How to Avoid Surveillance ... with the Phone in your Pocket

Christopher Soghoian

For more than 100 years, the telephone companies have provided wiretapping assistance to governments.

[0:18] For much of this time, this assistance was manual. Surveillance took place manually and wires were connected by hand. Calls were recorded to tape. But as in so many other industries, computing has changed everything. The telephone companies built surveillance features into the very core of their networks. I want that to sink in for a second: Our telephones and the networks that carry our calls were wired for surveillance first. First and foremost.

[0:49] So what that means is that when you're talking to your spouse, your children, a colleague or your doctor on the telephone, someone could be listening. Now, that someone might be your own government; it could also be another government, a foreign intelligence service, or a hacker, or a criminal, or a stalker or any other party that breaks into the surveillance system, that hacks into the surveillance system of the telephone companies.

[1:18] But while the telephone companies have built surveillance as a priority, Silicon Valley companies have not. And increasingly, over the last couple years, Silicon Valley companies have built strong encryption technology into their communications products that makes surveillance extremely difficult.

[1:36] For example, many of you might have an iPhone, and if you use an iPhone to send a text message to other people who have an iPhone, those text messages cannot easily be wiretapped. And in fact, according to Apple, they're not able to even see the text messages themselves. Likewise, if you use FaceTime to make an audio call or a video call with one of your friends or loved ones, that, too, cannot be easily wiretapped.

[2:00] And it's not just Apple. WhatsApp, which is now owned by Facebook and used by hundreds of millions of people around the world, also has built strong encryption technology into its product, which means that people in the Global South can easily communicate without their governments, often authoritarian, wiretapping their text messages.

[2:20] So, after 100 years of being able to listen to any telephone call -- anytime, anywhere -- you might imagine that government officials are not very happy. And in fact, that's what's happening. Government officials are extremely mad. And they're not mad because these encryption tools are now available. What upsets them the most is that the tech companies have built encryption features into their products and turned them on by default. It's the default piece that matters.

[2:49] In short, the tech companies have democratized encryption. And so, government officials like British Prime Minister David Cameron, they believe that all communications -- emails, texts, voice calls -- all of these should be available to governments, and encryption is making that difficult.

[3:08] Now, look -- I'm extremely sympathetic to their point of view. We live in a dangerous time in a dangerous world, and there really are bad people out there. There are terrorists and other serious national security threats that I suspect we all want the FBI and the NSA to monitor.

[3:24] But those surveillance features come at a cost. The reason for that is that there is no such thing as a terrorist laptop, or a drug dealer's cell phone. We all use the same communications devices. What that means is that if the drug dealers' telephone calls or the terrorists' telephone calls can be intercepted, then so can the rest of ours, too. And I think we really need to ask: Should a billion people around the world be using devices that are wiretap friendly?

[3:54] So the scenario of hacking of surveillance systems that I've described -- this is not imaginary. In 2009, the surveillance systems that Google and Microsoft built into their networks -- the systems that they use to respond to lawful surveillance requests from the police -- those systems were compromised by the Chinese government, because the Chinese government wanted to figure out which of their own agents the US government was monitoring.

[4:19] By the same token, in 2004, the surveillance system built into the network of Vodafone Greece -- Greece's largest telephone company -- was compromised by an unknown entity, and that feature, the surveillance feature, was used to wiretap the Greek Prime Minister and members of the Greek cabinet. The foreign government or hackers who did that were never caught.

[4:40] And really, this gets to the very problem with these surveillance features, or backdoors. When you build a backdoor into a communications network or piece of technology, you have no way of controlling who's going to go through it. You have no way of controlling whether it'll be used by your side or the other side, by good guys, or by bad guys.

[5:00] And so for that reason, I think that it's better to build networks to be as secure as possible. Yes, this means that in the future, encryption is going to make wiretapping more difficult. It means that the police are going to have a tougher time catching bad guys. But the alternative would mean to live in a world where anyone's calls or anyone's text messages could be surveilled by criminals, by stalkers and by foreign intelligence agencies. And I don't want to live in that kind of world.

[5:29] And so right now, you probably have the tools to thwart many kinds of government surveillance already on your phones and already in your pockets, you just might not realize how strong and how secure those tools are, or how weak the other ways you've used to communicate really are.

[5:45] And so, my message to you is this: We need to use these tools. We need to secure our telephone calls. We need to secure our text messages. I want you to use these tools. I want you to tell your loved ones, I want you to tell your colleagues: Use these encrypted communications tools. Don't just use them because they're cheap and easy, but use them because they're secure.

[6:08] Thank you.

https://www.ted.com/talks/christopher\_soghoian\_a\_brief\_history\_of\_phone\_wiretapping\_and\_how\_to\_avoid\_it