Nico Sell: ‘Stop giving away all your information for free on Facebook’

blogs.lse.ac.uk/businessreview/2017/06/06/nico-sell-stop-giving-away-all-your-information-for-free-on-facebook/

6/6/2017

Nico Sell is part of a rare breed of Silicon Valley entrepreneurs who don’t practice ‘tech evangelism’. The co-founder of the encrypted messaging app Wickr and the Wickr Foundation is a fierce critic of current business models based on mining consumers’ private information. In 2015 she wrote an open letter to the UK’s then Prime Minister, David Cameron, complaining about the Investigatory Powers Act: ‘Encryption should be a global human right, Mr Cameron.’ You won’t find Nico on Facebook or on other social networks. “Kids know,” she says. They will tell adults, ‘Stop giving away all your information for free on Facebook.’ She spoke with LSE Business Review managing editor Helena Vieira during a conference in New Orleans.

What led you to create Wickr?

The idea for Wickr came from two places. I’d been helping the Dark Tangent (*as hacker Jeff Moss is known*) with DEFCON (*a hackers’ conference*) for many years. Part of what I would do there is work with the researchers that had zero base, or new flaws, in a vendor’s technology, and get that information disclosed out properly, and fixed. We had been using encryption, but it would always take several weeks, multiple IT departments to be able to exchange this information. That problem drove me crazy for about a decade. I was like, ‘will someone make encryption easier to use?’ It should not be this difficult. But what really got me off my butt to do it was that I launched r00tz Asylum, which is a kids’ version of DEFCON. As part of that, all these amazing kids from all over the world were coming together and becoming friends, learning how to hack, and then they were going to leave. How were they going to communicate when they left? I didn’t approve of them using Facebook for their private communications because I don’t think children’s information should be monetised like that.

That was the real reason that I built Wickr. It was for the kids. And actually we had the r00tz Asylum kids, 200 beta testers, using our product in the very beginning, because we needed it to be easy enough for a three-year-old to use. My three-year-old was actually one of the product testers the whole time. Number 1: she couldn’t mess it up,

right? You can hit the wrong button and expose yourself. It just needs to be easy and fun. But I think that's what made Wickr so unique, because that was the level of ease of use that we wanted. However, the encryption is the number 1 encryption in the world. We're the only ones who have never had a compromise. We're five years old now. It even got leaked that the Department of Homeland Security was paying a hacking team in Italy to hack us, and they hadn't been successful. We're the most advanced encryption technology, yet three-year-olds can use it and have fun using it every day.

People talk a lot about protecting our privacy from the government. Why don't they talk so much about protecting our privacy from private companies?

Thank you so much for asking that question. I actually think that the biggest threat to my friends and family are the data brokers. Experian in the US is the worst of them. We have a lot of them in the US. They sell lists of rape victims, erectile dysfunction sufferers and dementia patients for 7 cents a piece. You think of all this data that Facebook is collecting. People think that it's a private communication. Private just means that the public can't see it. It doesn't mean that they can't analyse it and that thousands of other people aren't seeing it. I really believe that to the average person this is a much greater threat than the NSA.

They argue consumers know it's a trade-off and use it because they agree. Isn't that because there's no alternative?

They actually don't believe that this would be happening. When I tell you that Facebook, Twitter, WhatsApp, Snapchat, Skype, the privacy policy, what it says, if I were to boil down their 30 pages to one sentence, is 'you're granting the company free transferrable worldwide rights to anything you put in that service for eternity.' So, even if you think the company is good right now, they're storing all this data in computers and the data base they hold could be breached. A decade ago we saw it with AOL searches. This was when AOL was the big search engine. You can tell everything by someone's Google searches. Imagine when the Google database is breached. Now, they have one of the best security teams in the world, but nothing is a hundred per cent. And I think that's what we really need to think about. A lot of people say, 'I don't have anything to hide'. But when you think about all of your emails and text messages being searchable to anyone you work with, everyone you interview, your mother, your daughters, that's the kind of thing that happens. And it's happened to my friends, and we don't want it happening to anyone else.

Why do you think there hasn't been a backlash?

I think the reason is that there haven't been alternatives. It's really because the Internet was built on such amazing trust in the beginning. By the way, it had to be that way, otherwise it wouldn't have gotten on, and I think people just really don't believe it's happening. They'll say to me, 'why will they destroy my conversations? I'm not important.' There' a lot of reasons why, from advertising to building AI. Yes, I really would like this to be a bigger topic.

Are you not on Facebook?

I've never been on Facebook. I don't have any Facebook friends. Facebook wasn't made for your benefit. It's an amazing marketing tool, and that's what it should be used for. Your private conversations and pictures don't belong in there. What hackers would say to someone like you and I is that it's irresponsible not to be on Facebook, because there's another attack that happened at DEFCON, where they took a bunch of influential people who didn't have Facebook accounts, created accounts for them and friended all their friends. So they said, 'you really have to create an account,' and I'm like, 'but I don't play that game.'

A blog post we published recently suggested consumer privacy could be a disruptive innovation. Is there a business model that could work that way?

Oh, I love that question, because I think that the business model that started the internet in the last decade is not the one that will survive over the next 10 to 20 years. I'm predicting in 2020 we'll start seeing a big data bubble, because

companies are suddenly starting to realise that the more valuable information they hold the more likely they are to get compromised. I believe that the business model that will thrive over the next decade is one where companies make money by selling services that users want on the internet. I don't think that it would have worked 20 years ago, because it wasn't proven. But the internet is proven now. With Wickr that is the case. We run a zero knowledge system. We have no idea who our users are, or how they use our system. Imagine trying to raise money like that, right? And yet we've got a very good business model. We sell an enterprise version of Wickr to companies and government agencies, and that's how we make money. We don't know anything about our users and we make money. And I think that this is something that we'll see more and more of.

So, you're the disruptive innovator. Do you consider yourself that?

Yes, yes, I can't help not be…

I downloaded your Wickr app and I saw that you can download it on your laptop. How can you be sure that it's not being spied on, with all these cookies that we're forced to allow in our computers?

It's a little tricky, because if your device is owned, then you're going to see anything that's unencrypted when you're looking at it. It really depends on your threat model. For activists that have very severe dictators following on them, or someone like myself, I don't have any apps on my phone, I don't go to any websites, I don't do anything fun. The same with your computer. You know, there are ways to get a key logger on there, and they'll see what you're typing. It's also a matter of keeping your computer secure. But cookies won't compromise Wickr. Or I don't use Wickr on my computer. I just use it on my phone, because my computer does more things, but that's the extreme.

You said you don't download apps or anything, so you're not using the Internet…

I do use it for trusted sites and trusted places, and I have a few apps that I'll download. But every app that you download is a vector in. My daughter found a zero-day (*a security vulnerability*). She is able to turn on a Samsung TV via the Facebook app, because the FB app has a way to turn the camera on and off, and the microphone on and off, so that's just one example of one vector in, because if that has to have permission and you get into that app, they can turn it on and off. You want to be really careful about the apps that you download and make sure that they have companies that update it, pay attention to security, have good budgets.

Tell me about the Wickr Foundation. What do you do, and what is your goal?

We realised there was a bunch of activists that were asking us for things that we wanted to do on Wickr but that we couldn't really justify from the business perspective, but were really important from a societal perspective. So we decided to have Wickr Inc, that would focus on making money and selling privacy and ephemerality to the enterprise, and Wickr org, which would focus on getting kids and activists to use encryption and ephemerality, and the focus not to be on making money. Because those aren't the kind of people we want to make money off of, but we did think it was really important for them to have all of this technology.

So what do you do? Teach kids?

That is r00tz Asylum, where we teach kids how to hack. With Wickr Foundation we take those kids and we teach adults how to hack. Wickr Foundation is not solely focused on kids. Also, I run a non-profit venture fund with the foundation. I invest in entrepreneurs that are building technology that's used for kids and activists, that I would approve of. We made four investments so far. Whistler was the first one, it's public, you can look it out there, or on the Wickr site, but that is the app that we made for activists. The CEO that I founded it with is called Srdja Popovic. He has been nominated for the Nobel Peace Prize numerous times because he overthrows dictators without violence. I didn't even know that was possible.

How does he do that, by hacking?

No, by using women and children. In a good way, right? How do you control a riot? They put all the women and children up front, to the officers, they talk to the officers, they find out what towns they're from, who their friends are, and then they pull their families, bring them in, and talk their way, all the way into the Oval Office in Serbia. They took out one of the worst dictators of our time, without any violence. And so Whistler is us automating Srdja's process and everything he does. It has Wickr in it, but other things too, such as a panic button. So if you're unduly arrested, it will notify all the people that you say ahead of time you want to be notified, then delete them from your phone, but not delete everyone else from your phone. It's able to send automatic press releases with human rights violations, to CNN, Amnesty International, and again, doing all this stuff at a three-year-old level, because these activists have many more things to worry about than technology.

You should teach adults the basics of how to protect their privacy, how to use computers, etc…

It's so funny. The kids know. They interviewed some kids and asked 'what would you tell adults?' and they were like, 'Stop giving away all your information for free on Facebook'. They don't use Facebook. Anyone under 16 that I talk to has anonymous Tumblr accounts for different personas. They are actually not into putting photos of their trips up on Facebook. No one that I know under 16 does that anymore.

That's great, thank you.

One other point I'd like to make, since you're based in London, is the idea of the Investigatory Powers Act. I actually wrote an open letter to David Cameron ('Encryption should be a global human right, Mr Cameron') at one point when he was talking about encryption, and I reminded him of the American Revolution. That's when the Brits were excessively spying on their citizens, and the United States decided not to do that. We keep a map of worldwide encryption laws and it maps almost directly: the countries that control encryption are the ones with totalitarian regimes. Countries that control encryption are countries that control their people. Encryption is power to the people. And so, when Cameron was talking about this, and May now, I say, 'hey guys, do you really want to be on the yellow team? Look who's in it.' It's not the kind of society that you guys want to build and live in either.

♣♣♣

- *This Q&A is the eleventh and last of 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.