Covid State of Play: Building a Public Sector Health Intelligence Capability

December 16, 2020

- Well, hello, I'm Jonathan Zittrain, along with the illustrious and brilliant physician and public health expert Margaret Bourdeaux, together we host from The Berkman Klein Center for Internet & Society at Harvard University, COVID State of Play, where we take up on an occasional basis, our own snapshot of what we're seeing and thinking about the state of the global pandemic, what ought to be done about it. And we often, as we do today, have an invited guest or two, to help lend an additional perspective on a given topic. And today's topic is around health intelligence, and I'll put it over to Margaret to introduce Tarah Wheeler.

- Thank you so much. Yeah, so, I am so excited to introduce Tarah Wheeler, who is a Harvard Belfer Cybersecurity Fellow this year, an International Security Fellow at New America, and 2021 US-UK Fulbright scholar in cybersecurity. So, what a mouthful! Tarah, I was actually gonna start off by just saying, do you remember when we first met the first conversation?

- Yes. Yeah go ahead.

- Yeah, well, it was a very striking day, because I think it was back in March or early April, when things were just starting off with this pandemic. And I talked to you because I think I was learning that you were gonna come to Belfer to be a fellow with me, and really, I hung up the phone and I was like, "That is the most interesting 60 minutes "I've spent in a very long time", sort of thinking about cyber security, and health, and health data. And whether the collection of health data, might be a problem, and might be a issue in terms of whether other countries, and countries that wanted to do the United States harm would be interested in attacking our data systems and our epidemiologic surveillance systems. And you had a lot of really provocative things to say about data and data systems, and whether they were secure, could be made secure. So, I hung up the phone with you, and then actually later that day, I was just confirming this as I was going back and looking at my calendar. I had one of the sort of saddest phone calls that I've had over the course of this pandemic and pandemic response. And it was from a friend of mine, who's a pediatrician in Chelsea, Massachusetts, who called to say, "Listen, Margaret, "I don't know that you're totally clued in here "about what's happening in Chelsea". Chelsea is a community, 80% immigrants, a large undocumented population, mostly Hispanic in origin and people, a lot of people working in the informal economy, a lot of service workers. And the other thing to know about Chelsea of course, was that rents had become very high, and so, a lot of people had been packing into a smaller and smaller living quarters. And she said, "What's happening is very... "COVID has really hit Chelsea very hard. She said, "I just got off the phone with the social worker "from the hospital, who was telling me about "two patients of mine, "two children who are in the hospital". I said, "Oh God, with, with COVID?" And she said, "No,

they don't have COVID, "but both of their parents were deported "in ICE raid six months ago, and so they were handed over "to a neighbor to be a caregiver, an elderly neighbor, "and the elderly neighbor just died of COVID. "And now these two children are, essentially an effectively, "orphaned and the community has nowhere to put them "except for in the hospital". And she was kind of going through how the community was mobilizing. There was a massive mobilization effort in Chelsea, by the community, really pulled together to try to help, the suffering that ensued from the pandemic. But really what I thought at the time after hanging up with her, I really thought this is how things were gonna go. I thought that the state of Massachusetts would sort of swarm into Chelsea with a lot of COVID tests, would go door to door and test people for the disease, and help people who were found positive to get the supports they needed to be in quarantine, or if they were sick, in isolation and get the medical care. And within a 48 hour window, 72 hour window, maybe at most, we would get our arms around the outbreak and Chelsea. And of course that was incredibly naive idea. And in fact, what happened was, no such testing was forthcoming. Even if the state had the capability to do that, the tests that they did expect folks to yeah, were really through their clinics, through their medical homes, their doctor's offices. And of course, many people in Chelsea either were uninsured or under-insured, didn't have a medical home, didn't have a clinic. Even if they went to the clinic at the time, the clinics didn't have the tests to give. And the groups that really did have the tests were at the hospitals and the hospitals were using them to admit people who were sick. So, even if they've gone to the hospitals, gotten a test, then the hospitals didn't necessarily report at that time. They didn't actually report that data to the public health departments. The public health department was struggling in that very moment to try to expand its reporting database of reportable diseases, and hospitals, the rules around what hospitals had reported in terms of testing results, was very limited, and lots of hospitals didn't bother or didn't want to report the negative tests they had done, for example. So, the state really had no real capability to collect data about who was infected, where they had gotten infected, and whether any measures that we were doing were working. And things have improved since that point, to some degree, but still, Massachusetts and the United States does not have that kind of capability, that kind of ability to see who has been impacted, the context in which they've been impacted, that has led them to be impacted by any health threat, and whether a public health intervention is working. And as I've kind of sitting here in the dark days of 2020, kind of reflecting over this year, I have reflected here right now, I would say, This is the best of times, it's the worst of times. This is the best of times because we really do see this vaccine coming, it's very exciting, but it's the worst of times, because we still don't really have a public health system or capability that can respond to this disease, in a way that limits the suffering from the fallout of things like lockdowns, and social distancing, and school closures, and things like that. And so, as I'm kind of looking out in 2021, I'm thinking a lot about this issue of how does this country and the world, have what I've sort of started to think of as public health intelligence, public health intelligence capability. That means the ability, again, to see who is being impacted, why they're being impacted, and what we're doing is working. And that seems to be a basic requirement of a functioning society in 2021. Because, I'm sorry but COVID is not gonna be the last pandemic. There are gonna be a lot of other epidemics, pandemics. There's also gonna be a lot of other health threats. We have an that could make all of our antibiotics ineffective, we have environmental hazards that are increasing in tempo and

devastation, we have pollution that is impacting communities in ways we don't even perceive, because we're not collecting the kind of public health data that we would need to be able to detect impact. So, there's a whole lot of issues here around how are we gonna collect data and how are we going to be able to make it useful? And that has really made me circle back to that conversation we had in March, because, you kind of put the fear of God in me about what can happen with data and how it can be misused. So, I find I'm in this very sort of rock and tight place moment, where I'm like, "Yep, I get it, it's really dangerous maybe, "but we can't move forward without a better data". And so, I'm stuck. And so, I'm so glad that you have come in to join us, because to maybe help me get unstuck or to say no, no, no, you're you really are stuck, and kind of how we're gonna proceed.

- That rock and a hard place is real. And I remember that phone call too, if I recall correctly, that was just very beginning of all of this. It was right in the middle of March. You were just starting to be called upon, and day by day, every global health expert in the world was just being slammed day by day. And I was so grateful to have that conversation with you. Because you're right, you're between a rock and a hard place. The problem is is that more people like you don't see that, don't see the rock and hard place, and that you're not going to choose one or the other. You have to steer a course between them. This is not an easy choice. This is figuring out the course between Scylla and Charybdis. We're trying to steer that middle course between not getting any data at all, and "Oh my God, what just happened to all that data?" And that's the challenge that we're facing. So, I'm gonna grump today, like a unixbird about security, about how we're handling it in this country. And that's because a lot of my morning has been on the solar winds hack actually. And about USG, the United States government dealing with how we handle data security in this country, and how we've been handling it. So, I'm gonna grump about it. But I want to recognize right at the moment that the fact that you were even about it at the time, means that you're someone who's seeing this problem holistically. The big issue with information security is that most people see only a part of it. I see, not only that, we need to figure out a way to protect people's data, but also, Margaret, I want you to win. I really need you to win because COVID is not gonna be the worst pandemic that we see in my lifetime. And I really need you out there. Cause I don't want to go get an MD. I want you to have the MD, and I want you to solve this problem. I'll help you with data.

- Thank God, thank God you're here to help.

- Well, here to help. Wanna live.

- I wonder... I appreciate Margaret and your introduction. I feel like you kind of managed to recapitulate all prior sessions of our webcast, which is great to have a kind of end of year summary, especially as it feels a little bit like maybe we're turning the corner, but you're speaking to really fundamental problems, and problems across the board. In this case, I guess we wanna focus a little bit on both the need for, and the dangers of building the kinds of databases we think you need for an infrastructure of so-called health intelligence. And for that Tarah, I wonder, in the public health context, is it helpful to distinguish between the kinds of data that decision-makers need and experts like Margaret need, for collective health decisions?

Where are their hotspots of COVID, and where should we rush resources or have differential application of public health measures that might not require such granular individual data, that if compromised would be a problem? So, that's on the one hand, and I also think a little bit, if we have a chance to speak to our colleagues, Cynthia Dwork and others who have invented differential privacy, as a way of making databases that can be queried for statistical epidemiological purposes, but even if breached don't compromise reliably individual data. And on the other hand, it sounds like there might also be a need, maybe under the rubric of health intelligence, to actually know what individual needs and problems are, at which point you don't want aggregate data. You need to know exactly who has COVID so you can help them, which makes it a little more tight between Scylla and Charybdis on how to secure that kind of stuff.

- I think it's a great question to ask ourselves how much data do you really need? And the answer is, as someone who is not a physician, but someone who has expertise in statistics expected utility and securing data, I know what I can give global health experts, that is unlikely to cause a breach. And at the same time, I think we're not being on enough to do that kind of work. Global health experts were getting called on instantly in the beginning of the pandemic to start working on the health implications of what was happening. I think this next year, kind of my prediction for 2021, is gonna be a mop-up job for a lot of information security specialists dealing with the cleaning up of the data that was collected in individual locations, that it was never audited, it was never secured properly. And we're gonna see a massive increase in the amount of interest in information security in health practices. That does not mean we don't need to create and provide the access to the kind of data that Margaret and other global health specialists need. Because, again, this problem isn't going to go away. The problem of needing access to collective amounts of patient data that is anonymized in some way, isn't going to go away, It's just gonna become more important. And yet I'm not honestly seeing the technical solutions getting implemented right at the moment or any call for it.

- Let me just sharpen that a little bit. Is it your view that in 2020, there are sometimes elusive things called best practices, and magically those building databases, having custody of them, securing the networks and everything, were to adhere to best practices, a big if, but if they were, we'd more or less be an okay shape, or do you think that the problem runs deeper than even if everything were done right, it's more or less than inevitability that you're gonna end up with data breaches and we have to account for that?

- It is an absolute inevitability. The data breaches are gonna occur at the highest levels. That does not mean we do not need to abide by best practices. And it certainly doesn't mean that we need to blame the people who have become victims of these data breaches. What it means is that we have to start understanding that systems that operate on a computer and store human data, are as flawed as the humans who created them, and secured them, and set the rules for their access. Health and patient data security is national security at this point. And the reason I say that is because, it only takes one time of losing a large database of health records in order to permanently compromise the people who experienced victimization in that data breach. Does that mean we need to not engage in best practices? Absolutely not. What we need to start doing is recognizing not only differential... I love the differential privacy example

that you gave. The capacity to query statistically for data that helps decision makers. And at the same time, we have to recognize that it's not a single step process, either you fully anonymized someone's data and it's safe for all time, or you don't bother to do anything about it, and you just try to keep it in one big bucket someplace, and put lots of locks and chains around it, and the Fort Knox of data. What I think we're going to start seeing, is that those best practices are going to involve a series of gates with a series of anonymizations, where it is respectively harder and harder to walk back towards the individual patient's data in order to identify that person. Of course, more authorization, more qualifications, more permissions from the patient. And yet at the other end of that, the data that is most accessible to the most number of global health specialists, to the institutions that need it, that you're going to see a greater degree of anonymization. It's not one or nothing when it comes to securing a big database like that. You can add multiple gates, you can add security by design, and without any doubt, we do need to have that access to that data. But I am seeing people giving up on the concept of best practices out of just the sense of utility.

- Yeah, it's funny that... My asking if best practices were sufficient, can so easily, cause it's out there, end up a question about whether they're even necessary. And I meant them more as the sufficient question, but maybe another way of rephrasing it is, let's suppose you've got a generally enlightened, well-meaning, and decently resource state policymaker, trying to do the kind of stuff that Margaret rues wasn't done in the early days of the pandemic and may not even be done now, with Massachusetts as the example. Is securing whatever someone like Margaret would recommend for data about people and their health, and the transmission of the virus, is securing it the kind of thing that a policymaker can do by writing a large enough check to some technology consultants or advisors or something. The kind of way that's like, I'm trying to build a building. I really need it. Now I'm gonna house people in it. I just need to make sure it won't fall over. There are people that can do that, or is it more somehow profound and fundamental to the process of assembling that data? Is there something more that those top policy makers would have to be bearing in mind to do it right?

- I think in the beginning of the pandemic, we saw an awful lot of blow up tents with camp cots in them to house victims of COVID is what I think. And I think that people were forgiving of the fact that we needed to create and deal with emergency measures in that moment. I think over time, it's not acceptable to simply write a check and hope that a third party vendor can rapidly solve a problem. You need the defense in depth of people who actually understand how to implement information security and in depth to secure the kind of patient data that you're talking about. Is it enough for a policy maker to just write a big enough check to secure this data? No, it is not. And it's because no one person, no one organization, certainly no one third party vendor, can solve this problem completely. When I say defense in depth, I don't just mean that we are putting enough gates around one source of information. I also mean that the kinds of best practices that you've mentioned, are something that every individual person in the chain of ownership needs to take ownership of. I spent a lot of time this morning explaining the solar winds hack to people. And I explained it, I don't know how adept you want me to go into this, but there's a trust element there. I think on the part of people in this country and around the world, when it comes to government securing data. And I think that one of the problems

we have is that we don't understand the difference between an organization or agency getting hacked, and where the flaw in the security actually was lying. The solar winds hack this morning, for those of you that are kind of tuned into this, what happened basically was that, what is speculated right now to be a Russian nation state attack versus us government agencies and information storing systems, occurred through breaching a third-party vendor, Solar winds, it's an it infrastructure provider, the kind of company that Jonathan is talking about right now about writing a big enough check to. That company had a breached software update process, where people downloading updates of their software were also downloading a backdoor into the systems that they were installing it on.

- Which has a certain irony that they were trying--

- Exactly.

- To do it right and stay updated and patched, and the very patch was the problem.

- This has a very good analogy to a vaccine. Just because there's gonna be one or two people that have a bad reaction to a vaccine, does not mean that we do not need to mass vaccinate. This is that moment where we see that there's a couple of flaws in the system, and statistically speaking, you cannot have a perfect 100%, a working vaccine that has zero side effects. I'm sure Margaret can tell you more about this, but what I'm telling you is that this is the equivalent in that moment of something like a vaccine. You still need to have everybody doing the right thing in that moment, just because one or two people, statistically are gonna have a bad reaction to it, just because several of the agencies that were part of the 300,000 customers of this third-party vendor were breached as a result of trying to do the right thing, doesn't mean we shouldn't also still do the right and secure thing. I actually, this is one of those moments where we have this great analogy between me and Margaret's work. This is like a vaccine. You still have to do it. Yeah, there are gonna be some bad side effects, and there is no such thing as perfection here, only trying to do it better, more, over time.

- I mean, that's really an interesting analogy to emphasize that you wouldn't want people to take the lesson from this. It's like, "Well, that's it, no more patches for me, "I'm going with the tried and true vulnerabilities "rather than the unknown new ones". And that's important lesson. Of course it might be a disanalogy that the vulnerability is to everybody who is staying patched. It's not a kind of idiosyncratic one-off reaction. It's that the election of the adversary, as they say, as to who will pay the price for the vulnerability, but this kind of gets to your... If not inevitable, you can try to lock every door and engage in every best practice, and at some point you're still gonna have a problem. Is there anything, if on the lists of hackys were to be the hypothetical custodians of, again, the kind of data Margaret would love to see gathered for the purposes of public health? Is there anything they could be doing to better... I know it's almost like there's gonna be a flaming tree falling on your house. Is there a way to waterproof it or something? I don't know what metaphor I'm looking for here, but what would we do if we were trying to wisely anticipate moments like these?

- This is a law of big numbers situation. You don't prepare for your house to get hit by a flaming tree. Statistically speaking, 10, 15, people are gonna have a flaming tree fall on their house this year. What I prepare for, is making sure that the lights are turned off when I leave, that the doors are locked, that I've got proper cameras around the place, because I am maximizing for a general, low level of threat and keeping my day to day as safe as possible, while recognizing that a tree could literally fall on my house at any moment. In fact, two years ago, a big branch from a tree near our house did in fact fall in the middle of the night, in the middle of a cold snap, woke me and my husband out of a dead sleep. "What the hell was that?" The there's a smashing sound. And here's what I'm here to tell you. I didn't take out an insurance policy the next day for, "Oh crap. A branch fell on my house", because it happened to my neighbor. What I did was I kept locking the doors. I kept not leaving the stove on when I walked out of the house. I mean, mostly I don't leave the stove on when I walk out of the house. I don't mostly leave the house right now, but the idea is that we've got to prepare and stay safe for the threats that are real every day. I want people updating because I want people thinking about heart disease, and cancer, and high blood pressure, to again, live over in Margaret's world on this one. We're not talking about dengue fever in the middle of Illinois. We're talking about something that everybody has to worry about. Statistically speaking, I'm still not gonna die of COVID. So, I still do pushups every day. I want people thinking about the general level of health that they've got to deal with. And that is the best practice every day. It is not fun to do pushups. And you know what? I don't like broccoli deal with that. I'm just not a fan. I don't like spinach and kale, Oh, but I'll eat apples. I'm good with tofu. I will make the best choices I can with my health. And that's what I want people thinking about with security.

- So, maybe Margaret, it makes sense to go back to you, if it's fair to ask, like what would the ingredients, either hypothetically, or from what we know from other places that appear to have things a little more together, what are the ingredients of a public health intelligence apparatus? What are the moving parts that you'd want people to know about?

- So, yeah, so, two things I think are helpful to kind of preface what I'll say. The first is, over our time together, JZ, I think one of the trends that we've seen is that when data is collected, really, there's an emphasis on trying to collect as little as possible, with the hope of preserving privacy. And I think one of the really unpleasant things to realize is that in every case, that was basically a mistake. So, the Apple, Google game framework around digital contact tracing, they took out the most important piece, which was the location of where people were. So--

- With great pride. I mean, that's to this day is trumpeted as yeah.

- Exactly, exactly. We really needed to understand the environments in which transmission was happening, and we needed to work with people to understand, whether the quality of the risk that they had, that they had actually been exposed, that you just simply couldn't capture with that kind of an approach. I think the second example is from a mistake we've made in the contact tracing program, where we kept saying to people, "Oh yeah, every time you talk to somebody who's infected, "they're gonna want to tell you all about "where they think they got it. "Ignore that, cut them off there, "just have them focus on telling you "who they've been in

contact with since they've had symptoms "or a couple of days before they had symptoms", when actually that, we were telling them to ignore the most important thing, which was where people think they got it from. And once we started investigating that, we started being able to do cluster analysis. And that meant we started to understand, "Oh, it's the locker room of the hockey rink "that is causing the transmission, not on the hockey rink".

- What was the well-intentioned motive behind "Don't let people say where they think it was", was it that would get it wrong? was it that as long as you write down everything, it's probably in there somewhere, what was going on?

- No, it was because we didn't think we needed health intelligence. We thought, okay, we're in the here now, all we're gonna do is use contact tracing to try to stop the propagation of that particular line of transmission, not use it as a way of understanding and characterizing where, and the context in which people are getting sick. And we didn't wanna do it because that was also, we knew it'd be dicey. We knew that it would be dicey because somebody would say, "Oh, I got it at the illegal club that's still running", or, "I got it at that wedding"--

- Or, "The protest".

- Or, "The protest". Or, "by the way, I was whatever, doing a drug deal "with somebody and I've I've exposed them", or whatever it was. And so, the more information though, that we got, the more personal, granular information about where people had been and who they had been with, the more valuable it was from a public health perspective. And so, I think that that's one tension that I've sort of seen out before. The other thing I think is really important to communicate, to cyber people and people outside of the health system, in fact, it's important to communicate to doctors is that, in this country, there is a stovepipe separation between our medical care system and our public health system. And the medical care system is where the, "Well, that's your doctor, your clinics, your hospitals", your public health system is a totally different system that is orchestrated as a public sector function. It's orchestrated at the local and state level, and it is resource poor, it has been stripped of resources, et cetera, and its connection to the medical care system is very tenuous. There's only a couple of, only a couple of connections. So, like one of the connections people might be familiar with is a newborn screen. If you have a baby, they take a little bit of blood from the heel and they put all paper piece of paper, and then they send it to the public health department from the medical care hospital. So, that's like one example of a program where, that information is given to public health system.

- And what is that used for?

- Yeah, so they are using that to detect genetic conditions that have a medical illnesses. And so, the public health department then runs the analysis says, "Oh, that child, can't eat certain foods "or else they'll have permanent brain damage". And then they go out and they call the doctor, and the doctor goes and tells the parent. For whatever reason, we've housed that in the public health domain. But you could imagine that that's a program that just would be run through

every hospital, they wouldn't necessarily need a public health lab to do that test, but those tests are sort of specific, and they're not something that every hospital lab would love to sort of specialize in. So, that's kind of a marriage of convenience connection. There are others. So, there are a set of diseases that have always been sort of tracked, and diseases with communicable potential, the plague, measles. These are things that if your hospital tests you for, if they can't rule it out, then they send it to the public health laboratory. And so, that's the other sort of connection. But most day-to-day doctors working in a hospital, they don't know anything about the public health department. They don't know who's in charge of the public health department, they don't know who's in charge of the public health lab. And that matters because the public health,, the sort of where the... I think the education around data security is much more sophisticated in the medical care side and not as much sophisticated on the public health side, So, you had some education around hospitals are very much worried about being hacked, and medical data being stolen, but the public health folks, are maybe not as attuned to what could happen. Now, part of that is because their information systems are very primitive. Most of our public health system is being run off of a fax machine. Countries like Afghanistan, if they're worried they didn't have anywhere to bomb, well, enemies don't have a lot of targets in the United States. And so, that's one thing that's maybe saving us from big epidemiologic surveillance.

- I see how like the physical filing cabinet is both secure in a digital kind of way, and extremely limited in a digital kind of way. So, I'm wondering is the picture you're painting, that we're then gonna ask Tarah to take a look at, and tell us where its vulnerabilities are. Is the picture you're painting, one of... There's a lot of tributaries of information that might kind of come out of the medical standard healthcare system? Hospitals, urgent care centers, apps, Google queries, who knows what. Tributaries that go into a river that feeds into, now, I'm gonna Hollywoodize it, some kind of public health fusion center, with crisply uniformed people looking at massive screens that have dots appear where like, "all right, we got another COVID in sector 12, four G", or whatever it is, and then they can snap too, but you don't need that many people in that fusion center, and they can just issue the orders and say, "All right, I need you to go do something stat". Is that the kind of vision you're painting for which then you need a sort of Fort Knox where the data lives, but you don't need a ton of people legitimately getting access to it all the time, Just kind of the public health whizzes who can deal with it?

- Yeah. So, I do think it is, in my mind's eye, there is some system where people come into their clinical home, their medical home, and they get a test for COVID and that positive test is funneled into, across the divide, across the medical system, into the department of public health, that is collecting all the positive cases, and then information about that patient is accompanied with that positive result, including where they might've gone, et cetera, et cetera. The public health folks take it, they analyze it, they anonymize it as much as they can, and compile it to try to understand how effective it is, and then vice versa. That the public health system is able to take information about emerging threats or environmental conditions that should impact patient care, and funnel that into the doctor's office, so that the doctor can say, "Oh, I see that you're living in an area "where there might be higher levels of lead in your water, "let me try to test your test you for lead". And so, I think that that's the kind of feedback loop

that I think would be really helpful, and in times of crisis, critical, but I'm just not convinced that... I just don't know how to do that. I'm not exactly sure what the ramifications would be. I mean, people are already reporting very sensitive things to contact tracers at public health departments that are collecting very sensitive data. So, that is already happening to some degree. And this would mean more of that, and maybe so much more of it that would become a much more valuable target for exploitation.

- Yeah. So, Tarah, given the picture that Margaret's painting, and the kind of desiderata of what would make for useful stuff for the public health system to know, I don't know, kind of, sort of threat surface or attack surface, do you see that makes it different, if at all, from all sorts of government databases that have sensitive data about who's collecting benefits, or tax returns, or you name it?

- The end state of all patient data is either that it is eventually deleted or tried it away over time, as patient data ages out, or hospitals go under, or records get deleted, or it becomes fully public and is in the hands of our enemies. That is the end state of every single piece of customer data, patient data. You can tell what I've been talking about this morning, Customer data, patient data, it doesn't matter who it is. The end state of all data at all, is either gone completely, or in the hands of somebody you don't want it in. And when it becomes sensitive data like health data, it becomes even more important to realize that is the end of all of the data that we're collecting here. The best case scenario is that we expire the data that Margaret's looking for in terms of individual personal access to it, as fast as possible--

- Sounds like we might be able to, just on that one point, probably thread that needle. I mean, we could have basically crisis duration access for a lot of the granular staff, and the rest can be duly aggregated, but it sounds like a lot of this is about acute response rather than sort of, "I need to keep 50 years worth of somebody's tax returns", If I'm the IRS.

- This might be the way that we steer through this course, because like I said, I want to see a robust public health response, with the information you need and not one bite more, for any upcoming health emergencies. And the best scenario that we have is an active response, that deletes data as fast as it is humanly feasible. The reason we wanna do that is because we know that collecting data over time leads to either its storage, use, and sale, or it's released into the wild unintentionally. If we were gonna steer a course here, and I'm speculating, honestly, because I've not seen this done very well by very many people. If we're gonna do this, the data needs to expire faster than most people would think reasonable. The reason for that, let me just, so first of all, right now, I know of somebody, and I'm furious about this, I know of somebody who received information that someone who was around people, that they were around tested positive for COVID, and very likely tested positive for COVID and got the results back days after they were tested. And also while they were waiting for results, was around people that the person I know was around. I'm furious. I said, "I know a lady that I want to call right now "and tell her all about this at a very angry, "her name is Margaret, and I want a public health response "to this immediately", and there's no one to call. That's the thing I think that we're trying to solve here. There's no one to call, because there's not this conflux of trust in a

system, and expert access to that system and that data, in a way that lets us get a robust response, while at the same time protecting individual rights. And the reason in this moment that I don't... I don't want to protect individual rights in this moment. I wanna know the names of all the parties responsible for the situation and that my friend who was at second degree exposed to COVID, very likely knowingly by the second degree person who tested positive. I wanna call the law. And believe me, I really what I call the law. I'm a security researcher we have a tenuous relationship with people who enforce the computer fraud and abuse act at best. But the idea that we can find a way between this, very likely looks like affirmative deletion of data, confirmation that we've gotten rid of personal information as fast as possible. I think that might be the only way we can go about this. And I cannot believe I am saying this, and somebody on the internet is gonna get so mad about this. This might be one of the very few reasonable uses of blockchain I've ever heard of. I mean, blockchain is terrible. It's not magic pixie cyber dust people. But, there's a reason to use it in cases where you want to, in a distributed fashion, affirm that an action was taken at a given point in time and place. And that right there might involve the confirmed deletion of medical records, not the records themselves. Oh God, no. But there might be a reason here in a way that we can use some of the more interesting disruptive technologies we've developed to really help the situation. And I'd love to see that happen.

- What blockchain would be doing there, that's different from the relevant organization, putting a certificate on their website of pain of perjury, "We deleted the data:, they're both just assertion.

- Oh it's different. No, no, no, no. See that's the difference. There's a fundamental technical difference there, and it's a mathematical one. Anybody, this is a question of kind of under penalty of perjury. Well, the reason we have penalties for perjury is cause people do that shit. I've been in information security and I've seen a lot of fraud, a lot of problems, a lot of people attesting to things they shouldn't be attesting to. I haven't seen in a distributed system like this, in contracts and ledgers, I haven't seen without some pretty sophisticated technical attacks, a way to fake whether or not a contract was or wasn't signed at a given point in time. That's something you're gonna get. I think you might actually have some more technical leaders behind that, possibly. Because, even like me, who thinks this is a bad idea, but we're gonna have to do it anyway.

- Yeah, I guess I'll have more reading to do. I find myself completely confused by this branch of our conversation, because, put something on the blockchain, all you're doing is saying that you have a private key that hopefully hasn't itself been compromised, that lets you flip some bits on the chain, which is the same as flipping some bits on your website. And I don't know if you're worried that somebody would hijack the website and say something wrong. I don't know, we're about to now get into like--

- We wondered too far.

- The electoral college vote and why the electoral vote should be recorded on the blockchain rather than sent by certified registered mail as they are--

- I want to keep having that conversation, but not now.

- But one thing coming loud and clear from this, and absolutely let's have that conversation, 'cause I am yet to be persuaded that that's a good use of blockchain--

- Oh lord, I'm not either.

- But expiration is a clear clarion call, and that's a great anchoring point that people might not have in mind. They're just like, "Build it "and we'll deal with data expiration later". But being able to build that in from the start, seems like a great idea. Are there commensurate sort of complimentary things that you would say, of similar sort of gravity, that you'd want to put alongside expiration, as principles for kind of building the kind of medical system, as one of the questions in the question and answer queue is saying. If you could build this thing from scratch, what would the framework look like? Are there things alongside expiration?

- So, I think exploration is a great idea. I mean, cause I think... I don't think that collecting less data is actually is a good idea because we need that data, at least in the short term to really make progress. I think this data will just deconstruct five minutes or something. It is a very interesting idea, and certainly wanna use some research. I think the thing that I get a lot, I have to say, a lot of folks that I get into conversations with about data security in health, and particularly health crises, have kind of one of two reactions, it's kind of schizophrenic, and maybe it's a very American thing. On one hand folks are like, "Oh my gosh, I am not sharing anything with this government "that's gonna come and arrest me in the middle of the night "and do bad things to me. "There's not one thing, I am very privacy oriented". And then on the other hand is the opposite reaction, which is, "Who cares if the Russians hacked my data?" "Who cares if China knows what my mammogram said, "I'm just not that interesting." Or, "Who cares if they know I have COVID", or whatever. So, the sort of--

- Yeah, that's a way of asking Tarah, like what's the... All right, let's say an adversary, and it's not any adversary, It's gotta be one with sufficient resources. So, it is like the government of a major nation state that's into this stuff say, what would we see them doing, that would be the most worrisome to us?

- We have seen this information used for blackmail purposes, for deep fake purposes, for the ability to recreate someone and their consent or identity without their knowledge of it. One of the things I've seen, and I think Margaret probably have seen a lot of this as well too during the pandemic. I have seen, from the very beginning that schools started to go online, I started to see parents having to sign their kids in every couple of minutes to online learning systems. About halfway through the pandemic, that flipped in every kid I know, now has all their parent's passwords. 'Cause every parent was like, "I can't handle this anymore". Kids starting to sign in instead. And so, what we're starting to see, I think--

- They're just a vector.

- They are absolutely both the vector and the attack surface. But the concept here for identity and access management is that we're starting to see identity is something that you own and operate, instead of something that you are. And when someone can grab a piece of that identity and attest to it with things like valid medical records, social security information, financial information, combine the OPM leak, with the Equifax leak, with a health care leak, with the recent solar winds leak, combined all those things, and you've got a real convincing government employee on paper. That's what we see. And it's a combination. Instead of attrition over time of that data, we see this accumulation, this creation of data that starts to make it more feasible, that you can attest to owning and operating properly, someone else's identity. That's a thing that only gets worse over time. It doesn't get better because of the way biometrics work, the way we conceive of computer security right now. I can't change my face. I mean I can, but it's expensive and I don't want to, I like it. I can't change my fingerprints, I can't change a great deal of the things that physically make me me, and yet using those things to identify me, and having a digital record of them that are taken, makes it incredibly problematic for me to prove I me, instead of someone else who has all the same records. So, that's the concern, I think you see many people having with this. The more sensitive the person, the more important the person, the more that's a weapon. And those are being conceived of as weapons in a new kind of way. We call it disinformation now, we don't call it propaganda, we call it disinformation, 'cause you can get a lot more grant money right off studying this information than you can propaganda, but these are all ways of attacking people's conception of the world. And that's what we see happening. And I think people are already distrustful enough, that the state of the world that is being represented to them is actually reality right now. We're having a big conversation in this country about whether or not what we see is what's actually happening. And I'm here to tell you that everybody watching any individual news channel is deeply convinced that they know the truth, and people watching a different media outlet aren't. That's incredibly problematic, not only for the kinds of health responses we need to see, the kind of fear that Margaret was talking about, like what do I do when the government gets all my data and never gets rid of it? Am I gonna even be helped by this or the opposite side of it? Why should I care if somebody has my information? I think that becomes a different question. Why should I care if someone has my data becomes a different question in five years, when you find out you can't get a job because your credit's wrecked, because your medical history has been exported elsewhere, and you're no longer able to qualify for a security clearance. There's a longer term game happening here with the collection and storing and creation of human beings in their identities. And that's what's happening. But at the same time, it makes it more problematic to be sure that what you're seeing in micro ads on Facebook and Twitter and wherever, are really what's happening, it could be just targeted to you to change your state of the world.

- It stands to reason, I would imagine, even like, let's just take this current example, if we wanted to have people quarantine for 14 days, now it's now to 10, can you just hack the exposure notification of system of Massachusetts, and say, "You've been exposed, "where

we're expecting you to go, "not go show up for work for 10 days, "and if you don't comply, then you're fined $500 a day". Right now we've taken such a very loosey goosey kind of approach to the intervention that people are not, really in forced into quarantine, things like that. But those things, they maybe coming down the line here, and also with worse diseases that we are more scared of, like, I dunno, Ebola or flu that kills you in three days or two days, kills children, et cetera. You can imagine that spoiling of data, combined with the seriousness and the power of public health law should it be used, might be a really bad thing. I can sort of start to imagine something like that now. I think, it's less likely, like I said, because we just don't have the systems in place to be able to do that, to be able to be attacked in that way. But that does give me pause as I sort of spin out a vision of what would be the ideal public health intelligence kind of capability, and what it would look like.

- And kind of the way in which I hear Tarah saying that you can end up with a whole greater than the sum of the parts in a bad way for compromise of personal identity, that any given fragment that's compromised may not be such a big deal, but if it's becoming part of, sort of the gray market dossier, that's not so hot. And that there's kind of a one-way ratchet that is more and more as compromised. That's kind of what I'm taking from what Tarah is saying. I realized as we're rounding the full hour, we didn't open with our tradition of sort of the snapshot of a word or three as you described the state of the pandemic right now. And I think Margaret, since we last convened, the vaccines have been approved. That had not happened when we were last talking I think. And so, my recollection is that usually, the assessments range from the horrible to the dire. Can I just ask what your, some of the state of play would be right now?

- Yeah, I mean, I guess I gotta take the liberty of having two thoughts. So, the first is the phrase, "It was the best of times, It was the worst of times". It seems to be how I would describe things. I do think the vaccine is incredible. And I sort of am sad that we had to prove our scientific innovation prowess this way, because, the worst of times, where so many people are dying per day in the United States, and basically we have completely run a mock, as we come to the end of this year, this is the other kind of reflection I shared with some friends in the other show that I do on question on quarantine, is that, come to the end of the year, we're facing a year that I think will be more hopeful, but there's a need, I think, to really pause and say that we failed, like to admit failure is a very important part of being able to do better in the future. And I was saying, I love the movie "Moneyball", and there's a scene in it where the coach, Billy Bean, storms into the locker room after his team is lost, and they're all, listening to music and kind of partying, and he picks a baseball battery smashes the radio and says in waits 10 seconds. And he's like, "This is what losing sounds like". And I do think at the bottom of the year, here in this dark winter, I think we need to say like, "This is what losing looks like", 300,000 dead and a public health response that is simply inadequate and unable to really underwrite our security in the future. But anyway, yes, I am more hopeful. I mean, the light is there. It is a dark tunnel, but there is a light. And it's an incredible one, a really incredible achievement these vaccines.

- Got it. And Tarah, your sensibility?

- My sensibility is that I'm tired of with people to stay in their houses and that the vaccines are arriving fast. And yet the level of disinformation that's occurred over the course of this year , has created so much fatigue in people, that I don't know how fast could have been fast enough. I think that there is absolutely no doubt that the faster we get people vaccinated, the faster we're gonna be able to get a handle on this. I think we're gonna see some incredible clashes between people who... We're in a privileged bubble in this conversation. I don't know how many people I talk to on an everyday basis understand that there is fundamentally nearly half of this country right now that doesn't believe anything we're saying, isn't wearing a mask, and are going into hospital still swearing COVID isn't real. That's a problem I don't know if we know how to solve, but I know that telling the truth as much as possible, as fast as possible, as competently and simply as possible, is what I think we're all trying to do here, and the more people we have doing that, engaging in that practice the better. So, if you are somebody out there who knows how to turn technology into a metaphor, if you know how to explain that the operating system that you're running right now, how it's like a solar calculator, if you know how to explain that something's like cooking, If you know how to explain anything in technology to someone and make them understand the reality and the truth of it, we need you right now in this moment. Tell the truth as much as you can, as simply and clearly as you can. And tell people not just what this is, because we know what it is, but what it's like and what it's gonna do. That's I think where I find myself on the pandemic. Also filled with rage, genuinely and honestly. We've been making these sacrifices all year long, and I see so many people that don't. And our holiday season is going to be darker and bleaker because of the sacrifices we have been making this long. And yet next year, I think it's gonna be a lot brighter. We're gonna have to let some of that anger go. I think, hang on. I'm just gonna squeeze it a squishy ball here at my desk for a while. But I think that sense of frustration and anger can be turned into something brighter next year, and I'd love to see that.

- Well, thank you. And for what it's worth, I know among the pollers of public sentiment, the pollsters, they are gonna be really interested it seems, to find out how much of represented hesitation about vaccines translates to actual hesitation about vaccines. Whether it's a snapshot of a moment now, totally bound up in partisan declaration and advertisement of feelings on either side, whether it's, "I don't trust a vaccine that came about "under the current administration", or, "I'm on team 'don't take it seriously' "because that's part of what America means to me", that if it's that sort of thing, it actually may not run so deep, once there's something available at the local Walgreens. But we'll find out, I mean, this is gonna be running the experiment right now to see how it's gonna work out. And of course, Margaret has a lot to say, perhaps in the next episode, on vaccine distribution and allocation, with its own issue and set of trade offs. And I confess Margaret, I wonder if all of the highly refined, "Here's the ladder of people who will get it at what time", it's gonna be like, "It came off the truck, it's use it or lose it, "pull out, anybody who wants to get in the lifeboat, "get in the lifeboat".

- We have a lot to talk about there, and I would say this as well, just to close it out. I mean, people in the United States have not reacted that differently than people in any epidemic I've ever studied or been part of, and it's almost hilarious how on script we are, and the concerns, and the disbelief, and the da da da da da, that's all very normal. And I have a lot more faith that

people are gonna come around, with consistent messaging, and all the nudges, and all the incentives. And then there are those that do not. And I will say one thing my dad always said to me, he said, "It's the person you can't reach", he was a teacher. He was talking about the kid you can't teach, "For the kid you can't teach "is actually the person that reaffirms humanity". Because if you can teach every child, then people would no longer be human. There'd be completely, just manipulatable of automatons that you could know what buttons to push and leavers to pull and that would be that. So, there always will be a reserve of people who don't wanna play by the rules, or don't want to do it, and I try to lessen my anger by thinking those are the people that are affirming humanity.

- It sounds like you're writing the script for an Apple commercial circa 2012. "Here's to the crazy ones".

- Oh.

- Indeed. Well, it's at least as good to know that there appears to be a kind of third act, and then an end to this particular program, as it were, not just COVID state of play, but COVID itself, and possibly even heartening to know that in the debates or what passed for them in Washington DC, say about relief during this, that now it's truly about stop-gap, and we see an end point ahead for which, "All right, let's just get ourselves there", rather than we are in an indefinite situation, and are we just gonna keep releasing money. And that's where we're on the cusp of maybe something getting past there. Tarah, thank you so much for joining us today. It's really great. Thank you for sharing your knowledge and your rage, and Margaret, a pleasure as always, even the bleakness of the topic, and of the reality of what this pandemic has meant for so many people.

- Thank you so much.

- It's been a real honor. Thank you so very much glad to be here with you guys.

- Indeed. And we will catch you for the next episode.

- Bye bye.

- Cheers.