Cybersecurity, Surveillance, and Privacy: An Interview with Matt Mitchell

By: Matt Mitchell

SURVEILLANCE TECHNOLOGY

Vallejo, Catalina, and Matt Mitchell. "Cybersecurity, Surveillance, and Privacy: An Interview with Matt Mitchell" Just Tech. Social Science Research Council. May 3, 2022. DOI: https://doi.org/10.35650/JT.3031.d.2022

As part of our "What Is Just Tech?" series, we invited several social researchers–scholars, practitioners, artists, and activists—to respond to a simple yet fundamental question: "What is just technology?" This interview was conducted by Just Tech program officer Catalina Vallejo, who spoke with Matt Mitchell, Technology Fellow at the Ford Foundation. Mitchell (he/them) develops digital security trainings, technical assistance offerings, and safety and security measures for the Ford's grantee partners. A hacker, developer, operational security trainer, security researcher, and data journalist, he founded and leads CryptoHarlem, impromptu workshops that teach basic cryptography tools to the predominantly African American community in Upper Manhattan.

In their conversation, Vallejo and Mitchell discussed his personal journey, what it means to be a hacker, how surveillance technologies are tested on marginalized communities, and the value of conducting research—like the research done in tandem with CryptoHarlem—that centers affected communities and prioritizes empowering those communities at the same time.

Catalina Vallejo (CV): Matt I want to start by asking you a little bit about your career trajectory. How did you get to where you are now?

Matt Mitchell (MM): I'm a hacker and cybersecurity person, so I worked everything from military contractors to startups and the news business. I was a data journalist at *The New York Times* and there were a lot of extrajudicial killings of Black men in the United States. The national attention on this issue started with Trayvon Martin and the George Zimmerman trial. That happened between my time at CNN and The New York Times. The verdict took a while, I remember that day like yesterday. It was very sad.

I was hoping that this trial would find George Zimmerman guilty and you know anything can happen, but I wasn't prepared for my emotional, mental state. I felt like someone in my family or someone I had known had passed away. It had a very strong impact, and I think it's because this was one of the few times where a ground swell of local and organic use of social media brought attention to a story. Then it became part of the national conversation. For George Zimmerman to be fully acquitted, it hit me very hard. Going back to the regular work was impossible. I really wanted to do more.

I reached out to a bunch of nonprofits and got invited to a conference called the Circumvention Technology Festival (now called the Internet Freedom Festival), and I was like, "How is this a thing, how do these activists and human rights defenders even get here?" I got schooled on what a fellowship was. I decided, I must do something different, let me try.

I got the Ford-Mozilla Open Web Fellowship and I haven't looked back since. Now I work at Ford. That first fellowship changed me as a person. I'm always giving thanks for that through the work I do each day. Fellowships can also be for folks in the private sector—it doesn't always have to be for researchers. One of the things that I have tried to do is to attract folks from the private sector, specialists who work at tech companies or tech firms, and to bring their expertise into this space.

Once you know how things work, you know how they do not work as well. I really committed myself to try to raise awareness on surveillance practices.

CV: I would like to hear more about what it means to you to be a hacker.

MM: For me, being a hacker is looking at code, devices, and hardware, and making them do things that they were never intended to do. How can you trick technology into doing something its programmer or creators or the company that made it didn't plan for it to do?

Even as a child, I always took things apart. My dad was working for the train yards as an engineer. He'd always bring home some parts and take them apart. I would take my toys apart while watching him. When I was exposed to my first computer at school, I was like, "Oh what's inside of that? How's that happening? How's that work?"

I would get computer jobs and they would let us know quickly that our real job was to monitor and surveil employee behavior. I became quite alarmed by this, but this was my job. So I learned a lot about surveillance and counter-surveillance and how to stop things from working. Once you know how things work, you know how they do *not* work as well. I really committed myself to try to raise awareness on surveillance practices.

I'm very empathic and I always want to look out for other people. If you slip and fall, I don't laugh. I just run and pick you up. It's my natural impulse. Your average hacker? They're more like, "I don't care about

the world. I'm smarter than everyone, let me just use my skills and my knowledge for my own sake, and whatever I want to do– mostly to harm people or harm things." That's not me at all. I want to defend people from them. My work today allows me to look out for our grantees at the Ford Foundation.

Quite fortuitously, my skills really make a difference to protect organizations, causes, and things I believe in.

CV: What I find very interesting about hacking is that it's something that you keep doing. Now it seems to have a very different orientation, which is connecting social justice with all these technological skills that you have, but also helping people use their technological skills in a good way. So, I'm wondering how did you get into your work with CryptoHarlem?

MM: CryptoHarlem is the thing that I started while I was at *The New York Times*. I was like, "If I'm gonna help my people—Black people, people in Harlem, people around me I can touch—I need to do something in the community. I need to speak to the pastors of churches, the imam of the mosque. I need to talk to the high school teachers and find the kids where they hang out.

I need to reach everyone and just tell them, "Come talk about these things that are directly impacting the community: multiple layers of surveillance that—when you compound them—you have a community that's living in a very different world than the person sitting next to them on the train."

You'll find this in a lot of marginalized communities, whether you're undocumented, Black, brown, Arab, Muslim, queer, a sex worker, or whatever marginalized group. You're in a web of surveillance that criminalizes your very behavior. It's like walking through landmines every day and it's quite easy for something to go off. There's literally a police box on robot legs with someone inside of it in your neighborhood. You don't see that in other parts of Manhattan. Why is it here? Who put it there? What does it do? What are the sensors in it? How's it work? What's the company that makes it? How do we push back against it?

Portrait of computer hacker Mathew Mitchell. By Ethan Hill.

Those were the things that we spoke about and I continue to speak about at CryptoHarlem and it actually helps people. All young people are told, “express yourself, go on social media, TikTok, YouTube, Twitter whatever. Be creative, create all your content, we’ll make all the money, and maybe we’ll split some with you.” But if you’re from the inner city or if you’re black or brown or part of any of these communities there’s a strong likelihood that someone is monitoring social media and they’re going to misinterpret you and see you as the absolute worst, criminalize everything you’re doing, and you could easily end up going to prison for like a tweet, a number in your phone.

For me it’s just about researching this stuff and understanding it well enough that I can have a conversation with someone who has no reason to agree with me, and even they will say, “wow I didn’t know that” or “that can’t be right,” and then they look at the facts and they’re like, “wow that is right, something needs to change.”

All these technologies that are encroaching on our civil liberties happen in these communities first. They’re almost like beta testing these communities. So there’s a lot—if we can push back and stop it by just illuminating it with research and information, and some personal stories to bring it home—that we

can stop in its tracks. CryptoHarlem is about that. It's about changing the paradigm and understanding that this is what we all must do.

CV: It sounds that one of the things that you do is extensive research trying to define how surveillance takes place. How does this research part work?

MM: Most of the time, someone already starts peeling the orange, right. There's a story about a man in Detroit who was accused of stealing some jewelry. Facial recognition was used from some blurry photographs, and basically the robots were like, "this is the person, arrest him immediately." They picked the wrong person and until a New York Times article, they weren't even going to expunge this record. He could have gone to prison for the bulk of his life. You'll see stories like this, but I believe that people who are directly impacted–and the people who love them and care about them–will solve their own problems.

At CryptoHarlem we hold community events, and someone will say, "I was stopped on the street, man. I was on the corner and they asked for my phone, and took my phone for two hours." And I'm like, "What? Wow, that's really weird." Then you follow up on those stories and that's how you get the best research. I'll call some homies in Chicago who are doing privacy work. And I'll say, "Hey you ever heard anything like this? That's happening here too, it's really weird." And then you're getting this completely different angle on it.

That's where we live, because I want to help real people. I don't want to help researchers.

I don't want to help people with six figure salaries. I want to help real people who are getting crushed under these things.

To do that, you got to be real, you got to talk to folks, you got to know their stories, you got to know the things that are like, "well this happened in my case, it was kind of weird, it's an imperfect story…" It's not imperfect to me because it unveils a process that's being used against an entire populace.

And that's what we do.

I'm a nerd. I love technology. It breaks my heart that something I love could hurt anyone I care about or anyone in my community.

CV: This community research points to the ills of technology for minoritized communities, but at the same time you also see the potential of technology to do good things, right?

MM: I'm a nerd. I love technology. It breaks my heart that something I love could hurt anyone I care about, or anyone in my community. For me it doesn't make sense to just point out the ills and the problems. I try to stay solution-based and evidence-based. Why don't we do this? Here's people who are trying to do this. Here's the successes they're finding. These are the challenges they have.

People will say, well facial recognition caused this thing to happen. Are you saying there should be no cameras? Are you saying the cameras shouldn't be able to see a face? What if one of your relatives is hurt and something happened to them and facial recognition could've helped them?

In surveillance, privacy, and tech people have too much of a libertarian view, and too little of a humanist view. There's no heart. You'll hear arguments like, "Encryption is used by horrible people who commit crimes and hurt children. But cars are used by bank robbers and we don't ban cars." Let's go back to the people who were hurt. How can we help? What's your solution? How can we keep people from getting hurt?

Consider Apple looking at every photo in your iCloud to flag pictures of children in an illegal images database. There is some good that can come from that. But let's talk about the bad that comes from that. For many LGBTQ folks—especially young folks—their phone will end up reporting them through a false positive that could ruin your life. In the name of protecting the most vulnerable—whether that's stopping terrorism or protecting children or public safety and policing—we create a lot of evil things.

I don't want to just say turn off those things. I want to say, let's open it up for more feedback on how many people get hurt by it and how many people get helped by it. When you get everyone who's affected by this on all sides together, I'm sure we can figure something out that's better than what we have today. That's what these challenges call for, not a blanket: "this technology is bad" or "this technology is good."

> *We have to understand that all technologies have the potential for very serious harm, and that there are communities that will be harmed disproportionately. We should think about that first, to protect against and mitigate those harms.*

CV: What are the reasons to be optimistic about the possibilities for tech justice?

MM: Things are getting better. I remember when—to use an app or to use a piece of software—there were no terms of agreement or privacy and security settings.

The speed of progress is not fast enough for me. We need to celebrate all victories. I celebrate every victory. I celebrate the smallest thing.

There's something about the human spirit that will always try. We have to respect our ancestors who dealt with fewer options, and people in other parts of the world who have very restrictive environments. They still manage to find hope each day, and still manage to find a way to protest, improve, and teach the next generation that this infringement on our liberties is not normal.

I'm going to push as hard as I can. And I want people to push with me. And I know that we're going to get there. I love tech. Tech is awesome. It's the promise of all the libraries of the world to all the children of

the world. But we can't be foolish. We have to understand that all technologies have the potential for very serious harm, and that there are communities that will be harmed disproportionately. We should think about that first, to protect against and mitigate those harms.

CV: I want to finish by asking who are some people working in the cybersecurity and civil liberties space that you think we should be paying attention to?

MM: There's the work of Simone Browne who wrote *Dark Matters*, which is the history of surveillance of Black people. Once you read that book, it helps you realize these things were in place when technology was the wheel, or fire. It's a long struggle. There's the book *Predict and Surveil* by Sarah Brayne. Also Joy Buolamwini who was in the movie *Coded Bias* and Timnit Gebru who used to work at Google and is one of the co founders of Black in AI. Ifeoma Ozama, who used to work at Pinterest, is fighting for tech worker rights. She is trying to make legal change because a lot of these tech companies have interesting employee agreements where you sign away your rights. There's a lot of new reporting on people at Google, Apple, and other companies trying to fight back and get their rights back, and it is a lot harder for them to expose the wrongs that they're seeing because of their employee agreements.

Some organizations doing amazing work include Media Justice, Color of Change, Black in AI, the Algorithmic Justice League, Calyx Institute, and Blacks in Cybersecurity. I think the thing that is the same about all these groups is they're made up of directly impacted people and the allies who did the work. That is the secret sauce for being effective.