00:04

How many of you have ever heard someone say privacy is dead? Raise your hand. How many of you have heard someone say they don't care about their privacy because they don't have anything to hide? Go on.

00:17

(Laughter)

00:19

Now, how many of you use any kind of encryption software? Raise your hand. Or a password to protect an online account? Or curtains or blinds on your windows at home?

00:32

(Laughter)

00:34

OK, so that's everyone, I think.

00:36

(Laughter)

00:38

So why do you do these things? My guess is, it's because you care about your privacy. The idea that privacy is dead is a myth. The idea that people don't care about their privacy because "they have nothing to hide" or they've done nothing wrong is also a myth. I'm guessing that you would not want to publicly share on the internet, for the world to see, all of your medical records. Or your search histories from your phone or your computer. And I bet that if the government wanted to put a chip in your brain to transmit every one of your thoughts to a centralized government computer, you would balk at that.

01:17

(Laughter)

01:20

That's because you care about your privacy, like every human being. So, our world has changed fast. And today, there is understandably a lot of confusion about what privacy is and why it matters. Privacy is not secrecy. It's control. I share information with my doctor about my body and my health, expecting that she is not going to turn around and share that information with my parents, or my boss or my kids. That information is private, not secret. I'm in control over how that information is shared.

02:01

You've probably heard people say that there's a fundamental tension between privacy on the one hand and safety on the other. But the technologies that advance our privacy also advance our safety. Think about fences, door locks, curtains on our windows, passwords, encryption software. All of these technologies simultaneously protect our privacy and our safety.

02:28

Dragnet surveillance, on the other hand, protects neither. In recent years, the federal government tasked a group of experts called The Privacy and Civil Liberties Oversight Board with examining post-9/11 government surveillance programs, dragnet surveillance programs. Those experts could not find a single example of that dragnet surveillance advancing any safety -- didn't identify or stop a single terrorist attack. You know what that information was useful for, though? Helping NSA employees spy on their romantic interests.

03:02

(Laughter)

03:04

(Audience: Wow.)

03:06

Another example is closer to home. So millions of people across the United States and the world are adopting so-called "smart home" devices, like internet-connected surveillance cameras. But we know that any technology connected to the internet can be hacked. And so if a hacker gets into your internet-connected surveillance camera at home, they can watch you and your family coming and going, finding just the right time to strike. You know what can't be hacked remotely? Curtains.

03:37

(Laughter)

03:38

Fences. Door locks.

03:40

(Laughter)

03:41

Privacy is not the enemy of safety. It is its guarantor.

03:47

Nonetheless, we daily face a propaganda onslaught telling us that we have to give up some privacy in exchange for safety through surveillance programs. Face surveillance is the most dangerous of these technologies. There are two primary ways today governments use technologies like this. One is face recognition. That's to identify someone in an image. The second is face surveillance, which can be used in concert with surveillance-camera networks and databases to create records of all people's public movements, habits and associations, effectively creating a digital panopticon.

04:30

This is a panopticon. It's a prison designed to allow a few guards in the center to monitor everything happening in the cells around the perimeter. The people in those prison cells can't see inside the guard tower, but the guards can see into every inch of those cells. The idea here is that

if the people in those prison cells know they're being watched all the time, or could be, they'll behave accordingly. Similarly, face surveillance enables a centralized authority -- in this case, the state -- to monitor the totality of human movement and association in public space. And here's what it looks like in real life. In this case, it's not a guard in a tower, but rather a police analyst in a spy center. The prison expands beyond its walls, encompassing everyone, everywhere, all the time. In a free society, this should terrify us all.

05:35

For decades now, we've watched cop shows that push a narrative that says technologies like face surveillance ultimately serve the public good. But real life is not a cop drama. The bad guy didn't always do it, the cops definitely aren't always the good guys and the technology doesn't always work. Take the case of Steve Talley, a financial analyst from Colorado. In 2015, Talley was arrested, and he was charged with bank robbery on the basis of an error in a facial recognition system. Talley fought that case and he eventually was cleared of those charges, but while he was being persecuted by the state, he lost his house, his job and his kids. Steve Talley's case is an example of what can happen when the technology fails. But face surveillance is just as dangerous when it works as advertized.

06:30

Just consider how trivial it would be for a government agency to put a surveillance camera outside a building where people meet for Alcoholics Anonymous meetings. They could connect that camera to a face-surveillance algorithm and a database, press a button and sit back and collect a record of every person receiving treatment for alcoholism. It would be just as easy for a government agency to use this technology to automatically identify every person who attended the Women's March or a Black Lives Matter protest. Even the technology industry is aware of the gravity of this problem. Microsoft's president Brad Smith has called on Congress to intervene. Google, for its part, has publicly declined to ship a face surveillance product, in part because of these grave human and civil rights concerns. And that's a good thing. Because ultimately, protecting our open society is much more important than corporate profit.

07:32

The ACLU's nationwide campaign to get the government to pump the brakes on the adoption of this dangerous technology has prompted reasonable questions from thoughtful people. What makes this technology in particular so dangerous? Why can't we just regulate it? In short, why the alarm?

07:52

Face surveillance is uniquely dangerous for two related reasons. One is the nature of the technology itself. And the second is that our system fundamentally lacks the oversight and accountability mechanisms that would be necessary to ensure it would not be abused in the government's hands. First, face surveillance enables a totalizing form of surveillance never before possible. Every single person's every visit to a friend's house, a government office, a house of worship, a Planned Parenthood, a cannabis shop, a strip club; every single person's public movements, habits and associations documented and catalogued, not on one day, but on every day, merely with the push of a button. This kind of totalizing mass surveillance fundamentally threatens what it means to live in a free society. Our freedom of speech, freedom of association, freedom of religion, freedom of the press, our privacy, our right to be left alone.

09:01

You may be thinking, "OK, come on, but there are tons of ways the government can spy on us." And yes, it's true, the government can track us through our cell phones, but if I want to go to get an abortion, or attend a political meeting, or even just call in sick and play hooky and go to the beach ...

09:20

(Laughter)

09:21

I can leave my phone at home. I cannot leave my face at home.

09:28

And that brings me to my second primary concern: How we might meaningfully regulate this technology. Today, if the government wants to know where I was last week, they can't just hop into a time machine and go back in time and follow me. And they also, the local police right now, don't maintain any centralized system of tracking, where they're cataloging every person's public movements all the time, just in case that information some day becomes useful. Today, if the government wants to know where I was last week, or last month or last year, they have to go to a judge, get a warrant and then serve that warrant on my phone company, which by the way, has a financial interest in protecting my privacy. With face surveillance, no such limitations exist. This is technology that is 100 percent controlled by the government itself. So how would a warrant requirement work in this context? Is the government going to go to a judge and get a warrant, and then serve the warrant on themselves? That would be like me giving you my diary,

and saying, "Here, you can hold on to this forever, but you can't read it until I say it's OK." So what can we do?

10:44

The only answer to the threat posed by the government's use of face surveillance is to deny the government the capacity to violate the public's trust, by denying the government the ability to build these in-house face-surveillance networks. And that's exactly what we're doing. The ACLU is part of a nationwide campaign to pump the brakes on the government's use of this dangerous technology. We've already been successful, from San Francisco to Somerville, Massachusetts, we have passed municipal bans on the government's use of this technology. And plenty of other communities here in Massachusetts and across the country are debating similar measures.

11:25

Some people have told me that this movement is bound to fail. That ultimately, merely because the technology exists, it will be deployed in every context by every government everywhere. Privacy is dead, right? So the narrative goes. Well, I refuse to accept that narrative. And you should, too. We can't allow Jeff Bezos or the FBI to determine the boundaries of our freedoms in the 21st century. If we live in a democracy, we are in the driver's seat, shaping our collective future.

12:08

We are at a fork in the road right now. We can either continue with business as usual, allowing governments to adopt and deploy these technologies unchecked, in our communities, our streets and our schools, or we can take bold action now to press pause on the government's use of face surveillance, protect our privacy and to build a safer, freer future for all of us.

12:36

Thank you.

12:37

(Applause and cheers)