BUSINESS PRIVACY

Inside Apple CEO Tim Cook's Fight with the FBI

By Lev Grossman

In an exclusive interview with TIME, Cook discusses your privacy, America's security, and what's at stake in the battle over encryption

The day after the massacre in San Bernardino, Calif., where Syed Rizwan Farook and Tashfeen Malik shot to death 14 people and wounded 22 others at a holiday luncheon for the county department of public health, an FBI Evidence Response Team descended on the couple's townhouse in nearby Redlands.

They recovered, among other things, 12 pipe bombs, thousands of rounds of ammunition of several different calibers, and three cell phones: two from a dumpster behind the townhouse and one from the center console of a black Lexus IS 300 parked outside. The two phones in the trash had been crushed by the terrorists, but for whatever reason—maybe an oversight, maybe there was nothing useful on it, who knows—the third phone was intact. It was placed in the care of the Orange County Regional Computer Forensics Laboratory. When investigators booted it up—it was an iPhone 5c running iOS 9, on the Verizon network, serial number FFMNQ3MTG2DJ—the phone asked them for a four-digit pass code.

What followed was like a kid's game of fortunately-unfortunately. Unfortunately, they didn't have the pass code, and the person who did was dead. (Farook and Malik were killed in a shoot-out with police a few hours after the attack.) They could have tried to guess it, but the phone was set up to erase itself after 10 wrong guesses. Fortunately, the phone was Farook's work phone, so technically it belonged to San Bernardino County. Unfortunately, the county didn't have the pass code either, nor did it have the password for the iCloud account associated with the phone, which in the Apple security ecosystem is different from the phone's pass code.

But the county did have the power to reset the iCloud password, which it did. That iCloud account turned out to contain several full, unencrypted backups of the phone. Unfortunately, Farook hadn't backed up his phone to iCloud since Oct. 19, so the data was out of date. Further misfortune: not all the information on an iPhone is necessarily included in a backup.

All that data was still on the phone, but encrypted with a pass code that nobody had. Not even, amazingly, the company that made the phone: Apple.

The FBI did ask. “We didn’t hear anything for a few days,” says Tim Cook, Apple’s CEO and the successor to the late Steve Jobs. “I think it was Saturday before we were contacted. We have a desk, if you will, set up to take requests from government. It’s set up 24/7–not as a result of this, it’s been going for a while–and the call came in to that desk, and they presented us with a warrant as it relates to this specific phone.”

At 55, Cook is wiry and silver-haired, with an Alabama accent that he has carefully transplanted to Silicon Valley. We spoke in his office at Apple’s headquarters in Cupertino–the address, famously, is 1 Infinite Loop. It’s a modest office, an askew trapezoid, almost ostentatiously unostentatious, with a few framed “Think Different” posters on the walls, some arty photographs of Apple stores and a large wooden plaque with a quote from Theodore Roosevelt on it (the “daring greatly” one). Jobs’ office is next door. It’s dark, with curtains drawn, but the nameplate is still there.

To be clear: Apple complied with, and actively assisted, the FBI’s investigation, right up until it didn’t. There was plenty of cordial back-and-forth, exchanges of information and know-how. “We gave them some unsolicited advice–we said, take the phone to the home or apartment and power it, plug it in and let it back up. And as it turned out, they came back and said, Well, that didn’t work.” It emerged that resetting the iCloud password had been a serious tactical error: they could’ve gotten the phone to make a fresh backup of itself automatically, but once you change the iCloud password, it won’t back itself up without the pass code.

That’s when the FBI made a further request: O.K., Apple didn’t have the pass code, but maybe it could code up a new version of iOS 9 without the 10-guess limit (and without enforced pauses between guesses, another security measure) and then persuade the San Bernardino phone to install it? A four-digit pass code has only 10,000 possibilities. The FBI could brute-force that in a day and everybody could go home.

Inside Apple this idea is nicknamed, not affectionately, GovtOS. “We had long discussions about that internally, when they asked us,” Cook says. “Lots of people were involved. It wasn’t just me sitting in a room somewhere deciding that way, it was a labored decision. We thought about all the things you would think we would think about.” The decision, when it came, was no.

Cook actually thought that might be the end of it. It wasn’t: on Feb. 16 the FBI both escalated and went public, obtaining a court order from a federal judge that required Apple to create GovtOS under something called the All Writs Act. Cook took deep, Alabaman umbrage at the manner in which he learned about the court order, which was in the press: “If I’m working with you for several months on things, if I have a relationship with you, and I decide one day I’m going to sue you, I’m a country boy at the end of the day: I’m going to pick up the phone and tell you I’m going to sue you.”

It also wasn't lost on Cook that the FBI chose not to file the order under seal: if Apple wasn't going to help with a case of domestic terrorism, the FBI wanted Apple to do it under the full glare of public opinion.

The spectacle of Apple, the most admired company in the world, refusing to aid the FBI in a domestic-terrorism investigation has inflamed public passions in a way that, it's safe to say, nothing involving encryption algorithms and the All Writs Act ever has before. Donald Trump asked, "Who do they think they are?" and called for a boycott of Apple. A Florida sheriff said he would "lock the rascal up," the rascal meaning Cook. Even President Obama, whose relations with the technorati of Silicon Valley have historically been warm, spoke out about the issue at South by Southwest: "It's fetishizing our phones above every other value. And that can't be the right answer."

As against that, Apple has been smothered in amicus briefs from technology firms supporting its position, including AT&T, Airbnb, eBay, Kickstarter, LinkedIn, Reddit, Square, Twitter, Cisco, Snapchat, WhatsApp and every one of its biggest, bitterest rivals: Amazon, Facebook, Google and Microsoft. Zeid Ra'ad al-Hussein, the U.N. High Commissioner for Human Rights, spoke out in Apple's defense. So did retired general Michael Hayden, former head of both the NSA and the CIA. The notoriously hawkish Senator Lindsey Graham, who started out lambasting Apple, switched sides after a briefing on the matter. Steve Dowling, Apple's vice president of communications, showed me a check for $100 that somebody sent to support the world's most valuable technology company in its legal fight. (Apple didn't cash it.)

You can see what the fuss is about. The optics of Apple's decision are pretty terrible, and the reasons for it aren't obvious or simple. The main reason is technical: if Apple created what amounts to a tool for cracking open iPhones, Cook argues (and security experts tend to agree), and that tool got out into the wild, through hacking or carelessness, the security of every iPhone everywhere would be compromised. This is not an unlikely scenario: code, like the dinosaurs in Jurassic Park, often finds a way to get free. Under this scenario, GovtOS would be the holy grail for hackers everywhere and a gift to authoritarian governments willing and eager to pry into their citizens' secrets. "To invent what they want me to invent," Cook says, "puts millions of people at risk."

To be clear, Cook doesn't mean people are at risk of having their nude selfies put online. He sees the risks of hacking as real, real enough to weigh against the nightmare of a possible terrorist attack. "It's not that one side has life and one side is your financial information or your photo or whatever," he says. "Think about something that happens to the infrastructure, where there's a power-grid issue. Think about the people who are on a medical device that depends on electricity … these aren't fantasy things by any means." (He also doesn't think that GovtOS would help the FBI much anyway, but more on that later.)

The FBI has argued that the new code could be tailored to just that one phone in particular, but modifying the code to attack other phones would be relatively simple.

Apple also maintains (and the FBI has as good as conceded) that this case isn't a one-off: it will set a legal precedent. And even if Apple deleted the tool as soon as the FBI was done with it, there would be a line around the block of district attorneys clutching iPhones in evidence baggies demanding that Apple write it all over again. "It's not about one phone," Cook says. "It's very much about the future. You have a guy in Manhattan saying, I've got 175 phones that I want to take through this process." (The guy in question being New York County district attorney Cyrus Vance, who did in fact say that.)

This is the technical argument. Apple's legal argument in the case hinges on the interpretation of the All Writs Act, which is something of a catchall: it authorizes federal courts to issue "all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law." Apple's lawyers argue that to compel the company to write, test, debug, deploy and document the necessary software would be excessively burdensome and exceed the bounds of the All Writs Act. (This isn't the first time Apple has been on the business end of the All Writs Act, by a long chalk. In October a similar case came up in Brooklyn involving a meth dealer who claimed to have forgotten his iPhone pass code, and Apple made a similar argument. On Feb. 29 the judge ruled in Apple's favor, though that ruling has no legal bearing on the San Bernardino case.) Apple also floated a slightly more fanciful claim to the effect that compelling Apple engineers to write code they objected to would violate their First Amendment rights.

But these arguments are just the legal and technical shadows cast by another, larger one, which is that people have a right to privacy, and devices like the iPhone, with which we live on terms of unprecedented intimacy, provide both hackers and law enforcement with a way of invading that privacy like never before. Encryption is the only possible countermeasure. "When I think of civil liberties, I think of the founding principles of this country," Cook says. "The freedoms that are in the First Amendment, but also the fundamental right to privacy. And the way that we simply see this is, if this All Writs Act can be used to force us to do something that would make millions of people vulnerable, then you can begin to ask yourself, If that can happen, what else can happen? In the next Senate you might say, Well, maybe it should be a surveillance OS. Maybe law enforcement would like the ability to turn on the camera on your Mac."

It's an argument in favor not just of privacy but of a new kind of privacy, one forced on us by the utterly changed nature of the technological environment we now live in. Device by device, service by service, we have built over the past decade a world in which an amazing amount of what we do is recorded by our personal devices: our social lives, our health, our money, what we watch, who we talk to, where we go, what we look at. Ten years ago, if I went for a jog, any and all information relating to that jog would evaporate as soon as it happened. It would go uncaptured. Now that information is not only preserved–where I went, how far I went, how fast I went, what I listened to, what my heart rate was–it gets uploaded to the cloud and propagated across my social networks.

The legal scholars Peter Swire and Kenesa Ahmad have coined a phrase for this: the Golden Age of Surveillance. Idly and thoughtlessly, purely because we like the little

conveniences and personal services that smart devices give us, we have comprehensively bugged ourselves but good. Devices like Amazon's Alexa or Samsung's smart TVs or even Mattel's Hello Barbie not only monitor the conversation around them but stream it to the cloud to be run through speech-recognition algorithms. They listen and report.

George Orwell knew mass surveillance would invade our homes. The twist he didn't see coming was that it wasn't Big Brother who would do it. We did it to ourselves. "It wasn't very long ago when you wouldn't even think about there being health information on the smartphone," Cook says. "There's financial information. There's your conversations, there's business secrets. There's probably more information about you on here than exists in your home." The question is, now that we have this deeply, richly, intimately installed new surveillance infrastructure, should Big Brother be allowed to access it? And if so, when and how? Or should private citizens have the means to protect it, from hackers and thieves but also from the government?

Oddly enough, this particular fight has actually been fought before, more than 20 years ago, in what is known as the Crypto Wars. In 1993, jittery in the face of the growing power of encryption, the White House announced a device called the Clipper Chip that would encrypt digital communications while allowing the government to keep a key. Needless to say, the industry resisted the Clipper Chip on any number of grounds, including the fact that it would render American-made communications technology distinctly unattractive to foreign buyers. By 1996 it was effectively dead, and by 2000 the government had thrown up its hands at the whole quixotic business of trying to legislate encryption.

Strong encryption remained the exception rather than the rule, even as American cybersurveillance ramped up in the wake of Sept. 11. But by 2011 law enforcement was getting concerned again about its practical ability to monitor electronic communications. The FBI's general counsel described them as "going dark," a phrase that has become something of a rallying cry.

After the Edward Snowden revelations in 2013, some technology companies began integrating encryption more tightly and seamlessly into their products and enabling it as the default setting–Apple's iOS 8, released in 2014, was a watershed in that respect. Google's next release of Android did the same. There were already rumblings about encryption legislation long before lightning struck in San Bernardino. Last year, the Washington Post quoted an email from Robert S. Litt, second general counsel in the Office of the Director of National Intelligence, which speculated, presciently, that the general climate for such legislation "could turn in the event of a terrorist attack or criminal event where strong encryption can be shown to have hindered law enforcement." And here we are.

Law enforcement has long been accustomed to obtaining warrants to search almost anything it wants, subject to the limits spelled out in the Fourth Amendment. (That's the one about "unreasonable searches and seizures.") But encryption creates a new kind of

warrant-proof space, a virtual bolt-hole in which private citizens can put the vast amounts of sensitive personal data they generate. It's still accessible to law enforcement in theory, but in practice it's impenetrable without a pass code.

FBI Director James Comey put this new predicament starkly in a congressional hearing on the San Bernardino case in February. "Law enforcement, which I'm part of, really does save people's lives, rescue kids, rescue neighborhoods from terrorists," he said. "And we do that a whole lot through court orders that are search warrants. And we do it a whole lot through search warrants of mobile devices. So we're gonna move to a world where that is not possible anymore? The world will not end, but it will be a different world than where we are today and where we were in 2014."

Comey, who declined to be interviewed on this subject, has framed the conflict as a choice between privacy and security, a zero-sum trade-off. If it were that simple, Apple would have a steep battle indeed: whatever benefits we get from encryption would have to be weighed against the possibility of lives lost to acts of terrorism. But Cook flatly rejects this view as a red herring. "I think it's very simplistic and incorrect," he says. "Because the reality is, let's say you just pulled encryption. Let's you and I ban it tomorrow. And so we sit in Congress and we say, Thou shalt not have encryption. What happens then? Well, I would argue that the bad guys will use encryption from non-American companies, because they're pretty smart, and Apple doesn't own encryption."

In other words, GovtOS wouldn't help much, because there's no legislating away encryption. The bad guys will remain encrypted as ever, no matter what. "The Internet doesn't have boundaries," Cook says. "You can wind up getting an app from Eastern Europe or Russia or wherever, it doesn't matter which country, just outside the United States. And that app would give you end-to-end encryption." Sure, you might get the data off Farook's phone, but that's the last one you'd get. Then you're back where you started, except worse off, because everybody else's crypto is now more vulnerable, with their data ripe for the pillaging. You're only punishing the good guys.

The stakes are rising on both sides. In 2015 alone, the federal Office of Personnel Management was hacked to the tune of 22 million personal records; hackers released 32 million accounts from AshleyMadison.com, a site that facilitates adultery; and Anthem, the IRS and the director of the CIA got hit as well. "Think about the things that are on people's phones," Cook says. "Their kids' locations are on there. You can see scenarios that are not far-fetched at all where you can take down power grids by going through a smartphone." This isn't entirely speculative: in December somebody managed to take down part of the power grid in western Ukraine, leaving 230,000 people without electricity. "We think the government should be pushing for more encryption," he says. "That it's a great thing. You know, it's like the sun and the air and the water."

Except that it protects terrorists as well as good guys. "We get that," Cook says. "But you don't take away the good for that sliver of bad. We've never been about that as a country. We make that decision every day, right? There are some times that freedom of speech,

we might cringe a little when we hear that person saying this and wish they wouldn't. This, to us, is like that. It's at the core of who we are as a country."

Encryption is one of those technological realities that are so ubiquitous and powerful that they alter political realities–it has a whiff of revolution about it. It changes the balance of power between government and governed.

Apple isn't in the business of revolution, or not that kind anyway. Cook's emphasis is on the extent to which encryption protects your data from the bad guys, the hackers and other malefactors, rather than from law enforcement–but at the same time he does convey a certain leeriness about the government's unseemly eagerness to get at personal information. "I'm the FedEx guy," Cook says. "I'm taking your package and I'm delivering it." He doesn't want Apple to be in the position of storing messages for the government to read. "I'm not saying that from a cost point of view or anything else, I'm saying it from an ethics and values point of view. You don't want me to hold all that stuff. Right? I think you guys should have a reasonable expectation that your communication is private."

He also points out that the All Writs Act doesn't specify what kinds of criminal investigations it applies to. "This case was domestic terrorism, but a different court might view that robbery is one. A different one might view that a tax issue is one. A different one might view that a divorce issue would be O.K. And so we saw this huge thing opening and thought, You know, if this is where we're going, somebody should pass a law that makes it very clear what the boundaries are. This thing shouldn't be done court by court by court by court." (Cook can't completely conceal his irritation at the un-Apple-ish vagueness of the All Writs Act: "You can tell it was written over 200 years ago." As if to say, they ought to let Jony Ive loose on that thing, get it milled to the proper tolerances, upgrade it to a respectable level of precision.)

Whether it will or won't be decided by courts is an open question. The FBI, in a series of increasingly strident court filings, has accused Apple of undermining "the very institutions that are best able to safeguard our liberty and our rights: the courts, the Fourth Amendment, long-standing precedent and venerable laws, and the democratically elected branches of government." It has also threatened, not very subtly, to unleash a nuclear option: subpoena the iOS source code and Apple's "private electronic signature," the certificate with which it identifies its code as valid to its devices, which is the software equivalent of the secret name of God.

As for Cook's talk about privacy and civil liberties, the FBI dismisses it as "marketing." It's fair to say that emotions are running high on both sides. "Do I like their tactics?" Cook says. "No, I don't. I'm seeing the government apparatus in a way I've never seen it before. Do I like finding out from the press about it? No, I don't think it's professional. Do I like them talking about or lying about our intentions? No. I'm offended by it. Deeply offended by it."

To be sure, Cook has been positioning Apple as a defender of personal privacy for some time now, at the expense of several of his key rivals–Cook is fond of pointing out that Apple's business model doesn't involve harvesting and mining its users' data the way that, say, Google, Facebook and Amazon do. (At Apple a lack of interest in customer information is practically gospel–Jobs used to claim that Apple didn't even use focus groups.) Cook's stance is also of a piece with Apple's well-known obsession with top-down control of every detail of its products. For the government to come in and get its grubby, inky federal fingers on Apple's perfect gleaming code must be excruciating at 1 Infinite Loop.

It's ironic that Cook's tough stand on privacy has forced him further into the spotlight. By nature he's as intensely private as the CEO of Apple can be. It also represents another step in a curious trend that has Silicon Valley engineers increasingly acting like statesmen and policymakers, taking positions and making decisions on political and social issues. As more and more of our social and cultural fabric gets integrated into the Internet, power over that fabric is being siphoned off, through mysterious cross-country subterranean channels, from Washington to Northern California. "We're in this bizarre position where we're defending the civil liberties of the country against the government," Cook says. "I mean, I never expected to be in this position. The government should always be the one defending civil liberties, and yet there's a role reversal here. I still feel like I'm in another world, that I'm in this bad dream."

Cook is doing his best to wake up. He says he doesn't actually want to make this decision. What he's pushing for is to get it out of the hands of a judge and into Congress; a commission could study the issue and presumably propose some sensible laws to clarify it. "We see that this is our moment to stand up and say, Stop and force a dialogue," he says. "There's been too many times that government is just so strong and so powerful and so loud that they really just limit or they don't hear the discourse." He stresses that whatever the outcome, when the law is handed down, Apple will follow it.

In the meantime, product development in Cupertino will continue to race ahead at the speed of technology, which is considerably faster than that of congressional commissions. It has been reported–though not confirmed–that Apple is evolving a version of the iPhone that even it couldn't crack, not even with the help of GovtOS. It's theoretically possible: if, just for example, the 10-guess requirement in iOS 9 could be incorporated into the phone's hardware, rather than its software, then even modifying the operating system wouldn't get rid of it. No one talks about future products at Apple–to do so would bring the ghost of Jobs howling back from Silicon Valhalla–but Cook says nothing that makes me think it's not going to happen. "I would never do what you're saying with the intention of doing that," is how he puts it. "Our intention is never anything to do with government. It's to protect people. Is it a consequence of it? Yes, I mean, over time you do more and more and more. That's the road we've been on for a decade." The effect would be to render controversies like the present one moot and remove Apple from the legal equation completely, bootstrapping it out like the Lorax.

Cook also suggests that with all those huge invisible billowing clouds of data we leave behind everywhere we go, the encrypted data on phones just isn't that big a deal anymore. Law enforcement shouldn't be whining about iPhones; it should be rolling around in all the other free information that criminals and terrorists are spewing through social networks and Nest thermostats, surveillance cameras and Hello Barbies. Apple even has the keys to iCloud backups, which are readily subpoenable, so why get hung up on the device itself? Which, by the way, 10 years ago didn't even exist? "Going dark–this is a crock," Cook says. "No one's going dark. I mean really, it's fair to say that if you send me a message and it's encrypted, they can't get that without going to you or to me, unless one of us has it in our cloud at this point. But we shouldn't all be fixated just on what's not available. We should take a step back and look at the total that's available, because there's a mountain of information about us."

Its slightly exasperated tone aside, this argument echoes the findings of a report published in February by Harvard's Berkman Center for Internet & Society and signed by an impressive roster of legal and security professionals. The report points out that there are powerful trends at work that balance the spread of encryption: the prevalence of business models that rely on mining users' data; the growth of cloud computing, which puts data on central servers that are more easily accessible; and the proliferation of networked devices referred to collectively as the Internet of Things. "These are prime mechanisms for surveillance," the report says, "alternative vectors for information-gathering that could more than fill many of the gaps left behind by sources that have gone dark–so much so that they raise troubling questions about how exposed to eavesdropping the general public is poised to become."

In fact, we seem to be going through two equal and opposite crises at the same time, depending on who you listen to. On the one hand we're going dark, and on the other we're giving away our privacy left and right. These are local effects that need to be integrated into a bigger picture. Bottom line: the Internet is a vast, messy, porous place, and that same messiness that makes encryption impossible to regulate also means that however strong and seamless and pervasive encryption gets, it can only ever cover a fraction of the data that flows out of us all day, every day.

The next round in the shoving match between Apple and the FBI is set for March 22, when both sides will appear at a hearing in federal court in Riverside, Calif. Sooner or later, all that shoving will have to yield to a delicate balance, one that takes into account the realities of what encryption is and what it isn't, and leaves us with a legal framework strong and clear enough to spare us from having to refight the Crypto Wars a third time. "You know as well as I do, sometimes the way we get somewhere, our journey is very ugly," Cook says. "But I'm a big optimist that we ultimately arrive at the right thing."

This appears in the March 28, 2016 issue of TIME.