Cindy Cohn: ‘They have our lives in their hands’

5/18/2017

The US non-profit Electronic Frontier Foundation (EFF) champions user privacy, free expression and innovation, which they see as civil liberties. The EFF fights cases in court, publishes papers and develops privacy technology. An LSE and University of Michigan alumna, Executive Director Cindy Cohn was named one of the 100 most influential lawyers in America in 2013, and has received a number of other awards. She spoke with LSE Business Review managing editor Helena Vieira on 3 May during a tech conference in New Orleans. “One of the problems I find when many people talk about privacy and security is that they put all of the responsibility on your shoulders, to protect yourself,” she says.

After the Snowden revelations, a lot of people lost their innocence about how much surveillance goes on. Nothing changed except that we’re more aware that this can and will happen. Is this our new way of life now?

I don’t think that that’s true that nothing has changed. I don’t think enough has changed. But the government immediately went from doing three hops to two hops, so it’s only you and the people you talk to, but not the people that they talk to. It was a much bigger number. They did that on their own. They stopped their telephone records programme, they stopped it two years ago. It got shifted in a way that still isn’t good, but believe me, the NSA doesn’t lose very often. So anytime that we can cut their powers back even a little it’s a dramatic change.

Last Friday *(28 April)*, the government said they weren’t going to do this thing called “about searching” anymore. It remains to be seen how that’s going to play out, but that is also something that they did not want to stop doing but they stopped doing because of the continual pressure by public and lawmakers. So there’s a lot that has changed. Most of it is not the way it needs to be. These are big, hard fights, and when you’re fighting the national security infrastructure of all the governments in the world,… believe me, those are people who don’t lose very often and they’ve lost a lot in the last few years. So Mr. Snowden did us all a big favour.

The other thing we’ve done since then, and the bigger thing, frankly, is not on the legal and policy side, it’s on the tech side. We have encrypted tremendous amount of web traffic since then. Part of the reason why they dropped the "about searching" is because of encryption. We use https everywhere, we have certificate authorities as well as deep geek stuff but we have encrypted the web at a level much faster after the Snowden revelations than we did before. As a result of that, we all have much better security as well as privacy.

I don't mean to be a Pollyanna, but to say that nothing changed is not true. And I think the biggest changes have happened in ways that are technically important and may not be as visible to ordinary users, but that doesn't mean they didn't happen. I'm talking to you with an Apple device. This device is encrypted by default, and the data on it is encrypted, just like it is on your Apple computer that you have here. This (*points to the computer*) they were doing before Snowden. This (*points to the phone*) is after Snowden. Again, your phone doesn't look any different to you, but it's actually significantly more secure. Your data on here is significantly more secure than it was.

That's very good to know. How do you fight against other governments, how do you fight against a global enemy?

The main thing you have to do is to encrypt stuff as much as possible. The technological protections, given the difficulties in enforcing laws and policy online in a way that jurisdictions play into this, being that a foreign government may not be subject to the same rules that your own government is. This means that we have to focus our attention on technological protections. It's really important.

We also need laws that support them. Somebody who's building encryption into your tool, it needs to be legal for them to do so, and that's a big fight in the United States that is coming up, whether you can offer as strong an encryption to people or not.

Law supports tech, but the first step is to have really strong technologies because they protect you regardless of their jurisdiction. However, EFF is actually representing a guy who lives in Maryland, who is a member of the Ethiopian diaspora who had his computer infected by the government of Ethiopia, and everything he did shifted back from his home computer in Maryland to a server controlled by the government in Ethiopia, as part of a pretty well understood spying programme that the Ethiopian government does against the diaspora dissidents. We brought a civil wiretap claim and an 'intrusion on seclusion' claim in Washington DC against the government of Ethiopia. We had a setback recently but the court has actually asked for additional briefing and they may change their position But we need to develop the law, so that people are empowered to take steps to protect themselves both legally and technically. By the way, the case is called Kidane.

That leads to my next question: how do you work with the law if laws are national? Do we need supranational institutions?

Well, we do have international laws. Even in our pre-internet world there were lots of things that work over borders, certainly the whole international human rights infrastructure is based on the idea that there are certain rights and protections that you as an individual have, just by virtue of being an individual on the planet. But including the idea that the surveillance of you should be necessary and proportionate, and there's an international group of NGOs, some members of the UN and other people who put together this thing called the necessary and proportionate principles, which is an attempt to take the international human rights standards for surveillance and apply them to the digital age. So it talks about things like mass surveillance being a human rights violation and those sorts of things. Those structures, a lot of them already exist, they don't have a lot of teeth, I'm not sure how much more teeth we want to put into them, but the standards are international standards and there are small areas of disagreement and wide areas of agreement about the limits of any government's ability to surveil you.

Most of your work is protecting citizens against the government. Do you draw the line there or do you also work to protect consumers from the use of their private data from companies?

Sure. EFF is interested in empowering users regardless of whether it's the government or a private company that is getting in the way of their using technology to their fullest, so we have a plugin for Firefox called 'The Privacy

Badger" that is very easy to use and that blocks third party cookies from being installed on your computer. It's really sweet, easy, anybody can use it and it helps block some of the commercial tracking that happens to people. It's got some sliders that you can turn on and off if it breaks things. That was an idea to try to implement something called 'Do Not Track". The 'Do not track' idea came from a former EFF intern who was at Stanford. Your browser ought to send a flag to all the websites you go to about whether you want to be tracked or not. And those websites should honour it.

The policy idea got mired down because ad companies had so much power that we just built our own browser extension that follows do not track and lets your message be something that if the company doesn't honour your request not to track then they don't get to track you, they don't get to place cookies on your device. We work on the consumer side as well. We've just issued a white paper on student privacy. Companies like Google and Apple are giving a lot of technology to schools for kids. There's lots and lots of tracking on it. We did a survey on the tremendous amount of these kinds of edutech – it's what they call it – and how well they do at protecting people's privacy. We issued a white paper just a couple of weeks ago that points out how bad the deal is for kids' privacy – that is being offered by a lot of these companies. We certainly do work not just on the government but on the private side as well.

I have a personal example. I read an article in a newspaper advising people to use web browsers that allow you more privacy, so I downloaded Tor, but I couldn't access my email and social media accounts and couldn't even read the newspaper that published the article on Tor.

Yes, look, we need more pressure on these companies to do the right thing and make sure Tor works. Facebook has a hidden service for Tor that you can use where you know you can't be tracked at all. Facebook supports that but if you go in the front door in the regular way then they want you to be able to log in. We need to create more spaces. I'm on the board of Tor. I think Tor has too hard a time right now and it needs to have a better time and we need to put pressure on these companies to do better and to let us access this information in a way that works for people. So you know the technology will help a little but we also need policy and legal support for us to be able to browse anonymously. So the Tor browser does as well as it can given that it's, like, 15 people writing a browser against the whole world, but we need more. We need more support for these kinds of tools.

What can people do to protect themselves?

While there are some things that people can do, it's not enough. One of the problems I find when many people talk about privacy and security is that they put all of the responsibility on your shoulders, to protect yourself. And there are some things that you can do to protect yourself and I'm happy to talk about Tor, Tor where you can, Signal, and as an open source thing there's a tool called Jitsi, that lets you do voice calls. There are tools available that will help with almost every problem, but they're all hard to use and they're all trying to operate at the margins of the Internet. So we need collective action. We need people to work together to put pressure on these companies to do better and to support things that do it.

The tech alone, I like to use this as an example: if people had cars where the brakes failed all the time, yeah, you should learn enough about brakes so that you can investigate your brakes and see if they're really good ones and maybe install your own brakes that are better. That's not what we tell people to do. Sure, you can do that. That's awesome, then you'd have really good brakes because you know enough about having good brakes. You know the other thing we do? We don't let them sell cars unless they have really good brakes on them. So you don't have to have all that knowledge and all that technical sophistication to have a car that stops when you put your foot on the brakes.

We need our technology, frankly, to have a lot more incentives to work for us, to protect us, sometimes that's regulation, sometimes that's incentive, sometimes that's the government's purchasing power, so that the government only purchases stuff that supports this kind of thing. They're a huge player in the market. There's liability. If this tool hurt your privacy you should be able to sue, you should be able to sue a foreign government who attacks you. This is what we use in the rest of the world to try and make sure that the tools we rely on for our safety and security actually work. We need to start bringing more of those to bear on the digital tools because, frankly, they have our lives in their hands.

♣♣♣

- *This Q&A is the seventh in a series of interviews with tech leaders during the Collision conference in New Orleans, 2-4 May 2017.*
- *The post gives the views of the interviewee, not the position of LSE Business Review or of the London School of Economics and Political Science.*
- *Before commenting, please read our* Comment Policy.