
# A Conversation on Privacy – Part 5

*Note: This transcript may not be 100% correct.*

**Nuala O'Connor:** So bringing the terrorism and national security conversation back to each of us individually and locally, obviously a critical case working its way through the courts right now is Apple v. FBI. I'm incredibly proud, by the way, of the CDT (The Center for Democracy and Technology) Amicus Brief and I'll just give away the punchline that we are firmly on the all pro encryption side of that case. I want to ask the panel what their thoughts are and what this case signals for individual liberties and individual privacy in the truly always on digital world. But to crystalize this question from the CDT chief technologist Joe Lorenzo Hall who writes: We have never had so much of our environment networked and computerized and we have never had the ability for average citizens to hold truly hard secrets, secrets that frustrate even the most powerful government access through our increasingly secure mobile devices. Do societies and really civilization in general have to come to terms with the ability for common people to hold hard secrets?

**Glenn Greewald:** So, I'll just start with a couple of observations about what's at stake in that FBI/Apple conflict. You know, before I was a journalist I was a lawyer, as you referenced earlier, and I used to defend a lot of free speech cases. And the tactic of the government whenever they want to erode free speech is to pick the most unsympathetic possible person to abridge their free speech that precedent is created, that they have the power to abridge free speech and then they can start making their way outward to more sympathetic cases. But by then it's too late because the person they began with you hated so much that you allowed them to do it. And that's why free speech defenders like the ACLU (American Civil Liberties Union) find themselves defending the Klu Klu Klan or Neo-nazis or Fred Phelps, the most hated people in society, because they are the ones who are most vulnerable to having their rights abridged in a way that will let your rights be abridged after. That's exactly what the FBI did in this case, was they found the least sympathetic case possible. Who would ever argue that the FBI should be blocked from accessing the telephone of the person who committed the San Bernadino murder. Nobody would ever argue that.

And yet, what the FBI was doing in this case was pure deceit. They wanted to create a precedent whereby Apple and other companies were forced into essentially involuntary labor on behalf of the government. Where they would be forced to build, using their own engineers, backdoors that would let the FBI access not just this iPhone but all iPhones. That would also then be a backdoor that a lot of other people could use. And the broader philosophical question that really was raised by this is, which is what the question suggested, which is should there ever be a way that citizens can communicate in a way that the government just physically cannot access? That really is what the government is attempting to do. Their motto, sort of like how football teams have mottos or car rental agencies have mottos, the NSA has a motto and their motto, as Ed said earlier, is „Collect it All". You know not collect a lot of it, and not collect all the terrorist communication, they want to collect it all, which is another way of saying they want to be able to collect and store all communications by and between human beings on this planet, which is another way of saying

eliminating privacy in the digital age. And that‘s what‘s at stake in Apple v. FBI. And the one thing that always fascinates me is that we read 1984 in high school and it‘s sort of almost become a cliché to bring it up in privacy debates. And unfortunately for me high school was a really long time ago, which is when I read 1984 and I had actually misremembered it. I remembered the warning of Orwell being that if you live in a society where you are always being watched, that‘s when you lose freedom. And so you raise 1984 and people would say no our society is different. We‘re not all being watched. We‘re not all having all our emails read and telephone calls listened to. But I actually went back and read 1984 when I started doing this work and the world that Orwell was warning of was not one in which we were all being watched, it was a world in which we could be watched at any moment.

And Winston Smith, the narrator, said that this monitor that was in your home, you never knew if it was on, you never knew if anybody was actually ever watching you at all. What you knew was that you could be watched at any moment and therefore you had to act as though you were being watched. Which meant people who know they could be watched act obediently and compliantly and submissively and without dissent. That is the precedent that the government is trying to create in the FBI v. Apple case, is that there can never be a moment when you are able to communicate beyond the surveillance arm of the United States government.

**Noam Chomsky:** Happy to endorse those remarks.

**NO:** Ed, what are your thoughts?

**Edward Snowden:** Okay. When we think about this. Again, I think the core issue here is who is privacy really for. Privacy is not for the powerful when we think about who should hold secrets, should the public be permitted to hold secrets. Nor is it new. Again the ephemerality of human communications is actually the status quo. That‘s the way it always was in the history of or species. Think about it. If you were a police officer and you were investigating a crime, would you rather have the technology and the state of play of communications today available to you or would you rather have it two hundred years ago when telephonic wire taps didn‘t exist? When there were no records of all of your travels. Everywhere that your Easypass went on your car. Every purchase that you have ever made as a result of your credit card. And critically, it‘s important to understand that in controversy at this case is not actually who these individuals were calling, it‘s not who they were in contact with, because all of that information is metadata.

Metadata does not simply exist on the telephone. Because metadata are the actual activity records. The way the phone system works, right, is you‘ve got a phone here for you and you‘ve got a phone for the distant end, the person that you are talking to. They don‘t communicate by magic. The signal has to travel over service providers’ lines who are not owned by the customer. And records of all of these activities are being created by the businesses for legitimate purposes. Just for the purpose of keeping track of the billing and monitoring and metering and so on and so forth, qualitative service levels. And to make sure you get charged for making a call. Now these records have already been turned over to the FBI. They’ve had them since only days after the investigation. So they already know that these phones weren‘t in contact with foreign terrorists and so on and so forth. Because if they were it happened by magic. And if we are dealing with terrorists who are also wizards we have larger problems.

But the central issue that I that I want to really come back to here in the context of what the questioner was asking of „Do we deserve privacy? Is the world ready for the public to have privacy?“ Again, it‘s embedded in our language. We are called private citizens and public officials because the government is supposed to know in almost every case very little about us, about the ordinary people, whereas we are supposed to know nearly everything about their activities. Yet, because of the growth of state secrets, the growth of classification in many different ways, we know less and less about the government than we ever have before. And we see this becoming a culture in government. We see various senior officials in government creating their own email servers to hide their communications from public records requests, which as Professor Chomsky said are sort of the antidote to this. Well, okay, they can have whatever communications they want, as long as we can file a Freedom of Information Act request. As long as they can get requisitioned or declassified down the line. But what happens when a culture of unaccountability begins to blossom and take root within our government? And we know nothing about what they are doing. And if they are engaged in unlawful or inappropriate activity we can never know because they have created a system to hide it from us

at the same time that systems of global pervasive surveillance are being stood up. Not just in the United States but every other country in the world. And everything that we do is becoming transparent. While the activities of powerful members of society, privileged members of society, are becoming opaque.

**NO:** So just to follow on the that Ed. This case, for so many of us work in technology, really focuses the ability of one as an individual to use technology to shield and to protect. Do you want to comment or could you comment, for so many people who asked online, your thoughts about tools that individuals should or could be using or what should we be aspiring to in our use of technology? I welcome others to weigh in as well.

**ES:** So this a really challenging question to compress because unfortunately it‘s still quite difficult. You can‘t be truly invisible online. There‘s no invisibility cloak, there’s no magic wand that‘s going to protect you from everything. Particularly, even if you are using secure tools, if you do not understand how they function you can make mistakes or you can be leaving trails and so forth. And this is one of the reasons that the FBI‘s jobs and the FBI‘s claims that they are going dark are so ridiculous. Even if you have an encrypted phone, even if you have encrypted communications programs, those things like those metadata records, again, the private activity records, the details that are thrown off as pollution, just by the fact that a communication, even if they can‘t read the communication, they can see the fact that it happened. And if they see a US person or anybody else who they are concerned about being involved in terrorism or something like calling the Al Qaeda hotline in Pakistan, even if they can‘t tell it what was said on it, they know that person is probably a person of interest. But just raw technology for those who are interested, who are motivated, you should be using Tor, the Tor Project, or the Tor browser bundle as is commonly downloaded by normal internet users to hide and protect the general activities that you are involved in online from corporate spies, from your internet service provider, from AT&T and Verizon and Comcast. So they don‘t have records of your activities if they don‘t need them.

This isn‘t just about the government.  This is about having the privacy to type something into Google prompt without having it follow you home. For communications on cell phones, sending text messages, just download an app called Signal. It‘s in the app store for either Android or iOS. And this works on telephonic communications. Again, and this way when you‘re sending text messages back and forth or sending pictures that could be intimate, that could be private, your cell phone company can‘t see them. And the NSA can‘t be swapping them around as they did with nude photos when I was working there. Because there is a counter balancing thing here where you go „Well, if you have these tools does this mean the terrorists will get away scot free, that we won’t know what‘s going on?“ That‘s not the case. Again, even in the case of perfect software based encryption, in theory, you have to understand the technical principle here, which is, anytime you are enciphering information, right, you‘re scrambling so that your adversaries can‘t see it,  it means you can‘t see it either unless you decipher it, unless you unlocked it at some point. Now typically, this is on the base of a password or some type of derived key. But the way to kind of conceptualize this is that when you turn your phone off, when you put it on the counter, when you leave it behind, whatever, it‘s scrambled, it‘s white noise, but it‘s not any good to you either. It‘s just a brick sitting on a shelf.

If you want to actually see your text messages, if you actually want to call someone, if you actually want to look at your photos or whatever, you have to be able to unlock the phone. And when you do this, this is the point of vulnerability that governments can and do exploit. As do criminal groups and other organizations because they simply hack your device while it‘s hot, while it‘s live, while it‘s decrypted, and they steal the key that unlocks the device. Or more simply, this was the case of the Silk Road drug market, there was an individual, they considered him sort of a criminal mastermind type using encrypted communications and so on and so forth, so they went oh gosh we won‘t be able to get our evidence, which we need to convict this individual, even though they didn‘t really need it in this case, how do we do it? Well‘ if we can‘t break the encryption are we totally out of luck, right? If Apple couldn‘t unlock this phone for the FBI, if they wouldn‘t unlock this phone for the FBI, does this mean the government has to throw its hands up and say, „ We‘re done. We have to close up shop. There‘s no more law enforcement investigations.“ Well, in the case of this person who was using encrypted communications, encrypted hard drives and so on in this Silk Route case, they created a very simple ploy. This individual was operating out of public libraries. So when they opened their laptop, decrypted their device, began engaging in their alleged criminal schemes, two FBI agents in disguise as a husband and wife pair were standing to this individual’s left and created a gigantic scene. They acted like they were having some sort of spat. When the individual‘s head turned to the left, an FBI to his

right simply picked up his laptop, which was now unencrypted, and took it away.

The NSA get around encryption every day of the week and twice on Sundays. I have lived this. Encryption is an impediment, right, but the value to the public of securing your rights, not just in the United States but other countries where you can‘t rely on rights all the time, where you have local police agencies that could be investigating journalists, this provides a way of enforcing human rights through new means which are reliable in international space. And we should not sacrifice that simply for the desired efficiency of having access to information that a few years ago wouldn‘t have existed to begin with.