
Tim served as the first Director of Privacy and Civil Liberties for the Obama White House national security staff, and is following this case closely. Tim, do you see a fundamental conflict at the heart of the Apple v. FBI arising from the different ways lawyers and technologists view privacy? Fill us in on that conflict.

TIM EDGAR: Sure. One problem that we’re seeing in the whole debate over access to encrypted communications is the different ways in which lawyers and technologists use words. And here, I’d like to talk about the word privacy. What does a lawyer mean when he or she says privacy, and what does a technologist mean when he or she says privacy? Because they mean two very different things, even though they’re using the same word.

So, when I talk about this in my classes, I like to use the example of Louis Brandeis, who is the great Supreme Court Justice, the author of The Right to Privacy, one of the greatest thinkers in American law on this topic. His famous dissent in Olmstead v. United States was all about this concept. In that case, the Supreme Court had to decide whether wiretapping was an invasion of a right protected under the Fourth Amendment. And that was in the late 1920s, telephones were a new technology.

And most of the court just couldn’t get their mind around the idea that this was a search, to listen into somebody’s telephone conversation, because they said, well, you’re not invading their home or searching their body. There’s nothing physical being invaded. And this really rubbed Louis Brandeis the wrong way. Justice Brandeis said, no, no, an intangible invasion of privacy is a search under the Fourth Amendment, just like a tangible, physical search is. And it went all the way back to his earlier work, when he wrote that Law Review article, "The Right to Privacy."

So he talked about how privacy was the most comprehensive of rights. It was the right most valued by civilized people. It was the right to be left alone.

But then when he gets into talking about, what does that actually mean, he starts using wiggle
words, which is something that lawyers always do. They talk about reasonableness. They talk about whether something is justifiable. He said, unjustifiable intrusions by the government on the privacy of the individual must be deemed a violation of the Fourth Amendment.

Well, what does he mean when he says unjustifiable? Well, of course, what he means is that the Fourth Amendment gives you a right against unreasonable searches-- not against all searches, just against those searches that the law deems unreasonable. And the most important thing when it comes to a search, for a lawyer is, has there been a warrant issued to justify the search? So that's what Louis Brandeis was talking about.

Now then I wanted to think about, well, what's an example for technologists of the word privacy being used in a similar, sort of seminal way? And I went back to a very famous paper published in 1978, by three famous technologists-- Adi Shamir, Ron Revest, and Len Adleman. This is the famous RSA paper, the paper that made it possible to have public key cryptography in a usable and practical way. It had been already developed in theory, but Shamir, Rivest, and Adleman made it something that was really practical and usable. It's what underlies all of the privacy on the internet today.

So, they defined in their paper what they meant by privacy. They said, encryption is the standard means of rendering a communication private. And they introduced the famous characters of Alice and Bob. This is the first paper that talks about Alice and Bob.

So they said, how can Bob send a private message to Alice? That's the question. Without Eve listening in. And they defined privacy as an intruder listening in on the channel cannot decipher any message, because it is not possible to derive the decryption key from the encryption key. That's what a technologist means when they think something is private. In other words, the system is either secure, in which case it's private-- Eve can't listen in on Alice and Bob-- or it's breakable, in which case it's not private.

So you see, there's no wiggle room in that definition. It's not a lawyerly definition. They're not talking about, well, can we prevent unjustifiable listening in on Alice and Bob? Well, we don't care whether something is justifiable or not. If you can listen in, it's not private. If you can't, then it is private.

So, what does that mean for FBI v. Apple? Well, you see this exact same dichotomy happening. You look at the FBI director, Jim Comey. He says, we're just trying to search somebody's phone with a warrant. We want Apple's help to do that.
We're not looking for a back door. We're looking for a front door. We're going to go in with legal process, a judge’s order, and say, please help us unlock this phone.

But then Apple looks at it and they say, oh, if we do that, we set a precedent that our phone can be broken into. It’s no longer private. If we do it for you, Mr. Comey, even in the most justifiable of circumstances-- well, how do we draw the line when some other government asks us to do the same thing, maybe under a circumstance where we don't think it's justifiable? Once we've broken our phone, it’s broken and we can be asked or forced to use that key over and over again.

So you see this fundamental clash playing out in *Apple v. FBI*, between the lawyer who says privacy is when you’re able to protect your communications legally, where you need a judge’s order and a warrant to invade that privacy. But technologists say, no, privacy is when you can protect your communications technically, where they can’t be broken into. And the strongest definition of privacy-- actually, Apple fails. Because in the strongest definition of privacy, even Apple can't break into it.

So technologists look at this case and they say, the problem here is that Apple created a phone that they could break. And the solution is for Apple to create a phone that they can't break. A lawyer would look at this and say, the problem here is that we don't have a way to break into communications when society needs to. But if we create that way, maybe we create insecurity for everybody else, and so this is a policy dilemma that we have. And so, the two communities are in some ways, talking past each other.

**ALAN USAS:** That's very interesting, Tim. I think what it reminds us is there is a technical language, really on both sides of this, that is technical lawyer language. And there is technical technologist language. And we are really in a clash between those two worlds. On the legal side, we have the courts. And I wonder if you could talk about how you expect the courts to play into this issue between Apple and the FBI?

**TIM EDGAR:** So, fascinating issue, because it raises issues that are statutory-- very important under the All Writs Act. It also raises constitutional issues-- not just the Fourth Amendment, but the First Amendment. So I want to go into each of those.

The biggest issue, probably, that's going to resolve the case is under a very old law called the All Writs Act that was passed in 1789 at the same time as the Bill of Rights was passed. And it
basically empowers the courts to issue orders necessary to execute other orders that they've issued. So, the court has issued a search warrant, and the government says, we need another order to make that search warrant effective, an order against Apple to require them to provide us with assistance.

And there's an old case, not as old as 1789, but in internet terms, just as ancient. It comes from 1977, it's called United States v. New York Telephone Company, and it required the telephone company to help the government install a pen register device, which tracks metadata, on its property. Very analog case. For those of us who are surveillance geeks, it's a lot of fun to go back and read these old cases, and read about the technology, because it's just so different than the technology today.

And basically, the issue in that case, the telephone company says, we don't want to be involved in your surveillance activities. You want to install a device, go ahead, but don't make us provide you with the phone line and the facilities to do it. The Supreme Court said, no, you do have to help the government provide this. But we're going to put some limits on the government's power here to make sure that this doesn't go too far.

And the limits were, you have to have some relationship to the search-- and in that case, they found there was, because the criminal investigation was using the lines that the telephone company had. It can't be an unreasonable burden for the telephone company to do this. In that case, they said, that was fine because they use this sort of equipment all the time to check billing. And the third was, it needs to be necessary to execute the search warrant. Those were the three standards.

Now, all those standards are at issue in the Apple case. So the government says, well, this is an Apple phone, you designed the operating system, you update the operating system, that gives you enough of an access to the phone. Apple contest that and says, no, we're just selling a device. It's different than a phone company that has its own equipment and lines involved.

So, the second point is reasonableness. That's the big issue, I think, in the case. Apple is saying, this is an unreasonable burden on us. You're making us hack our own phone. You're making us do something we find to be very offensive-- that was a term used by the Supreme Court in the earlier case, saying it wasn't offensive for them to track phone numbers dialed.

So, Apple has a pretty strong case on this whole issue of being unreasonable. The real issue
is going to be, are they going to look at that very narrowly, the way the government wants them to? The government just wants to look at how difficult is it for Apple to create this software. Apple wants them to look much more broadly at the burden. What's the impact on their business, on their reputation, on the security of the internet?

So that's the big statutory issue. If it's resolved in Apple's favor on the statutory issue, we don't get to the First Amendment issue, which is even more interesting. Apple is making a First Amendment argument that code is speech. The computer code is like speech. And therefore, if you're forcing them to write code that they don't agree with and stand by, computer code that breaks their phone, that you're compelling them to speak, and to say something they disagree with, and that violates the First Amendment.

In the case of New York Telephone, that issue didn't come up, because we weren't writing computer code. So now we're writing computer code, and the government is saying, we can force you to write certain kinds of computer code. And now, technology companies and software companies have a new argument that they can't be forced to write computer code to government specifications, because they have a First Amendment right to express themselves through computer code. So that's a very interesting argument as well.

**ALAN USAS:** It sure is, Tim, and thank you very much for your provocative perspective on this complex issue. In future podcasts, we'll share additional perspectives on Apple v. FBI, and on other cyber issues. For information on future podcasts, program news, and upcoming events, visit brown.edu/cybersecurity.