ARTICLES > INTERVIEW

Digital Security in Social Justice Work: A Conversation with Sarah Aoun

By: Sarah Aoun

MOVEMENTS & MOBILIZATION

Vallejo, Catalina, Eliana Blam, and Sarah Aoun. "Digital Security in Social Justice Work: A Conversation with Sarah Aoun." Just Tech. Social Science Research Council. May 10, 2023. DOI: doi.org/10.35650/JT.3055.d.2023.

Just Tech invited several practitioners and researchers to respond to a simple yet fundamental question: "What is just technology?" This interview was conducted by Just Tech Program Director Catalina Vallejo and Program Assistant Eliana Blam who spoke with Sarah Aoun about the importance of following digital security safeguards when working in activism and human rights.

Aoun is a security and privacy researcher whose work lies at the intersection of tech, human rights, and transformative justice.

In their conversation, Vallejo, Blam, and Aoun discuss the role cybersecurity plays or should play in activist and community work. Often neglected, Aoun explains how the lack of digital security can endanger everyone from protesters on the streets to activist organizations, and she shares how she works to inform others on the importance of cybersecurity.

Catalina Vallejo (CV): Sarah, thank you so much for taking the time to talk with us. You define yourself as a technologist that works on human rights. In the context of the United States, people don't use the term "human rights" as much as social justice or racial justice. "Human rights" is a term, in my perspective, that is applied to other countries. So, I wanted to ask, why do you define yourself as a technologist that focuses on human rights?

Sarah Aoun (SA): It's a great question. Honestly, I've had such a hard time over the years trying to define what I do, because when I started there was no clear path. There still is no clear path. I have tried to make up random titles and names for what I do, but the idea really is being someone with technical

skills, a hacker, a privacy and security researcher, who works specifically with activists, human rights defenders, and journalists.

It's true that the human rights angle is a bit more global, but that's because a lot of the work I do is very global. I'm based in the United States, so I work a lot on domestic issues, but a big part of my work over the last decade is and has been with targeted and surveilled folks around the world, whether it's East Asia, South Asia, Latin America, or the Middle East.

Growing up and working in activism, at some point, I became fascinated with technology, prompting me to ask: "Surely, there must be an intersection somewhere?" Thinking about the proliferation of surveillance cameras, the fact that your name is being collected, your location is being collected, or any type of data trail is being collected, got me to consider the intersection of technology and human rights.

> *We're building all this technology on the assumption that it is going to be used for good, and there will be no nefarious use.*

The question is always, what is the worst-case scenario? What happens if this information falls into the wrong hands? We're building all this technology on the assumption that it is going to be used for good, and there will be no nefarious use. But when you go back in history and take a look at examples of data collection—whether it's the Holocaust or the civil war in Lebanon—it has been used to facilitate crimes. It has been used to facilitate genocide. When you supercharge it with technology, you basically get the same risks at a much bigger and faster scale than was possible before.

CV: I am Colombian and I come from a context in which human rights violations have been an issue since I can remember. But it hasn't been until recently that I thought about the relationship between human rights violations in the context of different political or social problems and technology, and you are bringing to this conversation the factor of cybersecurity. In particular, one of the things that you have in mind is how to help organizations or human rights leaders face the worst possible scenario.

Can you tell us more about what those risks are? Because when people are thinking about the risks that human rights defenders face, it concerns their physical safety or that of their families. I don't think everyone has considered the cybersecurity angle and the horrible things that can happen in that realm.

SA: The reality is that there's a direct correlation between cybersecurity harm or online attacks to real-world attacks and to physical attacks. If you look at Pegasus, for example, which is a spyware developed by the Israeli spyware company NSO Group, governments have used it to target politicians, journalists, and human rights defenders and activists. In looking at all the use cases of it, there is a direct correlation of someone being targeted and hacked by Pegasus to then getting arrested or imprisoned for their work.

It always escalates and this is the first step. Someone is surveilling you, tracking you, monitoring you, following you everywhere you go, looking into the type of work you're doing. You have this constant

shadow behind you of someone that's deep in your digital life, which is your device. It's the most intimate and vulnerable part of you in so many ways. You carry it with you every day. You use it all the time for photos, notes, calls, text messages, searching on the web. This small device carries basically all of your thoughts and feelings, and someone is surveilling it and has direct access to it. That very often also leads to situations of you being arrested, attacked, or worse, for the work that you do.

With all the protests that happened over the past couple of years, one very common tactic on both sides of the political spectrum was to dox people. Photos and videos of protests were shared to identify who was present and then put protesters' information online, call their employers, call their family members, or just expose them. That also leads to physical violence as anyone can show up at your house, or find you and follow you, and sometimes worse. So, there's always a direct correlation between online threats and technology's impacts on your well-being, whether it's physical or psychological. If all of a sudden your information were available online, even if it doesn't necessarily translate into a real physical threat, the emotional and mental impact can be enormous and very difficult to handle.



CV: One of the things that we want to do with the Just Tech platform is include reflections about the Global South. We are hoping to highlight more global perspectives and this is in part why we wanted to include your voice because you work in both the United States and abroad.

Could you share some cases or countries where you have worked and that we should be paying attention?

SA: It's a great question. The answer is complicated because truly it's everywhere. I've worked on Hong

Kong, Ukraine, Palestine, Tibet, Myanmar, and others. Anywhere where there is a conflict or there is that type of clash of powers. There's always a group who will pay the price and who will carry the burden of greater conflicts, like journalists, human rights defenders, activists, and minorities.

Let's look at the example of Ukraine, because it's one of the most recent ones. When the conflict started, one of the main concerns was how to support journalists on the ground. They were just starting to report on the war, and they were going to be targeted, harassed, and could face imprisonment or death. A big question was, how do we support journalists to communicate safely with each other in a way that someone cannot intercept their communication? How do we support them in encrypting their files? How do we support them in being able to receive information and also share information with the rest of the world? How do we support them when there is an internet shutdown?

> *Very often the cybersecurity advice that you're giving to a group of people differs from place to place or country to country.*

There are so many different considerations, and it's a very challenging situation because the geopolitical context is unique. Very often the cybersecurity advice that you're giving to a group of people differs from place to place or country to country. Ukraine is not the same as Palestine, and is not the same as Tibetan refugees in India.

I've been lucky enough to get to work with all of these different groups because of this very unique position of working on cybersecurity, privacy, and human rights, which is truthfully a rare intersection. There's not a lot of people that do this work—cybersecurity with the context of what it means to be targeted and on-the-ground and in a conflict zone.

Eliana Blam (EB): Could you share a little bit about CryptoHarlem?

SA: CryptoHarlem is, as you know, a great initiative by Matt Mitchell. I've been super lucky to know Matt and consider him a very dear friend of mine. One thing that we've done together is CryptoHarlem.

In 2020, when protests started in the United States, Matt and I, for the first few weeks, were sleeping three or four hours a day because of how much we were supporting protesters. Because, again, there's not a lot of that intersection between having security skills and knowing how to work with targeted and vulnerable populations.

So, we were putting out guides. We held a lot of workshops to teach people about digital security. We did a lot of triaging and incident response work. Basically, explaining to people, how can you show up to a protest safely? What does it mean for you to show up to a protest with your phone on you? What can and cannot be tracked? How can this get you into legal trouble?

As things kind of calmed down after the first few weeks of us working around the clock, we transitioned a

lot of this work to a virtual space. It was the pandemic so it was hard to meet in person, so we set up a weekly stream where we would just talk about security and social justice, security and protest, and abortion security. Whatever topic was important and was being asked for by viewers.

Matt has been organizing CryptoHarlem events for years, and he started the stream during the pandemic in 2020, and it's continued for the past two years. We meet online once a week: We pick a topic where people ask us to talk about something; and then we dive into the implications and the intersections of social justice, human rights, and technology. Most recently, with all the abortion ban cases, that was one thing that we tackled and that we talked about. There's always something.

CV: I wanted to ask you more about the community work that you do, because my sense is that the one-on-one work will be with individuals, but you are also working with organizations. So, how has that been for you and how do you build these connections with organizations? My sense is that it extends a little bit to CryptoHarlem because you're also working with a community.

SA: CryptoHarlem is very much like a community educational project. It started by serving the community in Harlem and people who are overly surveilled, Black and Brown folks, and extended online. It has a little bit of a bigger reach, but it's still, at the end of the day, a very introductory look into technology and how it impacts people. It's meant to serve a very wide audience and folks that are impacted by surveillance.

On an individual level, I work with high-risk individuals and highly targeted individuals, and I also work with a lot of organizations. For organizations, sometimes it looks like engaging with them for a few months. Sometimes it means working with them for a few years, but it's essentially looking at the mission, what they're doing, and making sure they have a strong security stance to protect their work.

There are a lot of organizations doing incredibly important work that are on the front lines of change, but they don't have two-factor identification on their accounts or they're not using a password manager. We're talking about very low hanging fruit here, but they are small changes that could significantly impact the security stance of an organization and ensure the safety of its employees.

> *The organization is supposed to ensure that security. You can't assume that each individual is going to be responsible for their own security.*

Very often a lot of the conversations around digital security are at an individual level. What are you supposed to do for your own security. The conversation needs to shift to the organizational level, which shifts that responsibility onto the organization itself. The organization is supposed to ensure that security. You can't assume that each individual is going to be responsible for their own security. As an organization you have to be able to have certain policies and make sure that everyone has some protection. Because an organization or a group of people, like a community, is only as safe and as secure as their weakest link.

If you're thinking about an organization, maybe the person who will be the most targeted and who has the most public profile is the director or the CEO. But the person who actually might end up getting targeted is, say, the assistant or the entry-level employee because we just assume that they're not going to have very strong privacy and security protections as opposed to the C suite executives. So, it's really important to make sure that everyone in the organization, whether you're the lowest level employee or the highest-level employee, has a very good understanding of security.

Thinking about working with organizations in the Global South, one thing that's usually quite challenging and a huge difference to working with US organizations is around hardware and software access. A lot of organizations I've worked for or with, usually have one laptop per three employees. And that laptop was bought years ago and hasn't been updated since then and barely works, except for the internet and, say, Microsoft Word. You cannot upgrade the laptop. You cannot do a software update. You cannot add passwords. It's stuck in time. So, how do you ensure the security of an organization when there's only one laptop for three people and that laptop is over a decade old?

These are very difficult questions to deal with, especially when a lot of these organizations are funded by US and European funders who will not fund equipment. They will fund projects, but how are you supposed to work on your project if you don't have equipment? That infrastructure level is very often neglected and forgotten about, yet funders will want to come in and fund security work or digital security work or interesting projects, but not fund your hardware equipment or your subscription to pay for a security service.



CV: What are the particularities of working in the Global South? You mentioned conflict and now you mention infrastructure. Do you still see technology communication becoming very important? Do you think that something changed with the pandemic? Do you see any change or anything particular happening, maybe not like a new problem, but something that got exacerbated by that moment in history in which basically the only way in which you could connect was through technology?

SA: A lot of things changed with the pandemic. A big one is when governments take advantage of public fears to justify rolling out more surveillance. They did that after 9/11 in the United States. They instilled these new surveillance practices that never went away. With Covid it was the same thing. Governments and people in power exploit public crises, like fear, to justify rolling out quite excessive surveillance practices that are never rolled back. Once they're rolled out, they seep into public consciousness and are very hard to remember what life was like before. You walk down the street and you see surveillance cameras and don't think twice anymore. You go to the airport and now you have to scan your face before boarding flights. And people are like, "Yeah, I guess so, we have to do it." People don't really challenge authority, especially when the excuse is public safety.

During the pandemic a bunch of governments rolled out contact tracing apps supposedly to track down the spread of the virus, but a lot of them had excessive permissions. Some of these governments were

European nations, and some of these governments were Gulf governments. Amnesty International has a good investigation on this.

That's basically what happens when the world is forced to transition to digital technology. The risks around technology obviously become a lot bigger, and hackers also take advantage of it. A big thing that hackers did during the pandemic is take advantage of people's fears and the fact that everyone was online and working remotely to then send you an email, "Hey, it looks like you've been infected because you were exposed to this person. Click here to find your health record." You would click on it and then spyware would be downloaded on your computer or they would try and steal your credentials.

When you equip the government, specifically an authoritarian government, with the means and access of surveilling people, they're never going to turn this back over.

With the move of everyone online, there was a huge uptick in hacking attempts on the one side, and a huge uptick in surveillance on a global scale in the name of public safety. But when you equip the government, specifically an authoritarian government, with the means and access of surveilling people, they're never going to turn this back over. They're going to keep that access, and they're going to use it to either criminalize or go after anyone who challenges authority and in a lot of cases that means human rights defenders, activists, or journalists.

EB: Thank you so much for sharing. My last question is where have you been finding inspiration lately? That could be people, organizations, places, media, anything.

SA: Really, anything that's not technology, as much as I can disconnect from it. Breaks are so important and so necessary, especially because I don't just work in technology. I work in technology and the world—society, human rights.

I take breaks away from technology when I can. That means finding inspiration in walking in the park or in learning a new random skill that involves building something with my hands, or reading a lot of fiction. The burnout is so real and so serious because we're working on security with incredibly sensitive populations. As much as I love my work and I love the people that I meet, a lot of the folks that I know are in prison. A lot of the folks that I know have been beaten. A lot of the folks that I know have been killed.

Burnout is serious, and there's a lack of capacity. There are not enough people that do this work but the world never sleeps. Conflict never sleeps. It's hard to say, "Oh, I'm going to take a vacation." I mean, it's a very intentional choice and a very difficult one to say, "I'm going to go find inspiration in the park." Or, "I'm going to go find inspiration and learn a new skill." It's something that has become a practice, a very intentional practice, and I hope we all find the space to do so.

This interview has been edited for clarity and length.