sonix

NAME

Seda Gurses.mp3

DATE

April 16, 2024

DURATION

44m 33s

START OF TRANSCRIPT

[00:00:17]
Welcome to Radical a-I, a podcast about radical ideas, radical people and radical stories at the intersection of ethics and artificial intelligence.

[00:00:27]
We are your hosts, Dylan and Jess. Just as a reminder for all of our episodes, while we love interviewing people who fall far from the norm and interrogating radical ideas, we do not necessarily endorse the views of our guests on this show. All right. So let's set the stage here, Jess. We are recording this episode on Monday, April 13th, 2020. In response to the breaking news that came out this past Friday that Apple and Google will be partnering to support contact tracing in response to the spread of the novel Corona virus.

[00:01:01]
According to Apple's press release, first in May of this year, both companies will release application programming interfaces commonly known as API Eyes that will enable interoperability between Android and iOS devices using apps from public health authorities. These official apps will be available for users to download it via their respective app stores. Second, in the coming months, Apple and Google will work together to enable a broader Bluetooth based contact tracing platform. By building this functionality into the underlying platforms, this is a more robust solution than an API and would allow more individuals to participate if they choose to opt in, as well as enable interaction with a broader ecosystem of apps and government health authorities. So what does this mean? Basically, Apple and Google are working together to enable third parties, be it the government, tech companies or health authorities to track. If you have been in close proximity to people who have contracted the Corona virus or been near others who have through your personal cell phone, obviously this is huge news and this is an unprecedented partnership between these two tech giants.

[00:02:21]
There are so many questions and potential privacy and ethical concerns brought on by this contact tracking partnership. So to break down all of the nuances of this breaking news, we brought in an expert for this episode. We were so lucky to be able to connect with a well-known expert in privacy and surveillance.

[00:02:41]
Dr. Seita Cursus Seita is currently an associate professor in the Department of Multi-factor Systems at the Faculty of Technology Policy and Management at T U Delft and an affiliate at the Kosek Group at the Department of Electrical Engineering at k._u looooove in Brussels. Her work focuses on privacy enhancing and protective optimisation technologies, privacy engineering, as well as questions around software infrastructures, social justice and political economy as they intersect with computer science.

[00:03:16]
We're going to skip our Norell intro and get straight to the heart of the matter. We are so excited to share with you this interview with Dr. Seita Garces.

[00:03:32]
So we're here with Seita to discuss this breaking news about Apple and Google debuting a major effort to help people track if they've come in contact with coronavirus and specifically and this is by The Washington Post. Apple and Google unveiled an ambitious effort this past Friday to help combat the novel Corona virus, introducing new tools that could soon allow owners of smartphones to know if they have crossed paths with someone infected with the disease. And we are so grateful to have say to. Here to explain to us a little bit about what this means and whether we should be worried about these new contact tracker apps that could be out to developers very, very soon. So sayto what should we think about this news?

[00:04:20]
The news is much bigger, entails much more information that is actually written in black and white, be it and ask here on paper. I think that that Apple and Google have to walk in for us to be able to develop contact tracing apps is itself, I think very big news, right? This means that in order to use advances in technology in our societies, we depend on a couple of companies at least to come in and make a decision. And that without their cooperation, certain things would not be feasible. I think that in itself is like a opener for those for that announcement. The other thing that happened.

[00:05:07]
I have the track back a little bit and say how how that decision.

[00:05:13]
Came to be. I don't know exactly how it came to you, but let's say why did it and now certain things and not others and what it was actually doing.

[00:05:21]
So there have been. We're also doing it with lockdowns. Many of us are.

[00:05:29]
Although some countries can't afford them. And and a lot of governments are thinking about how they're going to loosen the lockdown. They call this exit strategy. Many governments have pulled together teams that decide on these exit strategies. And oftentimes this includes government officials and unfortunately, mostly people from governments, you from companies that you would think they would also have people from civil society or communities. But I think those are usually absent in Belgium, where I am currently based there, actually starting to build a shadow exit strategy group so that they can give other recommendations than the ones coming out.

[00:06:04]
So the more official exit strategy, people, I think, believe that one way to not go back to a lockdown when we come out, when the number of Cauvin infected people increases again, is to be able to trace, you know, who is infected and get them to either self-quarantine or maybe even better yet, get tested. So to do this in a efficient way, the usual approach is to do it manually. So you have health workers who who trace by speaking with the infected person. They do an interview and say, who have you seen in the last five to seven days? Because usually I think depending on the number of days it took you to go to a health authority saying, I think I have covered 19. It's usually the case that you have symptoms. And then it's about five days before that that you are actually likely to be transmitting also the disease to others. So they'll ask you, the people that you have seen in that period than you can imagine. If we're out again for the public, this could be somebody who sat next to us in public transportation or this could be somebody we worked with or this could be somebody who was in the queue in a shopping center with us, etc.. So the idea is to be able to capture also those people and not just the people that you know.

[00:07:23]
So at least that's that's the story. Now, there are people who believe that tracing will work. And there are people who don't believe tracing will work. And those two groups also split in two different directions. One of those groups says we need much more data than just the contacts.

[00:07:41]
And this kind of tracing out may lead to a lot of false positives. You know, anybody you contacted is not going to be likely to get the infection. And so those people would say things like we need much more data, to be precise, so that we don't, you know, cause false alarms. And we can also see behaviors that are wrong, et cetera. And it's funny enough that a lot of these people who are asking for this are either from companies or they're people who do a lot of work with data and machine learning and A.I.. So I actually say Koven, 19, is the new A.I..

[00:08:12]
And what I mean by that is A.I. was the way for a lot of companies to do massive amounts of marketing or to get government to put a lot of funding into A.I..

[00:08:23]
And with that funding into computational infrastructures, we can talk about them in a little bit. Now, you just say covered 19 and you could start mobilizing money and investment and technology. So we're seeing the same thing. And so we called these the data grabbers. So these are the people who say, oh, we need everybody's location data. But that's a very weird premise, because location data is basically product data. Right. Like this is the kind of data that either telecommunications companies or big corporations like Apple and Google used to deliver their products. So they're optimized for their products and they're used to they're also optimized, generated and optimized manner for improving their products and their bottom line. And all of a sudden, consider that Data's health data is first of all, misleading, makes us think that data is somehow truth or representation of what we do instead of product data, and also conflates the basically the production of a new health infrastructure with a profit based infrastructure.

[00:09:23]
So it makes it very difficult to separate those two things.

[00:09:26]
So even when academics mean really well, they might be great in machine learning and they might have done some simulations and can imagine ways to contain the virus.

[00:09:37]
I think these people are not very aware of the kind of public statement they're making in terms of taking, you know, a somewhat controversial profit-making computational infrastructures and using that for a public purpose when there is no governance structure to control how those infrastructures will be used except the current as they are currently made for profit.

[00:10:01]
So.

[00:10:03]
And then, you know, some of those statements might be moderated by saying we just need anonymous data. We just need to anonymize location data. But you can imagine that that doesn't solve the problem. All right.

[00:10:14]
You still have the issue that you're using product data that looks like location data as a truth for health data. And you're conflating infrastructures.

[00:10:26]
So the other side of the people say we cannot have these apps. And I think that's a very interesting voice to hear. And they basically say what we're being offered is a dichotomy between either we have to stay home or we need if we want to go out, we need to be under surveillance.

[00:10:42]
And since these apps are likely not to work, they're just an excuse to open the doors to population tracking and population management and also being able to go back to business as normal.

[00:10:56]
This the business as usual that brought us covered 19. So we actually need to radically re-envision the world that we live in. Instead of, you know, being able to imagine doing global travel like mad again, where, you know, we maintain the risk of that through the surveillance of a whole society.

[00:11:14]
So I think that those are kind of like the two responses and the efforts that I'm part of are basically somewhere in between.

[00:11:25]
And they say, let's generate our own data. So let's build an app that generates tracing data so it doesn't use location data.

[00:11:35]
We don't need to know where people saw each other. We just need to know that they were close by. They were in proximity. And when people first hear that, it takes a moment to understand the difference. For example, Dylan, if I saw you at the supermarket, what the epidemiologists and the health authorities need to know is that I have seen you. They don't need to know that it was at the supermarket. That information is absolutely unnecessary. They might need to know approximate time so that, you know, when you go and say, who did you see in the last five days? You know, they can give an account of those five days.

[00:12:09]
And but they don't need to be location specific or have a very precise timestamp, because that is not necessary, neither for contact tracing nor for the epidemiologists to study how the virus is spreading.

[00:12:23]
So these applications.

[00:12:26]
Are being built mostly by people who I would say our privacy engineers, so people who try to think about ways to design privacy protections into hardcoded into the system so that it's not so easy to repurpose this system for something else. But so there are, let's say, two or three principles that privacy engineers go by. First of all, you need to tell me exactly what you need. So the idea is not you collect data and you see what you can get out of it, but you tell me exactly what do you need. So they go to, in this case, epidemiologists and health authorities and say, what is it that you need? OK. You need to trace contacts so you don't need people's location. You don't need timestep. Right.

[00:13:06]
And then they would then look to see how they can avoid it so that a centralized party or centralized parties get unnecessary data.

[00:13:18]
So is there a way to make the functionality happen without introducing a surveillance party? So this is what they did.

[00:13:25]
And they designed an app where phones would use their Bluetooth capabilities to send anonymous identifiers. So basically random numbers which are not totally random, they're cryptographically generated. They look random to somebody who's looking at them, but they're generated with a seed. And all the phones that have the same app would capture those random numbers and would basically say, OK, these are people I've been in contact with and they would have, you know, sort of time of day, approximately no power and no location data, just the fact that I have seen these numbers. Now, if I were infected, I would go to a place where I can get tested. And if I tested positive, I would use that to generate a new step with my app, which is that I could selectively take some of these anonymous identifiers that I emitted. So not my contact information, but just the ones that my phone emitted and packaged them in a way and send them to a centralized authority. So all the centralized authority gets an anonymous transmission of a package of numbers, OK? They can't relate them back to me. They know that the numbers belong to one party, but that's all they know. And then the centralized party sends this information to all the apps. So they update.

[00:14:42]
They basically get this package and then the phone locally checks to see if any of the people that have it see how do I say this? So let's say I am the one infected.

[00:14:59]
So my package of all of my numbers goes uploaded and then it gets sent to all the phones. Now, Dylan wants to know if somebody who he has been in contact with has been infected. I am not infected. We have been in touch. Which means he has some of the numbers my phone generated in his phone. So Dylan's phone now checks against this package. He cannot look inside the package, but you can check against his package to see if any of the numbers in his phone from all his contacts match with the package. And if it does, he knows that he has been in touch with somebody who's been infected. And the phone might have some application that says, OK, if you've been in contact with this person, Martin, a certain amount of time or many of those such people, then maybe you should get tested or self-quarantine. Exactly what that looks.

[00:15:45]
This is this is what Apple and Google are currently working on. Is this your kind of your pushback? So is this what they're doing or this is what you wish they would do?

[00:15:53]
I know I have to say so many things, and maybe you will find a shorter way to say all of this.

[00:15:58]
So now this is one way to do the app, right? What it does is there is no centralized authority that can find out who my contacts are.

[00:16:06]
The centralized authority, all that it's doing is transmitting these random numbers from the phones of people who were infected to all the other files so that they can check locally if somebody was in contact with somebody who was infected and they should get tested.

[00:16:21]
There were other approaches and these other approaches are anywhere from using location data, which is not precise enough. Right. Like it doesn't actually give you a contact information to people saying actually what you should do is when you're infected, you should upload all of your contacts to the centralized entity to see how that's different.

[00:16:40]
Like not just my numbers, but all the people I've been in contact with. And then that centralized authority, can we identify who my contacts are and send just them information saying they've been in contact with somebody who's been infected? So this means that the centralized authority gets the social graph of people who are infected and can reconstruct our whole social contact graph, which is very problematic here. But they can argue that they can they can do this because it allows them to improve their algorithms and they can do a eye on it. And all of these kind of things. But now we have an app that, as more and more of us get sick, reveals our social graph to a centralized entity. The advantage of that approach is that.

[00:17:26]
The people who receive notifications that they've been in touch with an infected person do not do that matching on their phone, which means they cannot hack their phone to find out who might have potentially infected them. Right.

[00:17:40]
Because if all the matching is on your phone, then all the data, if you really wanted to, you could, you know, add an app, you could take the numbers out every half hour and time them and write somebodies name down or take photographs of them. You can imagine somebody doing this as you would always imagine individuals who's going to do that. But you can imagine and incentivized person who might do that for a specific location and then you can check to see who might have infected you, which might be problematic. So what happens when you go to a decentralized design? So the first one is a decentralized design where the matching is done on the phones, not by a centralized entity. You now have attacks at the edges right around the phone. When you have the centralized entered design, you have attacks that are possible on the back end, which means that a government entity or law enforcement or intelligence agencies or hospitals. Right. Might all of a sudden use this information in unwanted way. So basically the two designs allow you to decide which of these potential negative outcomes might happen and how you're going to safeguard them, because at the end of the day, you can't safeguard everything with technology like that. The point is like, which map in a sense we're deciding between these protocols. But in another sense, we're deciding which kind of society we want to be and where we want to put safeguards. So we have two designs that are not the data grabbing. I'll take all location data in the world that are not I don't want any apps, which I think is also a legitimate position to have. But that says, no, we can actually do it. We generate our own data and then we can minimize the data, just get the contact. The only question is, does a centralized entity decide who is informed and has to get tested? Or do people themselves have the incentive to decide whether they are going to react based on this information and get tested or quarantine themselves? So those are the two differences.

[00:19:36]
For all of these apps to work that are based on Bluetooth, there needed to be cooperation with with Apple, because if I understand correctly, Apple does not allow Bluetooth to to generate or receive information if it is in the background. If the application that's using it is in the background, which meant that for any for people using Apple phones to continue using this app, they would always have to have it in the foreground, which, you know, that doesn't make sense.

[00:20:06]
It's a battery killer. You would have to have an app on when their phone is in your pocket. Right. Like if you use another app, all of a sudden you would not be using this app, etc. So there needed to be a cooperation with Apple anyways. Right, to make these apps work. What happened is Google and App agreed on some interoperable API and said we will allow you to use this bluetooth functionality, but only on the phone and only within the protected zones for a bluetooth. Let's just call it that way without going into too much technical detail, which meant that now you will never get your contact data out of your phone, which meant that all of those centralized designs are basically not possible.

[00:20:52]
Right. So they made a technical move that would enable these data minimize I minimizing privacy, preserving applications to be deployed, but only to decentralize ones which do the matching on the phone, the centralized one cannot be made based on this architecture.

[00:21:10]
Wow. Yeah. So it sounds a little bit like Google and Apple made a political statement there by doing that.

[00:21:15]
Yes. Yes. So they made a they made multiple statements. Right. Like they said. Well, if you want to have any sort of contact tracing with Bluetooth, you had to talk with us.

[00:21:24]
Hello. So that's number one. That was how we opened. Right. And then they said you can only use this if it's privacy preserving in a certain way, namely the tracking through the Bluetooth does not leave the phone. So you cannot make centralized apps.

[00:21:39]
So it's something that I'm wondering, I guess, without the centralized apps in the equation anymore, since that's not really possible. But the decentralized apps are location tracking apps. All of the possible solutions. It seems like there's pretty much a tradeoff that has to be made no matter what we choose, whether it's in terms of less tracking or in terms of longer quarantined privacy law, surveillance, whatever it is based off of your research. Two questions here. The first question is, which of these do you think is the best solution? And the second question is, which of these solutions do you think is most likely to happen in the future?

[00:22:18]
Oh, OK. So I personally am a believer that which is the best solution needs to be subject to Democratic discussion.

[00:22:28]
Right. And and I think that discussion has not yet happened. And in a sense, I'm kind of proud of the project that I am part of.

[00:22:37]
Dp 3T because it was the only project that in the design phase went public and put their design documents, design in progress documents onto GitHub and invited people to come and discuss the design and to give feedback and not just technical but also social and political ones. And I highly recommend seeing one of the comments that they got on GitHub, which I hope you can link to.

[00:23:02]
It's called the long tail of contact tracing and it basically is a bug report on the whole idea of a contact tracing app. So that's kind of a beautiful social critique of tracing apps that are in that that is in the GitHub. So that's kind of a fun thing to look at.

[00:23:21]
However, if you look at both the efforts of the government so far, which is Maze basically either talking with companies behind closed doors, there was a consortium petitti that the peace treaty was originally part of that never was public about their governance structure and how they would decide between designs. They came up with both a centralized and decentralized design.

[00:23:44]
The centralized design is still not public, but also the way Apple and Google just came out and said we'll open, we'll offer these API. Which was kind of important for being able to build these apps. But then they also said, and this is really crazy. They said, we'll implement the contact tracing protocol. And they didn't say it's an app. They said we'd put it into our operating system. Right. And so that is huge. What does that mean? Let's let's think through at least some of the things that means. So all of that I said about Democratic discussion about what kind of app we want to have, you might want to have that within a community, maybe maximum within.

[00:24:26]
That's a the jurisdiction of a nation state or in Europe, you can say maybe it makes sense because, you know, we've supposedly removed borders and Shengen kind of you know, every time refugees come, they close.

[00:24:35]
But but let's say like within EU, there's freedom of movement for some people. So it makes sense to make it EU wide decision.

[00:24:46]
That decision requires the local authorities, whatever or the local communities to have influence on the design. Right. And by putting a protocol into an operating system.

[00:25:01]
Or at least that's our proposal now. And it'll be interesting to see if they'll do it. They have removed the possibility of local discussions. Right. They made a decision. So what is the best protocol? And they just propose it to the world. They said we're gonna do this because it's the best protocol. So you mean you can ask me what I want? But, you know, Apple and Google decided something.

[00:25:21]
And good luck to any of the European countries to go and have a talk with Apple and Google. That could be changed is, you know, maybe we don't want it like this.

[00:25:30]
But even worse, is that the way in which, you know, these large computational companies can break democracy is by entering our pockets first. Right. So they don't need to even go through government institutions. Now, anyone who has a recent operating system with a recent update when this thing is done and installed into the operating system, their company, their organization can just ask them to turn down their settings and turn their contact tracing on.

[00:26:01]
And it doesn't matter if the government has agreed with this or not. Right. So they have basically, on the one hand, gone around any sort of democratic process that even nation states could have.

[00:26:13]
I mean, and they, you know, use their typical way of entering institutions and, you know, bigger structures, which is through the pockets of their users. Right. And becoming like the de facto standard. So they made both. They can now make both of these moves if they indeed fulfill their press release from this week, which is to put the contact tracing app into their operating system.

[00:26:36]
It's not an app. The users cannot just uninstall it. Right. Like it comes with the operating system. It's a huge decision.

[00:26:43]
Quick question for you on that SATA, in terms of like the privacy implications of putting this in the OS or the operating system, the GDP are at least in the EU in large part now in the States because of the way that they implemented it. It saves people from things like this usually. Is this not against the GDP? How is this legal? Is it. So actually.

[00:27:09]
So it'll be interesting to see. I haven't seen any opinion pieces from legal scholars or legal experts yet or, you know, people who do legal stuff as their hobby that they exist to. But I did see something from your pen Koopman, which I think was very nice, which WeChat, which, you know, he argued that purpose specification is is no longer fulfilled for this.

[00:27:36]
Right. Purpose specification says that you will only collect information for a specific purpose. But Google and Apple could actually use this Bluetooth functionality now for, you know, tracking people in supermarkets.

[00:27:49]
And we know that Bluetooth sorry, both Google and Apple have in the past sent beacons out to different brick and mortar shops and different areas to do testing to see if they can use Bluetooth based tracking, which is much more precise. That's why we're using it also in dbp 3T, because it allows us to do contact tracing. Right. And so now if more and more people turn on their Bluetooth, like I usually don't turn on my Bluetooth, but I'm just going out. I know I might be in the minority, but, you know, still I don't.

[00:28:24]
I think if more and more people are using this functionality and have their Bluetooth on because of, you know, health concerns, they believe that this is going to help with, you know, ensuring that they're not infecting their beloveds or people around them, then, you know, one could argue that Google and Apple could now more intensively use Bluetooth based tracking systems as they, you know, expand from the virtual or information based services to more local localized services.

[00:28:54]
Right. So in that sense, yeah. Hank Koopman was arguing that the purpose specification is broken, that you cannot be sure that this functionality will only be used for Cauvin 19 tracing, but for other things, therefore, it breaks the GDP. And I think we will see more arguments like this and we I'm sure we'll see arguments for and against. We've also seen it for DP 3T where people have said, well, this is a health application. You know, the data, the packages that I talked about that are sent out to everyone is health information.

[00:29:26]
And I'm sure there will be arguments for and against those things that we'll see if GDP are is strong enough to keep this contact tracing application to be from being rolled out. And if it can also give people the sense of control that it promises to give rise, that that's what it's supposed to do for those who haven't heard of GDP or GDP is the general data protection regulation in Europe.

[00:29:54]
And it's a European Union regulation that outlines how companies can collect process and store personal data. But I have I have two questions and they're almost like emotional questions because when you talk, I get I get a little worried, right? Like I get a little worried about how much power these organizations have or any of these companies have in coming in and kind of it makes you feel a little powerless.

[00:30:18]
And so I guess my two questions are, should I be concerned? Shouldn't should we as normally people who are working for these companies be concerned? And if we are concerned, what should we do about it?

[00:30:32]
What can we do about it? So, yes, you should be concerned, but you should not be disempowered. Two different paths to go, right? I think, you know, I've always been in my work.

[00:30:44]
I've always tried to work against what we've called Responsibility Nation, which is, you know, making individuals responsible for changing things that are, you know, not going to be something in their power.

[00:31:01]
Like people have said, you know, stop using Facebook. Right. And as a way to protect your privacy, I was never a proponent of that. I was always a proponent of making sure Facebook did the right things or Facebook didn't exist. Maybe that's even better.

[00:31:14]
And so I think that I think that, you know, when Google and Apple came, a help came out with their announcement on Friday. I had a meltdown. I was like I mean, I already had a meltdown with the lockdown happened and everything went online because I've been studying the political economy of these large companies.

[00:31:35]
I call them computational infrastructures because I think that's the best way to to summarize what they are, what they are.

[00:31:44]
I was already studying them and seeing how much global power they were amassing and that they were able to digest any of the things that we have been proposing in more progressive, let's say, or more critical corners of computer science or elsewhere.

[00:31:58]
They digest privacy data, just fairness. Right. They actually turn it to their advantage. And and yet they continue to amass massive amounts of power, the same as regulation. You know, if you want to regulate these companies, there's no way that you can avoid giving more power to them to enforce the regulation. So they're really they suck energy and just grow and grow and grow.

[00:32:21]
Amazon, when covered 19 started basically said we have to focus on delivering things that are absolutely necessary. So they just killed a bunch of small shop owners that were on there on their platform. So I think all of these are examples of the immense power that these companies have amassed. And this immense power is now, unfortunately, on top of that, coupled with global finance, these companies grew after 2008 crisis when the investors had nowhere to go and they just put a bunch of money into these companies. One could argue and this is work with Martha Poon that I do that. The growth of the cloud is basically large investors burning money to investing in a large infrastructure project, which is the cloud. Right. And they have too much power now. They just have too much power. So I think, yes, we should be worried and we should take this example of what happened with Google and Apple on Friday as as a prime indicator of the amount of power they have in not just, you know, messing with our privacy, but democratic structures. They literally can undo democratic processes and structures and they can do so at global scale.

[00:33:36]
So what are the path forward? First of all, I think we really need to think about how we can break down this power. I think I mean, I don't know if I think I believe in market solutions like antitrust. But I think there are some people working on that. And I think that is definitely a direction to go. But I think that there's a lot that institutions can do. There is no reason for any government right now to employ these companies as their basic infrastructure. Right. Most universities went on zoom were on Zoom right now. There is no reason for universities not to invest in their own infrastructure. They have the I.T. people, they have the money. They know approximately how much computing they need. There is no reason for them to buy. I don't know, 7000 licenses and start putting a million a year into a company like Xoom whose future is unknown and who basically will be. Which all means all of our universities will be burning money on the clouds instead of building public infrastructure. Right. I think we need to talk about these kind of what seem like small decisions, but they're not individual decisions. Right. It's not about not using Facebook, but asking your university, really? Do you think by going online with a company that has no educational values, that you can actually keep the integrity of your educational institution? I think these are the kind of discussions we can and we should be having, especially. We have more time because we're at home now.

[00:35:02]
Something that Dylan and I love to do with these interviews is to unpack a little bit of your story and your research as well. So we're really curious about your work in what you're doing right now. Why what you're doing is particularly radical in this space.

[00:35:17]
Oh, boy. OK. All right. Let's see. So I am by training a computer scientist.

[00:35:24]
I identify as she and her with immigration background. I'm originally from Turkey. I'm officially German. I have the privilege of being an academic. And I'm I would say critical computer scientist with a feminist and queer bent. And so, yeah, that means that I belong to a weird minority of, let's say, predominantly out coming out of Europe, feminist trained computer scientists and technologists who think very critically about computer science as a field. Right. Like not just its deployment and instantiation of the world, but how could we do computer science differently? It's something that I'm very passionate about and concerned with.

[00:36:13]
And I don't know if that makes me very radical, but it does make me a huge minority.

[00:36:20]
If minorities can be huge.

[00:36:25]
But yeah, so the DEPI 3T is just one amazing one other amazing example of terrible acronyms produced by computer scientists. It stands for a decentralized privacy preserving proximity tracing. It's a project that is led by Carmilla Tronc coso, which is a computer scientist and a longtime collaborator of mine who's now at the Technical University Federal poli- Technical University of Lausanne in Switzerland.

[00:36:55]
And she's a cryptographer and privacy engineer. And for many years we've been trying to describe how privacy engineering works. And so it's really amazing that at this very moment we can actually instantiate all the things that we've written about and put it to public discussion like saying this is what we imagined four years. Tell us if this is what we should be doing and tell us its limits and tell us tell us its potentials as well.

[00:37:19]
What else? Yeah, maybe one more thing that's really important to know. I was in New York. I was working with Professor Helen Nissenbaum at NYU for two years and had the privilege to work with a lot of great people, especially at m_f_c_c_, which is a media culture and communications department.

[00:37:38]
And.

[00:37:40]
While there, I would I started meeting people who were working in the tech industry, and there was this recognition at some point that what I had learned as a computer scientist as to how software gets produced has nothing to do with how software is produced today. So in the last 20, 25 years, the software industry has gone through a massive shift and and has basically transformed both how that industry functions, but also how the how institutions integrate technology into their bodies. And it was a huge revelation for me. And I started doing empirical work on how software is produced today to think about, OK, how can we bring privacy into it? And around that time, I met Martha Pwn, who does history of accounting, ethnography of finance. And together we'd been looking at the growth of computational infrastructures and their political economy.

[00:38:35]
One thing we try to show, for example, is that all the concerns about advertisment and data aside, what we really should be concerned about is not just the data, but the computational infrastructures and computational power that's being centralized. And in a sense, what we saw with covered 19 as we went really into these computational infrastructures, this was it's going to be a small project. We sped into it. We like spend into it. And I think, you know, when we look at I mean, if I really, like reduce social reality right now, we are now a society of two classes, maybe three, the one classes, a delivery class, the ones who deliver our goods to our doors or they deliver care. And the other is a receiver class. Right. And and then there's, of course, those who are none of these, which I don't know what to call them. But the ones who neither have jobs nor can, you know, be delivered to. And there are those who are on the streets. But I think that this delete delivery and receiver class society was already in the process of being made and it was being made reality. It was coming to reality through the computational infrastructures. So this was, for example, an issue that Martha and I had with all the fairness work. Yes. Fairness assumed that we universalize some sort of objective for algorithms, but these computational infrastructures were building a very unfair society as they were claiming they could make their algorithms fair. It never made sense that Amazon workers could be treated fairly because they usually came from a certain background. It never made sense that Uber drivers could be treated fairly because they're usually immigrants. Right. So what what does it mean to be fair algorithmically when these infrastructures are actively creating an unfair society? And I think we'll continue working on that. And Covered 19, unfortunately, is giving us a lot of examples of what that looks like.

[00:40:25]
Right. And it sounds like we've already I mean, there's been plenty of headlines coming out the last few weeks about how Koven 19 and responses to that are further marginalizing the already marginalized.

[00:40:38]
So there's plenty more for us to discuss on this. Unfortunately, we do have to move towards closing. Do you have any last advice or words for folks who are listening right now?

[00:40:48]
Yes, I think, you know, contact tracing. I think we'll also go into this.

[00:40:53]
We'll continue to make situation worse for those who are already marginalized. So that's, I think, very good to keep in mind. I think the delivery at class is going to be the ones who are gonna be traced massively. Right. They're gonna be the ones who are going to be affected by this surveillance. And with all of its vulnerabilities. But I think what's really important is to imagine what is it that we need right now to imagine the other society that will come after Cauvin 19 and not the one that we can go back to. Right. The whole idea of the tracing app and the vaccines is that once we have those things, we can go back to what we had before. But we are far away from what we were before. We're much more online. We have a different governance structure as we'll go back to our universities and find out that budgets are smaller because they bought a bunch of Xoom licenses. Right. So and they'll say, you know, we recorded all of these classes. Can't we just use them next year so we're not going back anywhere? We're going forward. And I think it's going to be very important to take this time to imagine what that forward looks like.

[00:41:51]
Saito, thank you so much for joining us today.

[00:41:53]
Yeah. Pleasure. Thanks for having me. It was really, really great.

[00:42:03]
We want to thank Dr. satah Garces again for joining us today for this wonderful and important conversation.

[00:42:10]
There's clearly a lot to digest here. I know I'm feeling a lot of emotions right now. How are you feeling?

[00:42:20]
I don't I don't know. Just there's a lot going on in our world.

[00:42:26]
And although I really appreciate Satan's invitation to not feel powerless, it's kind of hard when looking at all of this context. And this this partnership, just as, you know, a layperson or even as a researcher, I just think about, you know what? What can I do here to make sure that my data's protected? Or do I just have to trust?

[00:42:50]
Yeah, I have to admit. Trust is not one of the first words that comes to my mind when I think of Apple and Google working together. But I do appreciate her call to empowerment. I think that's important right now. And it's really the best that we can do.

[00:43:06]
Absolutely. And maybe the biggest feeling that I'm feeling right now is just overwhelmed.

[00:43:12]
I mean, this is a big deal. And Saito is saying it sets a precedent for what can happen in the future. And there's just so much to this topic. And because of how much there is to debrief about this topic in lieu of our normal full outro, we will actually be releasing a mini episode or a mini sode, as we like to call it, this coming weekend. And so we invite you to listen to that if you're interested in more of our reflections on this breaking news. So for more information on today's show, please visit the episode page at radical a-I dot org.

[00:43:47]
If you enjoyed this episode, we invite you to subscribe rate and review the show on i-Tunes or your favorite pod katcher. Join our conversation on Twitter at radical iPod.

[00:43:59]
And as always, stay.

END OF TRANSCRIPT