The Insightful Leader Podcast Transcript

Dialogues: Thinking about Adopting a Contact-Tracing App for Your Company? Here's What to Keep in Mind.

Kent GRAYSON: I think trust is so important. Trust in the employer. Trust in the company that's managing the technology. And then there's the trust in other employees that they're going to adopt and that they're going to carry their phones around.

[musical interlude]

Jessica LOVE: Welcome to a special bonus episode of *The Insightful Leader* from the Kellogg School of Management. When we planned our podcast season, we didn't plan on a global pandemic and the tremendous economic and social disruption that would follow. So we've been periodically sharing some of the conversations that are occurring between Kellogg faculty and business leaders, looking ahead at what comes next for these leaders, their companies, and their industries.

If you're thinking about bringing employees back to work, you're likely wondering: What should you do if an employee tests positive for COVID-19? Increasingly, that answer involves contact tracing. When someone tests positive, the company can use contact tracing to track down who else that person has had contact with.

This process can be done manually by calling up the employee who tested positive and walking them through everywhere they went and everyone they saw over the past several days. Or it can be done using technology, like an app that automatically tracks how often employees' cell phones come within a certain proximity of one another.

Either way, the benefit—in theory, at least—is that companies can pinpoint only those individuals who were actually exposed to the virus, so that they can quarantine and everyone else can stay safely on the job.

But the thing is, contact tracing also comes with some serious risks that leaders need to think through. Not only is the process hard to get right—but if you're using technology to help you do it, contact tracing also brings up serious issues of trust. How much do you need to know about your employees' private lives? What should you do with the data you collect? And will employees trust you not to misuse this information?

These issues have been top of mind for Kent Grayson, an associate professor at Kellogg and co-founder of The Trust Project. So he recently sat down with two people who work at the intersection of trust and technology. Heather Federman is the vice president of privacy and policy at data software company Big ID. Mathew Mytka is chief platform officer at >X, a design firm focused on improving trust through design. On this episode, the three of them walk through the pros and cons of contact tracing in the workplace, and what questions business leaders should be asking as they decide whether to institute a program of their own.

Grayson opens by posing a hypothetical to Mat. Heather comes in a few minutes later.

***

GRAYSON: Let's say I'm an employee at a medium sized company and my buddy Brad in marketing tests positive, and we know he's tested positive. And my organization has a contract, a contact tracing plan. It's not fancy, it's just a couple of people in charge of making it happen. So what will these people do when they find out about Brad in marketing?

Mathew MYTKA: Just step back and think about, like, without digital technology. It's a pretty laborious process. So the interviewing process to identify everyone that they've had contact with is pretty tedious.

GRAYSON: Right. I mean before we had tech contact, tracing has been used in previous epidemics. But this system depends on people's memories, right? That's the first. And the second is, it requires them to be honest. Because there are reasons, which we'll get into, why somebody might not want to say they were in touch with somebody at the company. And this is where technology can come in, in a perfect world, to help offset problems with memory and problems with honesty. And so, Mat, in an ideal scenario, how can technology help make contact tracing more effective? Let's just talk about the ideal.

MYTKA: Yeah. Look, in an ideal scenario, it would be as simple as the individual—Brad, in this case—let's say he was using an app on his phone. He was able to notify everyone that he was experiencing symptoms and people immediately got a notification on their phone that someone they've been in contact with—they don't know it's Brad—someone they'd been in contact with has been experiencing symptoms and has gone in to get tested.

GRAYSON: So that's perfect! And it does sound quite ideal. Everyone in the company has downloaded this app. They've complied because the company said they should, and everyone agrees, "Yes, that's a great idea." They're walking around with their phones in their pockets. And when he tests positive, the system automatically triggers. And then the app already knows who Brad's been in touch with because that's what the app is meant to do. It's meant to see if it's close to other phones, and automatically those who were close to Brad find out. And in some sense Brad's privacy is not negatively affected. Because it doesn't say, "You were in touch with so-and-so." And to the extent that the company isn't monitoring the system, everyone else's privacy is not violated, because they don't know who's been contacted as a result of having been in touch with Brad. But can we trust that the technology can even come close to that ideal, Mat?

MYTKA: Yeah. So I guess there are a couple of assumptions that you'd have to be making in this situation. The first one is that a large percentage, let's say 70 to 80% of the people, within this company are using this technology. So there's enough adoption for it to be effective. So Brad is using it and everyone else that he's had contact with during, let's say, the 14-day period, they're all using it. So that's the first assumption, is that people are using it. The second one is probably around the technology itself. Bluetooth doesn't factor in people touching surfaces. It doesn't factor in physical materials in between people like walls. So people might have been within 15 feet of Brad, but that was between a wall, or across the hall where there's a massive physical barrier. So there are two key assumptions there.

GRAYSON: Heather, I saw you were about to say something.

Heather FEDERMAN: Yeah. You know, I don't live in a world of ideals. I live in the world of, reality is basically some crazy version of dystopia. And you had said a key word when you were

posing this earlier about the sense of trust. You know, I think if we had had this conversation maybe several months ago, when we were in the beginning of trying to figure out what technologies we can use, if we had created a system that was trustworthy, things may have turned out differently. But because there's been such an embedded distrust of technology, the user adoption is likely going to be low. And Mat was pointing out some of the inefficiencies as well. So if you don't have the right amount of adoption, if you have all these inefficiencies built in, then what's the point? We might as well go back to manual contact tracing.

GRAYSON: Yeah, I think trust is so important. Trust in the employer. Trust in the company that's managing the technology. And then there's the trust in other employees that they're going to adopt and that they're going to carry their phones around. But my question is, the fact that we can get some false positives and false negatives—because, you know, we didn't catch you touching surfaces, or because you were between walls—even with those problems, isn't it better to have the apps augmenting memory and trying to offset lack of honesty? Even though it's imperfect, it adds an extra layer of information—flawed, but it's valuable information. It's a signal that is not completely noisy, that helps us to identify people who have been potentially infected.

FEDERMAN: I think it depends. Because to what extent are these, let's say, these apps, going to be tracking you? So let's say I'm at the office from nine to six. And I leave and I go to a gay club, or I go to visit my friend in prison. It's your personal life, but some of the choices that we make in our personal life can easily be misconstrued from an employer point of view. And there could be potential bias that is implicated within the job, up and to the point of discrimination.

So I'm not saying no to using technology. I'm just saying, we need to be really careful as to what are the limits that we're going to put in place here. Because, you know, let's say your direct manager within work, does not necessarily need to know your movements and your whereabouts at night. But perhaps you have a small group of dedicated professionals who, part of their job is just to make sure that when you fill out an attestation form saying, “I haven't been in contact with anyone with COVID.” And then let's say no one, you know, hopefully has gotten the virus, then after, let's say 30 days, you can dispose of that data. So those sorts of measures, when we put them in place, and we make the employee population aware of this, that creates trust with the employees to say, “Okay, I'm comfortable using something like this because I understand it's for it's for me to help protect me as well. And that my employers aren't going to abuse this.”

GRAYSON: So let's say I'm an employer. I want to keep open as much as possible, as long as possible. I want to keep my employees safe. I see the advantage of technology. What is your advice to an employer who legitimately wants to protect employee privacy, but also recognizes that by putting those protections in, I can increase the likelihood of compliance? One thing you mentioned is, I tell them that after 30 days we get rid of the data. Are there other ideas that you've seen, or ways in which employers can protect employee privacy and thereby increase compliance and adoption? But also protect employees from discrimination and all those other things?

FEDERMAN: Yeah. Depending on the sort of company—whether they have a privacy officer, who is the one who would be primarily responsible to think about these issues—have them involved early on in this process and be a partner. From my viewpoint, from their viewpoint, this is going to be basically like any other risk analysis that we would be doing. It just happens to be around COVID and contact tracing. What data are we collecting? How are we using it? For what purpose? So it's the same questions, I’d say, that any good privacy practitioner would be using for a given project or program, and just applying that in this situation.

GRAYSON: I think you both have had experience in working with companies and helping to establish these kinds of frameworks. In your respective experiences, are there some easy wins that some companies can accomplish? Let's say they haven't thought about privacy in this way before. And so when contact tracing comes up as a question, they don't know where to turn, they don't have any frameworks. Are there some easy stepping stones that, that people can start to walk across to get into a position where it's just a well-oiled machine and they know how to handle it?

FEDERMAN: You know, I think a lot of privacy practitioners, we might look to the Fair Information Practice Principles, which was created by the OECD, the Organisation for Economic Cooperation and Development back in the 1980s. And it essentially lists out eight various principles to keep in mind for any sort of data processing activity. And most risk assessments today are based off of these principles. And I'd say it comes down to: What are the notices? What are the disclosures in place? So are you being transparent about your data practices? And then it comes down to, well, what data are you actually collecting? And keeping in mind, is this the minimum amount of data necessary? Because, let's say for contact tracing purposes, you're only going to need a limited amount of data. You're going to need, perhaps some contact information, location information, and limited health information.

And then you get into questions of usage limitations—of, you know, are we making sure we're only using it for this specific purpose? And then retention—are we keeping this data for the limited amount of time that we need it? And then afterwards, are we deleting it? But I'd say at a very high level, starting just by asking these questions and then also thinking about, "Well, what's the benefit of doing something, versus what could be the risk of doing something when it comes to privacy?"

MYTKA: Practically speaking, we've just come out of a period of adaption to the GDPR world. So there's likely to be a lot of familiarity with these things and internal capabilities to deal with an internal privacy impact assessment, for instance. So in the absence of that—let's say it's an organization that doesn't have those capabilities—there's plenty of publicly available information to be able to reference on these things, particularly now. I think the Johns Hopkins Center for Health Security published a really great report on contact tracing, looking at a lot of things around civil liberties and some of the challenges that organizations, both public private institutions, are facing. So there are plenty of external resources as well without having to hire an expensive consultant.

[musical interlude]

GRAYSON: We've been talking about contact tracing within a company. But, as Heather pointed out, you know, people are going outside the company. And we have to start thinking about the effectiveness of contact tracing writ large. Entire regions or entire countries—trying to get them up to speed on contact tracing, why it's good, why technological solutions can be helpful with the right guardrails. As we think about, particularly, democratic countries trying to accomplish this, where authoritarian dictation is not a solution, how should people be thinking about contact tracing? Or let me put it another way: I sometimes think that if we can't mandate it, it's not even worth trying, because in many countries that have tried to get contact tracing up to speed, adoption has not been sufficiently high to make it worth the resources. Can you bring me a little bit out of my pessimism about this, or do you share my pessimistic view?

MYTKA: I mean, I'm definitely skeptical of this. I think the broader environment of distrust for public, private institutions, companies, governments, NGOs, whatever—trust is at an all-time low. So I'm super skeptical of whether even—let's start with the West Coast, in California. Let's say that they started building these apps. And the government was like, “Okay, we've got this government-sanctioned one for the state of California.” Even then there's a lot of distrust. You might say, “Okay, there's a larger percentage of tech-literate people in that region.” But getting to the point of the optimal adoption—you know, 75 to 80 percent of people using it—I think is just still a challenge. Because you need such a large portion of people adopting that technology for it to be effective. Otherwise it's just going to be ineffective.

GRAYSON: Well, okay. Well, one solution then, Heather, is that the government says, “Let's use the data that's available to us. Let's use cell phone tower data, let's use, you know, geolocation data that we're already collecting. Let's pass laws, and we'll do it democratically! We'll go out, we'll say, ‘Listen, people, we're not going to get adoption. Everybody knows this, but we need to stop this. We need to get some good contact tracing going. So let us pass laws that are temporary, and which allow us to get into some data that we haven't gotten before, but which will be a good proxy for contact tracing.’” What’s your perspective on that solution?

FEDERMAN: Yeah. I don't know how likely that's going to happen at this point. Because, like Mat really went into, there’s such a low amount of trust right now. And especially in the States. Here, everything's become so politicized. And if we can't even enforce mandate about masks—which are, let's say, the lowest form of technology there is to help prevent the spread of this virus—I'm not quite sure how you're going to convince people to download an app or give their data.

But what is happening from the data side is that we're now seeing a lot of third parties that were, prior to the pandemic, collecting data for other purposes—like location-based ad-tracking purposes—who had a bad rep before this, but now saying, “Okay, well, we're going to hand over to the government this sort of data to say, ‘We know people are converging in these parks and these arenas, and they're not really observing the guidelines around social distancing.’” So if we can't figure out user adoption, we can find ways around user adoption consent. But this ends up exacerbating the challenge of trust in technology and the government.

GRAYSON: Mhmm. Exacerbating it. But it's already so low, I can see people sort of saying, “Well, it helps us get to a solution where we can flatten the curve, because we can find out where people are congregating.” And I can imagine that people—I know that people are sort of saying, “If the cost is lower trust, at least people are safe.” And so I wonder, how should, let’s say, executives, as they’re thinking about their company—let’s bring it back to a company perspective—how should companies think about a tradeoff between, “Some privacy is going to be eroded. There may be guardrails, but we have to know where you are and we have to know where you're going. You have to trust us. We're not going to misuse it. And the purpose is to make you safe.” Or, “Listen, if your privacy is so precious that you don't even want us to get into your data, then the cost is that we may have to shut down our company sooner, maybe even tomorrow, because we are not tracking.” Is that a false tradeoff or is that exactly what the tradeoff is?

FEDERMAN: If we're thinking about the risk of some sort of data-driven or tech-based contact tracing initiative, or way to keep our employees safe in the workplace, then yes, there might be tradeoffs when it comes to, “We do respect your ability to have your own life outside of the work that you do. But for the sake of safety, there are certain things that we need to do.”

And going back to our earlier point, that's where it comes in to, working with the right team, the right experts, to make sure you're taking into account what is needed. And, God willing, this pandemic doesn't last forever. Are we going to then say when it's over, “Okay, we don't need to use this contact tracing technology anymore?” Because I think what my issue is, whether it's corporate or just in the ether of the world, is that it's going to become normalized to have this sort of tracking in place. And maybe we need it. I don't know. I don't really want to make an opinion on that yet because I don't know what the world is going to look like when this pandemic is over. But that is part of my concern—is that we're heading down this slide of normalized surveillance, and that's just going to become even more and more egregious as time goes on, where the pandemic and safety becomes a justification for that encroachment.

MYTKA: The big challenge with a lot of this is that you can't just do this as a company. There's no point adopting a technology for your company when it isn't related to what's happening external to your company. People, unless they're never leaving their house, or they're only coming into contact with people at your company, which is ludicrous. People go outside, they go on public transport. You know, so we can't think about this in isolation. That's one of the big challenges. It does require us to think about the interdependencies of us as people, us as organizations.

So business leaders need to probably just come to a position that “this needs to be done together.” If it's not done together, you're not going to get any effectiveness in using the technologies. It can't be done in isolation, which brings up consensus. And consensus with computers is easy compared to consensus with humans. So take the challenge.

GRAYSON: But I could see how a company might be more successful in getting adoption within their organization if they were to cooperation with, let's say, their three biggest competitors. You know, you work for a fast food company. You've always thought about the other folks as being, “We're always fighting against them.” But if the two or three biggest fast food companies could together say, “We're behind this,” I could see how that might encourage everyone to become more involved. And it might make the individual companies’ challenge a little bit easier.

FEDERMAN: You know, one potential avenue, then, is, a lot of companies typically belong to some sort of trade group organization. And I don't know if those trade groups are thinking about contact tracing and how they can do that. But a lot of practitioners are having discussions, at least on the privacy side. They are asking questions, “Well, what are you doing at your company and this company?” And they might all be in the same industry and technically belong to companies that are competitors. So I'm with you on this. You know, we are all in this together. My hope several months ago was that there would be a more uniform trustworthy system that we would be using. But unfortunately that's not the case. But I do—I'm with you on that we have to work together. Even if it's not at the government level, perhaps at the corporate, the inter-corporate level, we can do something.