had been filing these applications, *ex parte* and under seal, in dozens of cases since at least 2008, shortly after the iPhone first came out and before the 2010 and 2013 efforts at CALEA expansion. The legislative agenda was just one prong of the government's strategy to find ways to get around encryption. Like the private-meeting approach, going to court under seal let the government operate outside the light of public debate.

In their court applications, the DOJ lawyers didn't cite any governing statute specifically authorizing the technical assistance order to Apple that they sought. That's because, to Comey's chagrin, there isn't one, and sometimes they'd admit that. Instead, they'd argue that the requested order was authorized by the **All Writs Act**, a very old law which acts as a gap-filling residual authority for a court to issue writs not otherwise covered by statute. In its present version, the AWA provides that federal courts may "**issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law**." 28 U.S.C. § 1651(a).

Before the passage of the Pen/Trap Act in 1986, the AWA had been used in the '70s to authorize law enforcement to install pen registers on telephone companies' systems. The Supreme Court upheld that usage in the 1977 case *United States v. New York Telephone Co.*, 434 U.S. 159. Over three decades later, relying entirely on *New York Telephone*, the DOJ was telling federal magistrates around the country that the AWA authorized an order compelling Apple to provide technical assistance in unlocking iPhones. Even though Apple was a third party not directly involved in the underlying investigation, the government interpreted *New York Telephone* to authorize third parties to be compelled to assist with criminal investigations, so long as (1) they aren't *too* far removed from the underlying matter, (2) their assistance is absolutely necessary, and (3) the technical assistance is not unduly burdensome.

According to the government, Apple never objected to any of these orders. Law enforcement went to Apple with these "unlocking" requests for seized phones so often that Apple had a months-long waiting list. To streamline those requests, at some point Apple started requiring law enforcement to get a warrant or court order containing particular language that Apple specified. That language contained limitations on what Apple would have to do, so the government couldn't ask for more, and it didn't mention the All Writs Act. This choice by Apple, to go along to get along, was entirely understandable given the deluge of unlocking requests, but the government would use it against Apple later.

So: for years, the DOJ would submit Apple's form language in a proposed order, and each time they'd submit the same boilerplate brief in support of the request. That brief had one paragraph about the AWA and *New York Telephone* and one sentence of legal analysis that said *New York Telephone* gave the court authority to issue the requested order to Apple. That's it. In an "IRAC" format, the R was one paragraph and the A was one sentence.

And until early October of 2015, magistrates routinely signed off on the DOJ's proposed orders without alteration. In one 2014 case, a magistrate judge in SDNY wrote a separate opinion to give the thumbs-up to this use of the AWA, again based on *New York Telephone*, in a matter where the phone manufacturer's name was redacted—though he gave the manufacturer the chance to object to the order on burden grounds. By October, courts had entered at least 70 unlocking orders to Apple, for which the ACLU & I have submitted a FOIA request to the DOJ.

Orenstein to the Rescue

So, with Apple's form language, the government's boilerplate brief, and magistrate judges signing off unquestioningly, the machine of unlocking orders for pre-iOS 8 iPhones was humming along smoothly, even as Comey publicly grappled with how to deal with the advanced encryption in iOS 8 and, as of September 2015, iOS 9.

But then in early October, a magistrate judge in Brooklyn named James Orenstein received an unlocking request from the government for an iPhone, citing the AWA. This wasn't his first rodeo, though. Orenstein had seen the government try to argue for an overly expansive reading of the AWA's authority before. 10 years previously, he'd denied a DOJ request for real-time prospective cell site location data for a target cell phone, calling the government's AWA argument a "Hail Mary play" after he'd rejected its arguments under the Pen/Trap and Stored Communications Acts. He said the government's reading of the AWA was "breathtaking in its scope and fundamentally inconsistent with my understanding of the extent of my authority." 396 F. Supp. 2d 294, 326.

So when an Apple unlocking application somehow wound up in his court (a mistake that the requesting DOJ attorney must have quickly come to regret), Orenstein didn't

just sign off on it like so many other judges had before him. He issued an unsealed opinion on October 9 (which happened to be the Friday before the Monday when I started my job), refusing to grant the request until he'd heard from Apple.

Orenstein's order rejected the DOJ's All Writs Act argument. He reasoned that the Act, which is a gap-filling statute, cannot give the government "authority that Congress chose not to confer," and in passing CALEA, Congress did not choose to allow law enforcement to compel providers to decrypt devices. He distinguished *New York Telephone* in several ways:

- Apple's status as a private company, not a highly-regulated public utility, meaning it "is free to choose to promote its customers' interest in privacy over the competing interest of law enforcement";
- The existence of alternative legal means to obtain the information sought, meaning the unlocking order wasn't strictly necessary;
- The court's questionable ability to order Apple to unlock a device it manufactured, but does not own, particularly where it hadn't yet become clear that it was a pre-iOS 8 device (it was); and
- Congress's failure to show any intent to force Apple to provide the requested assistance to law enforcement, despite the FBI's expansion efforts I've mentioned.

Ultimately, the key factor in the judge's analysis was the question of the burden on Apple of unlocking the device at issue. Orenstein took briefing from Apple on the burden issue and from both parties on the applicability of CALEA and the scope of the AWA, particularly the ability to compel private actors to assist law enforcement. He held a hearing that lasted for two hours, where he pointed to another case pending in the same court in which an FBI forensic specialist had testified that the government has forensic tools to break into even iOS 8 devices, which suggested that he didn't need to order Apple to "do your work for you."

And then the criminal defendant whose iPhone it was pled guilty at the end of October. His sentencing was scheduled for the spring. After demanding to know why the guilty plea didn't render the unlocking request moot, Orenstein sat on the case for four months. In the meantime, the game changed again.

Paris and San Bernardino Happen

Shortly after the Orenstein case came to a lull at the end of October, the Paris attacks happened in mid-November. And soon after that, the San Bernardino shooting happened in early December. Rumors abounded that encrypted messaging tools had been used by both sets of attackers, though it turned out the Paris attackers had just used unencrypted SMS.

Suddenly, Comey and his colleagues, who'd *just* conceded they wouldn't seek a legislative solution, were emboldened to step back up. This was no surprise: in

September, a recent email from the intelligence community's top lawyer had been leaked, wherein he said that the legislative environment "could turn" to be anti-crypto "in the event of a terrorist attack or criminal event where strong encryption can be shown to have hindered law enforcement." Here was their chance.

In the wake of the attacks, CALEA II-type bills mandating that mobile device encryption be law enforcement-accessible were introduced in California and re-introduced in New York, where the Manhattan DA issued a report in November calling for federal backdoor legislation to fix the "going dark" problem he claimed, without much evidence, was plaguing his office. Senators in Congress promised a bill to "pierce" encryption. Another senator wanted to convene a crypto commission to "study" the problem of strong encryption vs. law enforcement access. Comey flew to Silicon Valley to meet with tech company leaders, so he got the closed-door meeting he wanted.

It was starting to look like law enforcement might be able to force that iOS treasure chest back open with a crowbar called "terrorism." Never mind that, as Comey admits, determined attackers will always find a way to encrypt their stuff. Never mind that the San Bernardino shooters killed people with guns, not iPhones. The specter of terrorism provided the perfect rationale for forcing Apple to make it easier again for the police to investigate Joe Average's low-level drug deals and assaults.

But again, the legislative proposals and the closed-door meetings turned out to be just two prongs in the FBI's anti-crypto strategy. It wasn't until mid-February that we saw the *piece de resistance*: the order the DOJ drafted, signed by Magistrate Judge Sheri Pym in Riverside on Feb. 16.

And that brings us to now.

The San Bernardino Order

As you probably know, the government had gone to Judge Pym asking for a technical-assistance order to Apple to help the FBI access an iPhone running iOS 9 that had been issued to one of the San Bernardino shooters, Syed [SIGH ED] Farook, by his employer, the County. The FBI got a search warrant for the device at 2 o'clock in the morning the night after the shooting. The County consented to the search of the device, which it owned. Because of the owner's consent, because Farook was dead, and because there was a search warrant, there is no Fourth Amendment issue in this case. It is not, in itself, a privacy case.

But the reason the FBI had to go to court was that they screwed up. They had the County's IT folks reset the password to the device's iCloud account within the first 24 hours after the attack. This was a huge mistake because changing the password meant the device wouldn't sync with iCloud and back up its most recent data. Apple does not encrypt iCloud, and so Apple could and did access Farook's iCloud account

for law enforcement. But there hadn't been an iCloud backup since mid-October. That meant the only way to get the last six weeks of Farook's data since the last backup was from the phone itself. But the only guy who knew the phone's passcode was dead.

Hence the request to Judge Pym. For reasons of its own, the government waited from early December until mid-February to go to court. And while the government had been in constant contact with Apple, which had provided as much data and voluntary assistance as it could, the government went to court without discussing the application with Apple beforehand. They *did* give notice to the press, though. And when they went to court, they took the unusual step of filing the application **not** under seal, as they had typically done. So Judge Pym didn't seal her order. This was something the government wanted us to see.

The order the government drafted and Judge Pym signed, without any alteration, cites the All Writs Act, just like other orders have. But it is fundamentally different from the unlocking orders the government had sought previously for pre-iOS 8 devices.

The FBI wants Apple to make it easier for the FBI to try to brute-force guess the passcode. To that end, the order compels Apple to create and cryptographically sign a special, crippled version of its iOS software that disables certain security features of iOS 9:

(1) a limit to 10 wrong passcode guesses, after which the phone locks down and won't let you guess anymore. Plus, if an optional feature is turned on, the phone erases all its data after 10 wrong guesses. The FBI doesn't know if this option is turned on.

(2) an increasing delay between guesses, meant to slow down attackers,

(3) making the user enter the passcode manually on the phone, when the FBI wants to hook the device up to a computer that will run through every combination of passcodes as fast as it can.

To be clear, none of this involves messing with the encryption on the phone. Apple can't decrypt the device, and the FBI isn't trying to require the impossible. This order is entirely about brute-force guessing the passcode as fast as they can. But that requires Apple to roll back features it had implemented to keep people from doing just that, since for most iPhone owners, their threat model is to keep their devices safe from thieves, hackers, abusive partners, or other snoops, not the police.

The government paints this order as modest. It's just this one phone, just this one time, they say. It's necessary to help investigate the worst Islamist terrorist attack on U.S. soil since 9/11. And it's not burdensome under the AWA. Apple made iOS; it makes software all the time, so it's NBD for them to write a little more software.

But this isn't modest. This case represents a major shift in the government's All Writs Act strategy. It isn't just attempting to compel Apple to do something the

company was already capable of doing, and had been doing voluntarily for law enforcement—namely, bypassing the passcode on devices running older versions of iOS. That was bad enough, and it already ran afoul of the AWA. But this order goes even further, stretching the AWA much too far to force Apple to create, and just as importantly sign, entirely new iOS software that doesn't presently exist.

The government's theory of the All Writs Act seems to have no limit on what it would permit a court to order a third party like Apple to do. Under its rationale, Apple, other smartphone makers, and manufacturers of the "Internet of Things" such as smart TVs, all could be compelled to turn their products into surveillance devices for law enforcement. Nothing in the All Writs Act or *New York Telephone* allows third parties to be dragooned into the service of law enforcement like that. The AWA doesn't let courts conscript private third parties to do the police's job for them. DOJ's reasoning leads to an extreme outcome—the commandeering of our consumer devices for surveillance purposes.

Not only is Judge Pym's order *legally* wrong, it also raises significant public safety issues. If Judge Pym's order stands, it won't be for just this one device to investigate a really bad terror attack. There will be more DOJ applications for more orders for more devices. The code will be used to investigate minor crimes that Joe Average commits. It'll be misused to keep tabs on the constitutionally-protected activities of political activists (just as DHS and at least one state AG's office have already done on social media to monitor Black Lives Matter activists). It'll be abused so that cops can surveil their ex-girlfriends.

And if a U.S. court can make Apple create this special code for U.S. law enforcement, then all the authoritarian jurisdictions where iPhones are sold will come to Apple wanting the same. They won't necessarily have the same due process protections we have. And some of them have criminal laws that are inconsistent with civil liberties and human rights – being gay, insulting the King, following a religion that isn't state-sanctioned.

If Apple says no, an authoritarian government could stop letting Apple do business in the country, seize its servers and property, or jail its in-country employees. We just saw that last week when Brazil briefly jailed a Facebook VP because Facebook didn't comply with a court order for user data from WhatsApp, a popular encrypted messaging service. And now France has a proposed bill mandating companies to decrypt data for police, with a 5-year prison sentence for employees if the company doesn't comply. And that's *France*, nominally a democratic country.

If Apple is compelled to create, cryptographically sign, and install this software, which Apple calls "GovtOS," then the code will be an attractive target to steal or buy. Apple may be compelled in future cases to hand over the code, even though Judge Pym's order allows the code to stay with Apple. But Apple has no control over law enforcement agencies' security practices, here or abroad. And as breaches at OPM and the IRS have demonstrated, the government's security practices suck.

Plus, even if the code always stays at Apple, Apple will end up creating a department of people charged with carrying out these law enforcement requests for the code, just like it streamlined the process for pre-iOS 8 unlocking orders. Each additional person who has to have access to the code presents a security risk. They'll be targeted with phishing scams, social engineering, blackmail, offers to buy the code for lots of money.

Judge Pym's order also poses a threat to the entire security ecosystem because it will undermine users' trust relationship with Apple and other device and app providers. The order doesn't just make Apple create new software, it makes Apple sign it. When Apple signs an iOS update, it's saying "Hey, this is Apple, we stand behind this software." But a cryptographically signed software update that Apple was compelled by the feds to create and transmit is indistinguishable to the end user and her device from an update the company created and sent out of its own free will. If people don't trust software updates, they won't install them, even if they're signed by Apple or the relevant vendor. But automatic software updates are a crucial means of maintaining device security. If left unpatched, devices can get infected and then become a vector for infecting other machines, such as when a mobile phone is linked to a desktop computer. This whole ecosystem is what's at risk if users stop installing software updates. In short, Judge Pym's order jeopardizes the security of everyone in the name of breaking into a single device.

None of this seems to have been taken into consideration by Judge Pym. That's not surprising, since the government's application was *ex parte*, meaning Apple didn't have a voice. But Judge Pym let Apple file a motion to vacate the order and explain why it would be unduly burdensome under the AWA. Apple filed that motion and explained not only the burden on it of complying, but that the AWA and *New York Telephone* don't authorize this sort of unprecedented dragooning of a private party at all.

Apple also echoed Judge Orenstein's rationale that CALEA occupies the field in this area of technical assistance, and because Congress chose not to confer authority to compel the assistance sought, the government can't use the AWA to get something Congress withheld. Apple also made arguments that the order violates its First Amendment right not to be compelled to speak – remember, in the last Crypto Wars, software source code was recognized as First Amendment-protected speech. Apple also made a Fifth Amendment substantive due process right to be free from an arbitrary deprivation of its liberty by the government.

Judge Pym also let the public request leave to file *amicus* briefs. So, my boss and I took her up on that. At the end of last week, we submitted an *amici curiae* brief

explaining the public-safety dangers I just outlined for you, on behalf of seven iPhone security and applied cryptography experts.[1]

The court accepted the brief, and we hope she reads it. Around 20 other *amici* submitted briefs and letters supporting Apple, and a lot of them made the same points we made about the far-reaching security consequences and international human rights implications of the court's order. And a lot of the briefs pointed out that the government's AWA argument is bunk, because there's no limitation to what private actors could be ordered to do. Some briefs, like the EFF's, made a First Amendment argument too.

Like I said, there were like 20 briefs, and I haven't read many of them yet. But Mike Masnick at Techdirt read all of them, and he wrote an article saying mine was the most interesting, so I guess I don't really need to read the others.

Orenstein Rides Again

Those *amicus* briefs all came in on Wednesday and Thursday of last week. A few days earlier, last Monday, something else had come out that amounted to an *amicus curiae* brief to Judge Pym. It came from Judge Orenstein. After sitting on the iPhone unlocking case before him since the end of October, he'd asked Apple to submit a list of other cases where the government was requesting device unlocking. Judge Pym's order came out later that same day, February 16.

On February 29, one week ago, Judge Orenstein issued his long-awaited order, denying the government's unlocking request in a scathing 50-page opinion. He totally demolished the government's All Writs Act theories, repeatedly calling it "absurd." He concluded it isn't "agreeable to the usages and principles of law" to "compel Apple – a private party with no alleged involvement in [the defendant's criminal activity – to perform work for the government against its will." He said the government's reading of the statute "would transform the AWA from a limited gap-filing statute that ensures the smooth functioning of the judiciary itself into a mechanism for upending the separation of powers." Ouch.

Orenstein stood by his CALEA analysis from his earlier October order. In CALEA, he reasoned, Congress had considered and declined to adopt a law mandating the technical assistance sought here, including any compulsion to backdoor Apple's products. Those exemptions in CALEA, the ones that were so hard-won in the '90s Crypto Wars, proved absolutely critical here. Congress, he said, knows how to require technical assistance from providers when it wants to: it did so in the Pen/Trap Act and the Wiretap Act. So, he concluded, Congress's silence in this particular context was a legislative choice, which could not be circumvented using

[1] iPhone security: Dino Dai Zovi, Charlie Miller, and Jonathan Zdziarski; applied crypto: Bruce Schneier, Prof. Hovav Shacham of UCSD, Prof. Dan Wallach of Rice University, and my colleague Dan Boneh at Stanford.

the AWA. The judge chastised the government for trying to do an end-run around the legislative process by using the courts to get its way. But Judge Orenstein is nobody's baby.

Orenstein's opinion was plainly laser-focus targeted at Judge Pym. It was the final act in a play he had orchestrated, seemingly on purpose, even though the government's San Bernardino ploy must have been as much a surprise to him as to the rest of us. Judge Pym's order for an iOS 9 device is fundamentally different from the pre-iOS 8 unlocking orders like the one before Judge Orenstein. But the government and Apple are both deploying to Judge Pym the AWA arguments they made in the Orenstein unlocking case.

Judge Orenstein had forced both Apple and the DOJ to come up with actual arguments about the AWA. He'd been the first and so far only judge to openly question the DOJ's AWA rationale. He made the government come up with something besides its boilerplate single paragraph of caselaw and single sentence of analysis. He'd also forced Apple to stake out a position on something it had been quietly going along with for years.

It turned out that the Orenstein case was a dress rehearsal for the San Bernardino case. As soon as his order came out, a bunch of people writing *amicus* briefs that were due in 3 days scrambled to rewrite them to include his opinion, which bolstered their arguments. Apple submitted it to Judge Pym as supplemental authority.

Judge Orenstein's order is not binding, of course, but it's thoroughly reasoned, and it utterly destroys the government's AWA argument, which was the only basis in law that the DOJ's application to Judge Pym cited for authority to issue the order. As I've said, the AWA is the *only* legal basis the government has *ever* cited in these technical-assistance applications, because as they've admitted, there's no law directly on point. Judge Pym can't ignore Orenstein's opinion, which magistrate judges around the country are reading now, and she'll be hard-pressed to figure out how to distinguish it.

That Brings Us to Today. So What Comes Next?

There will be a court hearing March 22, which will be the most exciting thing that's ever happened in Riverside, California.

Whether Judge Pym reverses herself or not, the case will surely be appealed to an Article III district judge and then to the Ninth Circuit. People are already talking about the Supreme Court, too. Maybe, if Judge Pym stands by her order and so do the Article III and the Ninth Circuit, but the EDNY and Second Circuit affirm Orenstein, there'll be a circuit split for an 8-person Supreme Court to hear somewhere around the year 2019.

I think the DOJ is going to fight in the courts as hard as it can. Remember, it sees all of this as preservation of the *status quo* under which it expects that it is absolutely entitled to access to data. That is, the government believes there should be no box that cannot be unlocked, no communication that cannot be eavesdropped upon. And they have shown that they are willing to sacrifice everyone's security to live in that world, even though robust security through encryption will *prevent* crimes too.

And because they're starting from a position of limited power under the Constitution, their incentive is to constantly seek to expand their power, even if in their minds, they're just preserving the *status quo*.

So I think the government won't stop using the courts unless we see a "magistrates' revolt" like the one Orenstein set off in 2005 when he denied prospective cell site location data requests made under the AWA. At that time, several other magistrates followed suit and issued similar orders in response to similar requests which, then as now, DOJ was filing around the US. (DOJ *still* makes those CSLI requests, 10 years later.)

But even if Judge Pym changes her mind in this case, the government can just judge-shop and forum-shop. It has a dozen pending requests for unlocking orders. Some of them involve iOS 8 or later phones. The government can keep poking until it gets another order, like Judge Pym's, that gives it what it wants.

That highlights why the courts are the wrong vehicle for deciding what Apple's duties are here. Everyone except the government, from Apple to Orenstein to *amici*, agrees that the courts are not the place for this decision. It's better left to Congress, which, as it did in passing CALEA, can take expert evidence and hear all sides, considering the civil liberties implications, the security implications, and whether strong crypto is actually, provably as big an impediment to law enforcement as they want us to believe.

But therein lies the rub—Comey and his ilk *want* a federal law. Their strategy has multiple prongs. Once they decided not to pursue a legislative solution, they tried to use the courts to get the result they wanted. If, like Orenstein, more courts say "no," Comey can point to that to prove there's a need for a legislative solution.

It may be that the battles in Judge Orenstein's and Judge Pym's courtrooms will lead directly to the passage of a CALEA II. It didn't work in 2010 or 2013, but maybe it'll stick this time.

I'd like to think that Congress might grow some guts and pass a law prohibiting the state and federal governments from dictating encryption design to anybody. A bill to that effect has already been proposed by Rep. Ted Lieu, one of four congressmembers with a CS degree. It's reminiscent of a legislative proposal that came close to passing in the '90s during the last round of the Crypto Wars, which was made by a representative from Washington State, namely the Microsoft district,

who's now a senator. If it had passed then, we wouldn't be having this debate today. But we get another chance now. So you can write to your congresscritter and tell them you are against a CALEA II and that you support a law guaranteeing that companies will be able to design encryption products free from government interference.

Unless and until a law does get passed, we're seeing a groundswell of interest in encryption software. As I mentioned, there are many free encrypted messaging tools out there, of varying degrees of security. The lessons for product design going forward are not to roll your own crypto, because doing it right is really hard, and to MAKE YOUR PRODUCTS USER-FRIENDLY.

The government's worst enemy in this fight is not the existence of strong encryption. It's strong crypto that's made easy to use by default and put in the hands of millions. That was Apple's killer app in designing the encryption in iOS 8, and that's what finally brought about the crypto revolution, 20 years late. Normalizing that kind of protection matters. Apple and the FBI are fighting in the court of public opinion too.

This is not just about one dead terrorist's iPhone. It's about what we want the built environment of electronic communications and storage to look like, particularly as the Internet of Things comes of age. We have the chance to push back against the surveillance state, to turn around "access for me, but not for thee," and make it work for us. It's absolutely imperative that we succeed.

Thank you.