MapCamp 2021 - Securing our Future

Okay. Hi everyone. Uh, good morning, uh, from London. Um, I know some of you are calling in from the U S and other parts of the world. Uh, and I know one of my coach after he is in Phoenix, so it's a bit, uh, For her, um, she'll be up the whole night, basically. Um, so welcome to this, uh, session, uh, which is called secret, securing the future.

And I'm glad to have, uh, Roz, Sarah and, um, Simon with me. Um, and then not going to take too much time away from them, uh, because we have a lot of interesting docs coming your way. Um, so I guess we're just going to get started. Uh, I'm going to not going to introduce, uh, uh, them because they will be to distance themselves from their thoughts.

Um, so over to you, uh, folks wonderful, sorry, zero ranch to sell Salesforce, or just introduce us having to go straight into the presentation. Yeah. Just, just make it part of your presentation. Of course. Uh, good morning. All. Let me get my, um, let me get my slides up. Just to bring income, um, that, that is coming across that range.

Uh, yes. Um, my slides clear, wonderful, good morning or a one on all a where it's always going to be a tough one to follow Simon directly. Um, I'm the other Simon the much less important one. Um, so good morning. I'm Simon Clifford. Um, I have been working in public protection in policing, particularly, uh, over the last, uh, five years, uh, and, and thusly.

Quite a lot of my focus is going to be biasing around that. Um, I hope people find this session, uh, really interesting. Uh, I've been working with, uh, rose and Sarah in terms of pulling together. Uh, a unified presentation that talks to the same area of activity, uh, underpinning, securing our future. Uh, but with some practical applications around that, and particularly when we're talking to the use case of, uh, video and AI, which I know I've been looking at extensively in the last couple of years and on speaking to others in, in every sector, private public, uh, and the third sector kind of there's intense activity around this, across the piece.

So we're going to describe this. Um, I've got the, uh, opener to try and describe how this would look from a strategic perspective, which is kind of my core area, uh, that C suite conversation as to the why's and the wherefores of all this. And, and certainly from my perspective, how mapping has been so helpful, uh, in my role and roles, um, working in, uh, in public protection, law enforcement, cetera, Um, but equally that will be passed on passing the Baton on to, to Roslyn Sarah, who we'll talk about the people that actually do the D a in terms of how this goes into operations and some wider sort of security considerations and ethical pieces.

So I'm the opener just to warm you up, but the real quality is, is coming and coming later. So, uh, the drive to innovation, um, we're all on this relentless drive to innovation and certainly. And within this context, uh, there is, uh, a constant push whichever sector you're button. I talk about private public and third sector, uh, whether it's for profit, uh, in the private sector or for efficiency and effectiveness value for money, with public purse, for the public sector.

Um, and, and why the do you know doing more good? Uh, in the third sector, we're all looking to drive down waste and cost, uh, bottom line, if it creates, in fact, I'll put that on quorum. Um, errands, let's say money. Um, but what do we do? This will ultimately it's driving. Um, it's driving the pace organization.

It's drying up driving our competitive edge. We want to drive better services, bringing down our costs, uh, increase customer satisfied. So that's the why, um, holistically, but actually from an individual perspective, if you are like me, literally my job is to drive transformation. Um, so actually how do we, as a, as a, from a human perspective, um, advance in our lives and our careers and our sense of worth, well, actually it's about, um, being good at our job and moving up forward.

And I highlight that because ultimately we're all siloed to one degree or another, and actually only communication can help us transcend that. So there's a market dynamic needs to do this as a competitive advantage as a continuous striving to drive down the cost of doing business. So. The as, as, as I identify the areas that we're looking at, our employment and an insurance claim within the context of using video video has been a massive, is driving massive change within society, whether, uh, children watching, um, tick talks, uh, the, the, the movement to YouTube and Amazon prime and streaming services video has changed all of our lives and all of our habits.

And increasingly a lot of home grown video. It's one smartphone CCTB dash cam, um, that is prevalent and actually managing millions. Billions of hours of video to derive. A real value is, is, is, is a major challenge. And ultimately when we're looking at securing our future, how we work together as these different cohorts, these different sectors, I think is going to be really meaningful and bold.

And ultimately one of the major challenges that we face. Is, um, what I call the cost of the narrow view. Um, there was a report that came out or UK government in the summer talking about the overhead of our technologists across government, which is estimates to be up to 22 billion pounds worth of technical debt, um, which is at least 50%, uh, Katie yellow, a new acronym for you on that this morning, which is keeping the lights on, um, which is basically every time a package goes out, something breaks and there's a whole bunch of tasking to fix it again.

This is so to remediate the problem that, that new security patches they're stuck between a rock and a hard place. You can't not deploy the security, perhaps we don't know what's going to break when you do. And when you have hundreds of systems, it's virtually impossible to completely test that all day long.

Clearly cloud is part of the solution. But it's no Shamgar either. We need to have a joined up systems. And increasingly that's part of the challenge is working one organization. I can think of one day space in government that has over 300 users across government and private sector. Um, the, the knock on impact, we can't know everything in their systems.

And one of the, one of the why the challenges are really goes to, you know, some of those core mission missions around the environment and actually delivering public, uh, public services, uh, with the challenges of migration and climate change, et cetera, et cetera, um, is all the time we're spending, keeping the lights on just keeping what already worked working.

We're not actually solving some of the bigger problems. Um, and actually this goes to the climate crisis that Simon referenced in his construction talk. This is the overarching imperative. I know we've all had our minds very deep in COVID thing, but as a transitionary thing or as, as significant and globally impactful and, um, president as it was, um, ultimately we're getting ahead of that now, uh, different countries at different speeds, but at some point the worst of it will be behind us, hopefully that is now.

Um, but certainly it should be getting better over time, but the climate situation actually, it's still, we still have a lot to do. And what I referenced that when I'm talking about, uh, technology, um, will ultimately onset of global power consumption is in data centers. So actually the burden is on us to actually drive really good and efficient technical.

The duplication is one of the big areas that I talk about. And I've been looking at in Publix public sector, whether within separate silos within an organization, say a police force or one department may not know who advanced technology is being rolled out in another department. But certainly when you look across multiple forces, multiple motives, multiple arms of government, there's lack that.

There's a great lack of detail in terms of someone's technologies that are available partly by virtue of the encrypt incredible complexity, the number of systems there are. And actually that pace, that relentless pace of driving out new cool innovation to particular service areas. Government is a big old beast, but it's not as big as government society of that sector put together.

And that's where mapping as a shorthand is incredibly valuable. So talking to these use cases, Fundamentally, I'm a strategist as bull everything down. It's really about request or a report. And when we're talking about the recruitment side of things, it's applying for a job, whether that's as an external candidate or even an internal candidate looking for a transfer and certainly large-scale organizations that might be certainly multi-regional.

They might be multi-national of doing an internal transfer, but even if you're an external applicant, um, a lot of recruitment is driven by LinkedIn these days. And I know how little money can go a long way in terms of amount of recruits you have, and then the burden of doing the sift. And do you hire an external agency to do that?

Why should you look at your quality, et cetera? Clearly, there's a massive. Interest in driving efficiency in that, because actually in some cases, something certainly a number of roles you want to draw out beyond outliers, but equally you don't want to, you don't want to have an endless pit of money going into the sift part of the recruitment process.

So again, that, that imperative of you want to do the best you can, but within, um, affordable constraints, whether it be time or money. And clearly there's a real interest in using, uh, automations and AI in the specs. And certainly, certainly some of the organizations I've seen now a much more hip and modern startup-y kind of organizations than public sector.

Um, but I think this will, um, You know, being more widely adopted is, is where the streamline nature of being able to apply for an application, being saying, just give us your name, your LinkedIn profile, and a groovy, funky video saying, hi, you're the guide for us or the girl for us. Um, and that sounds really cool.

And that's really very, very helpful for digital natives are very familiar with cameras, selfie. Hi, I'm Simon shepherd. I'm going to be awesome at this job. And here's my LinkedIn easy submit study in a couple of minutes. But if you are from the organization side, what do you do about that? And we'll go back and start in a bit more, more detail in a moment with a map and then talking about claims.

And this might be. Very very different, right? Um, whether, uh, a, you want to re report a, uh, an accident or even, um, a crime that you filmed on a smart camera or on a personally owned CCTV system on your house. Somebody stole your car or tried to break into a car, et cetera, how that might be submitted. So two very different use cases with request report, but actually underpinned by some very common technology.

So again, to talk a little bit more about the detail, um, a candidate, rapid low costs, sift as good personalizing friendly persona, it's creating a view of the organization that is recruiting as. You know, conscious of the candidates time, respectful of that time. So that's, that should be a plus to the candidate.

Um, maximize the return on investment. Ultimately, we spend X on doing a recruitment. We want to get the biggest draw of talent possible. So we want to make them first streamline. And then actually what most candidates might not perceive is actually the minute we are allowing somebody to, or requesting somebody upload a video or making it an option to them, what else can we derive from that video that actually you probably wouldn't pick up from the CV, the LinkedIn profile, um, for those that have been looking at this AI sentiment analysis, um, you know, mark is about honesty, um, good communication, styling, tonality, all of these things can be lifted very, very quickly.

Uh, whether that's the right quality is, is from our colleagues to discuss about, um, but you know, honesty, sincerity, quality of, of, of communication. And also these technologies scale, the bigger the organization, the bigger the ROI, ultimately they're multi-lingual by default because, uh, AI is fricking, um, so an insurance play, um, seemingly very different, but ultimately dash-cam CCTV as described.

Um, this could be for your own personal time on an insurance, cause you just want to push that through. So you get your grade back quite quickly. Um, but. Um, if you look at this as I have, uh, in terms from a mapping context, um, you start to think, and you consider the natural evolution of these things. So first pass, it could just be, this is an easy way to upload an insurance claim.

Certainly it's an area where we're increasingly reaching out to the public from a law enforcement perspective. If you're a witness to some violence or, or an accident, the dash cam. And that's being submitted, but some people that upload this aren't particularly technical savvy. So they upload the whole farm, like 30 minutes of video that has to be manually reviewed.

There's a massive driver to say, we'll come up and cast Nate at the time to review that evidence, to see if it's sufficiently evidential and absolutely just saying, Hey, here's a picture of the accident. Uh, please, when we're logging about sex or whatever period of time, we need to reconcile it with the right accident.

You know, virtual cards are great, black and silver, these things that doesn't help. So you need to identify it. Um, Reducing liability. So from the private sector, not to big consulting, talking about merchant services, clearly an insurance company has a, uh, an overarching, um, uh, requirement to try and show that it is it's insured.

Party is not liable wherever possible. So it's massive incentivize to capture evidence that supports that. Um, but ultimately we could see, as we've seen in certain previous insurance approaches the, um, introduction of the introduction of the. Uh, insurance benefits to people having road sensing devices in the home.

So for young drivers that they're not speeding or accelerating too quickly, et cetera, et cetera, you can see this naturally extending into the use of video. Increasingly cars have cameras built in 70. Tesla's got half a dozen. I think the truck's gonna have, uh, uh, um, it's not a big reach to actually make an option going straight to your parents, a small car.

So actually just say report that crime, or actually just saying, as long as you turn that option on that could be auto submit. It. It's a leap from where we are today. Technically it's not hard. It's not hard to do. And actually, um, there was an interesting statistics that I don't have to hand, but it was even all the cohort of the public that are really passionate about that privacy.

Um, uh, about 50%, we'll flip that privacy consent from mine. Um, convenience benefit out of financial benefit is probably take it up to 80, 90%. So you might be a massive private sector. We'll give you five pounds off your next visit to the supermarket and suddenly say, wow, have all the data. Um, uh, you know, we, we, we see that with kind of, um, Oh, I'll call it.

Yeah. Tesco Clubcard points. It's a classic example. What can be derived at a Tesco? Um, those are familiar. It's a large supermarket chain in the UK. Um, the, the, the customer service kind of value piece is I know for a fact that the amount of alcohol you consume in a week is considered if you, if you, if, if you reach out for their insurance.

So if you're looking to get a Tesco car insurance, I've, I've heard in passing, uh, the amount of alcohol you drink minor shifts like that, that, that premium. So ultimately you might give that up for, uh, two pounds off your petrol for like a week. Um, so that's the point. We talked privacy, but actually benefits the way.

Um, and this is where it comes together. So we've got two use cases, very different, but equally the same, the essential characteristics from my level, when I'm talking into sort of C suite, um, in terms of how this would get signed off, it was saying it's quite simple. Really. Um, customer service goes up, it gets improved.

People will be happier. They will, with our service, they will see improvement. We will bring costs down because we'll use an AI layer to, uh, help, help this being done, uh, which is cheaper than people. Absolutely. It is, of course it is. And it scales. So the, the, the long tail of this is significant. The, because we're using, uh, automated processing, uh, the, the.

Uh, disappears and Backroads overnight. Um, and equally the processing time reduced from house days or weeks, uh, to seconds or milliseconds, which again, a benefit and ultimately that all drives up profits. It drives up value for money that is literally our swarm purpose in public sector. And it's our core purpose in industry.

Um, and actually increasingly now, because of the maturity of, um, services from the major cloud providers and others, these are commodity components. So the actual, uh, use example where I'm talking about, uh, we're gonna have a fantastic new insurance product that will give you maybe 50% cheaper, as long as it gives all this data or totes and cheaper.

But we're making that back in spades in terms of reduced liability, et cetera. And that's the innovation, the technology components underpinning it commodity now. So actually from a project risk perspective, I'm using a series of commodity tools connected in a, in a, in an elegant and into a way that's very low cost from a delivery perspective at C-suite level.

I'm sure Roswell, you consider that. So a map, this wouldn't be map camp without a map. Um, here's a map of both processes. And the only difference is one is accent report. The other one is job application, and ultimately taking you through the steps. Those more familiar can read it, but I'll just talk you through.

So starting off with a user, they have a requirement to go to have an accident report or a job application. And the job application is slightly more. Uh, extra report is pretty much more standard, but again, that what's in the product category and they're going to do that by our website. How are they going to do that?

How are they going to be less than via the process we're skipping that stage of, of, of, of, of applying or, or engaging? So the website is going to request two things. One who are you to Clifford, and can you upload your video? Yes, please. So personal details for those that are covered by GDPR, we need to consider the GDPR consideration.

Um, and that is going to be captured on a hosting platform. That's going to be on cloud computing, um, the video piece, a secret source. Um, that's going to be very much a custom built competitive these days. Um, and actually what it's looking to do is identify key characteristics. You know, the, the, the, um, Key metadata as to what I'm saying, the nature of potentiality and, um, of, of, of, of how I present the video.

It's also going to identify on a male and white middle-aged and overweight, uh, and, and many other things combined. Um, so, so ultimately that's not in your CV, that absolutely is in your video. And that metadata is the, is a secret sauce in terms of what makes this more powerful. It's going to be quicker.

It's going to be cheaper and we're going to drive insights that skip a whole raft of activity in terms of conventional route equally true for the accident report or CCTV camera of a burglary. It's going to identify the perpetrator. It's going to densify the license, but it's going to identify blame very, very quickly and make a recommendation.

Ultimately, in most of these cases, a human is making the final decision, but heavily influenced by the data that's presented to them in black fall. And they're in. By some of the rough in terms of as long as it's accurate, I won't seal the cons of my colleagues. Um, the enabling technology component piece, obviously again, that is the, that the, the great bit, which is a range of, uh, composites, um, composite component, composite AIS.

So in terms of police mature to most mature voice to text, you know, we've all got, uh, intelligence speakers, or a number of us do. We can talk to our phones that is mature, mature, mature, not huge amounts of risk in that I would argue object recognition, something I've done a lot of work around, um, whether you're talking, faces, guns, et cetera, et cetera, within the law enforcement context, but equally license plate cars, descriptions of objects, brands, et cetera.

And the service offer either organizations doing is it's highlighted in blue here. Um, I didn't find the key characteristics, my space, et cetera. And then there's a wider consideration as well, which is that of legislation performance steps. So, um, where does this take us all? Actually, smartphones are present digital persona, um, and they represent our Abdallah identity.

So this video is not only, I'm gonna share a lot more information. Probably the late user would recognize linked to our, um, our profile data links on mobile phone. That's going to provide even more detail, which maybe we'll talk about in the Q and a session if people have questions about, um, and certainly there's an underlying demand to have increased data accuracy.

You can get new smartwatch and the latest one I'm looking at has a fire. He can have a five different geolocation map, uh, satellite systems. It's going to get more accurate. That's really, really valuable increasingly what we do with that. Um, and, and just a wider context. And again, this is a bit of a leap, but.

Uh, the, you know, the understanding of how much DNA is being shared on ancestry websites and, uh, law enforcement use of this in terms of linking it to crimes. Um, something I only learned quite recently is how, you know, how linked we all are genetically, uh, in terms of Heights like third cousins. So ultimately you only need about 2% of the population to be accessible by the innate database.

And again, that's that further connection at the moment we talk about the video that's linked to smartphone identity, potentially down the line. This could be linked to a genetic identity. Um, it can start to sound very. Um, but actually I'm an optimist. And I do think there is a joint up in terms of, uh, how we secure our future.

I think we need to have a more mature perspective in terms of data sharing between the major components of society. And I think if we are going to secure our future, we have to do it together. And, and part of that, uh, is, is about having an understanding what, what our roles are and what we're doing. I think there's a lot of stage gating in terms of how information is shared, but absolutely more showing should happen.

But within a transparent contextualized way, um, private sites have a massive part to play in this, but equally government control a lot of things. Um, so it needs to be in puncture. And this is where I've been on a journey with mapping and public sector, uh, where I've been using it for very senior stakeholders that don't understand.

But do understand strategy and steps to achieve certain outcomes. Um, and within that context, it's exactly this it's, it's about fundamentally it's about better understanding of risk reward getting rid of the clutter. Uh, I use it for technology process, ethics legislation, um, and, and with the combined.

Certainly coordinating between, um, C-suite finance technology and users can all read off of a single map and hopefully, uh, today's presentation. Well, we'll talk about how three different perspectives can be, uh, talking from a common purpose, uh, correlating those stakeholders, identifying bottlenecks is key like that, that clear, clear inertia from one, uh, one phase to another.

And then actually considering, uh, the piece we can call it. I've certainly done some stuff in terms of trying to put myself in the, in, in, in the shoes of a criminal and some saying, well, how would I innovate as a criminal and some of the, how I would get passes because ultimately in policing, we lock people up and then stick them in a box for a few years to figure out how not to get caught next time.

So ultimately sometimes we have to project ourselves in terms of how they will innovate to continue to be, be criminals. And that's my big dumb, uh, look forward to some interesting questions later. Thank you very much.

Okay, thank you for that Simon. Um, so as a Southern mentioned, there'll be a CUNY, you know, at the end. So if you can, um, type your questions in the Q and a section here on zoom, uh, not on chat, uh, that would be great. So we'll pick them up, uh, at the end. Um, I actually forgot to introduce myself. I'm Jen Ashley, and I'd been co-chairing this conference for, uh, five years now.

Uh, but I'm not going to take too much away, uh, from Ross time. So, uh, over the years, I just, I'll just introduce myself first. I'm Rochelle. Um, I've been in technology now for about 25 years. Um, mainly in the automotive and a bit of financial sector. Um, and I'm head of delivery. We buy any car. Um, none of these things I'll talk about are things that we're going to do it.

We buy any car, it's a representation of what we might discuss in the private sector, um, when we're taking some of these ideas and seeing how we actually kind of move forward and how we're going to get them through to delivery and actually make them happen. Um, so I think as, um, Simon. Said, we've got two opportunities here.

Um, one is around the HR videos themselves, where obviously someone's going to come in with that nice elevator sales pitch and say, great, okay. Opportunity for you. We can improve that CV safety. We can make sure that our candidates don't actually have to travel to you. So it's more convenient for them.

We'll get more candidates through the system. It will take less time. Um, it will be automated. So we're going to start removing some of that unconscious bias. Um, some of these things are going to be really, really important to us in the actual roles that we're trying to recruit. So it might be that the roles are kind of scarce and that you've got to recruit all across the country because there's only a few people that are really kind of thought leaders in the area.

Um, and our AI integration is going to really help us hire the right people for the job profile that these companies have put for. Um, similarly the insurance claim, um, assignments that this is going to give us some really, really good ideas of what the actual accident is, how accurate the damage is around this vehicle.

And we're going to get a lot of the metadata that's already in the submission from our, um, unfortunate person that's going to have to do the insurance claim. Um, we're going to say what their location is. First start with the geo targeting. That's associated with the video feed in the picture, and we're going to be able to see the weather conditions.

Was there anything else that was contributing to the accident? Um, lots and lots of things that you wouldn't necessarily get from a handwritten witness report. It's going to enable us to potentially identify further witnesses so that we can start saying, Hey, did you see the guy in the red car, um, improve those claim handling time so that we can potentially automatically pay.

On an insurance claim where we can definitely see it's a nettle fault. I've driven into a wall, just pay out, um, because it's like comprehensive insurance, our claim, and our AI integration, our unique selling point for this software is hopefully going to enable us to work out, which claims are genuine. Um, identify potential fraud, get things through the system faster, make our handlers lives easier.

Um, you can just imagine the kind of sales pitch that's coming from our marketing comms team. Um, and they've said, great, there's a massive opportunity here. We've, we've spoken to quite a few people and they've said, there's a need for, this is a genuine need in the market. Create is a solution. So one of our first things that we just got to actually consider just at a very high level is keeping our users secure, um, there's legislation in place, GDPR, um, for our right to be forgotten.

But we also have a need to retain some of that data. So in the case of where we might have employed and the actual person that came through to interview, um, in order to save for any future prosecution against contractual issues, it might be that we've got to retain some data for six years because we did actually employ them.

Um, similarly, if there has been a claim and there's some criminal, um, opportunities, or there's been some crime committed, we may still actually have to retain that data for a lot longer as well, so that we can actually just make sure that that claim might not reach the courts for, um, several years. And we've got video evidence that's going to help, um, get the right outcome for our client.

Um, you've also got the fact that somebody out there is just using their mobile phone to say, God, I've just been in an accident. Let me upload this. And what you're actually getting is a little video of the kid eating breakfast this morning. And it's like, oh my Lord, let me change that video. And please remove the one that's already there.

We're going to have to be really, really clear what the purpose is for this video. Um, just to make sure that people understand that this video will be used, um, in the process of this claim. And that might involve us having to share these videos with external agencies. There's a good chance that we're going to have to share this with law enforcement agencies.

Um, we're going to have to share it with the opposing insurance company, um, so that we can say, this is the evidence that we've got. This is a no fault claim on behalf of. Clients. Um, but that data may be shared. Um, similarly, we've going to hold the metadata for the, for that particular piece. And we've got a decision as a company to decide whether we just share the raw footage.

Um, maybe the place to say this is the accidents occurred, or whether we also are going to end up sharing our metadata, which may include some of our AI tags to start saying, this looks like an honest person giving the witness account. And, um, you know, these are the weather conditions at the time, et cetera.

We've also got to just keep in mind who can view this video. Um, so we're going to have to put in place moderators, um, the people who might be either doing the CV sift or people who are actually examining, um, some of the accidents and being able to say, yeah, is a genuine claim or not. And we're going to have to answer the question of where is my data.

Where's my data being held. Um, I've got considerations for the actual solution itself. So technically, um, I'm going to have some like headliners, I'm going to give you something that is cyber secure yet easy to use. If I'm integrating into a system like LinkedIn or I'm integrating into a system, um, that already exists for our insurers.

There's a good chance that all you've got to do to log in today is to give a Facebook click or a Google Hangouts click or put in a simple email and password, um, may want, because this is more actually sensitive data to put in some two factor authentication, for example, so that, um, we really are protecting the data at the end.

We've got some technical business decisions to make around our solution being scalable, secure, um, optimizing the cost for our company before. We are a third sector, charity, not for profit organization. We've got a profit at the end of the day to make here. So we've got to try and actually come up with something that's cost effective and reliable, and that we can also support as a company and in our vendor selection.

Um, when we move into the map, which is identical to the one that Simon shared previously, um, I'm going to choose where my database is and where the cloud compute is for those particular pieces. I'm going to look at some of the latest legislation and GDPR, or what's coming and go with the sort of Schrems too, and actually just work out.

Where is this data being held? Um, what do I know about the company that is in my vendor selection is my company saying I'm only going to work with, um, people who are actively reducing their carbon footprint and green suppliers. I lay that there's a whole load of options when we're considering who to actually.

Signed a contract with and get compliance involved into the illegal journey that we're going to have to go through contract review and everything over who we actually choose to keep our data with and who can actually help us process some of this AI. And then we've got long-term storage considerations.

So as I said, if there's a piece here that has got some legal implications, we can't necessarily, um, release that data because we've got to hold it for legal reasons, six years for employment law in the UK. Um, that's if it's a successful hire and there could be a contractual claim against it all, um, with car insurance claims, as I say, it could go on through the courts for awhile.

And are we keeping just the metadata or are we actually storing the raw data footage itself and, um, processed manner, because that might be the piece that we need in seven years time, we can't necessarily predict what's going to be important.

And also when we passed it to a third party and someone said to us, right, okay, delete it. How confident are we that that is actually deleted off their systems? And it's not actually just hanging around in some kind of backup somewhere. So looking at the map, um, from this private sector of the company, am I expecting that I'm actually working on this area of uploading the video, the personal details, the key characteristics and the metadata that we were going to be storing for these two stories, the HR piece and the car insurance piece.

And, um, I would like to go back to the mountain. So just ex excuse me a second. Um, the identifying key characteristics piece is in our Genesis phase. And if I take an example of the, um, the video in the custom built phase, then in these kinds of areas, um, the identifying the key characteristic. Because we are definitely in this Genesis phase, um, it's going to be very experimental.

We've got to identify, uh, what does an honest person look like? A lot of these technologies are not yet fully, fully formed. Um, I'll go back to think it's about 2018. Amazon in their early days stopped using some interview recruitment software that they were creating because it had a gender bias. Um, it definitely didn't like females and they didn't like women who were talking about being part of the women's chess club.

Um, and they chose not to use that things have come a long way and the technologies have developed since then. But I would imagine in the company that I've got, that is going to develop a solution. I've not got the scale and the number of developers that are big corporate, like Amazon, Google, Facebook of golf.

I'm going to have to go through quite a few phases of looking at videos and assessing whether those ones are genuine claims or not genuine claims. Fraudulent, to be able to tell the model to learn that this is actually an example of a bad interview or an example of a fraudulent claim. Um, I've got to keep going through a feedback loop here, and this is going to be a very, very costly phase.

And I've said it in my solution design that they team competencies initially low it's an innovative area. Um, but there's a good chance that my software engineers haven't dealt with some of these technologies before that they're learning to, um, they will learn initially through mistakes and we don't necessarily want those to happen with the people that we're partnering with.

So we're going to have to go through some phase. That are very much exploratory to see what a production ready solution would look like for this. If you're looking at the custom built phase, um, uploading video, that one, I'm probably a lot more confident about. I've still got probably some problems where my team might just be, go into, um, use some open-source code.

I'll go to stack overflow is kind of like the answers over, how am I going to actually just do this and achieve it and get up to speed. Um, but they're going to get up to speed a bit more quickly than an area and a domain that we're just not familiar with. And hopefully I should be able to get to out in a kind of iterative manner and be able to keep developing on those stories, um, and get something out as a solution to market a little bit.

But then I'm going to be in a say in contrast to Simon's optimist, I'm going to do a bit more of a pre-mortem and say what could go horribly, go wrong for our company, for our brand. Um, we're going to do some potential brand damage. If we get a data breach, that's just a given. Um, if we do get this data breach, I'm expecting to end up all over the press.

Um, my stakeholders, if I've got, um, uh, listed with the U S Sharemarket, then the sec is going to have to be notified about data breach. And if any of my directors are trading shares at that point in time, then they could be jailed for a bit of insider trading, because they'd know about the breach way before all the different stakeholders and the shareholders would, I've got a rest that the AI doesn't have the intended outcomes.

So, um, as we. They suddenly started recruiting a lot of, um, male hires because of the bias that the AI had developed towards, um, to women. Um, you've got to be able to recognize that and be able to actually just put those stops in place. If that happens, we still got a massive problem here that we might not be first to market.

We are a private sector company and we want to make as much profit as we can do. Um, and part of that will be grabbing market share as we just get this launched and we might not be profitable with this idea. Um, in the early days, I'm going to have to set some confidence thresholds over how much I trust this AI process data.

The early days, I'm definitely going to be doing a lot more manual verification of the model and trying to train the model up. Um, and that might involve an awful lot more pairs of eyes on the video feeds than we would normally get. Um, I've got ethical risks to consider around privilege. Um, data protection and intended use today, I could start my company doing a screening of developers that have got cul skills.

Um, two years down the line, I might be saying only hire developers that have got SQL skills because they've got like a hundred percent higher rates. Um, I've got to be very, very sure that I'm matching something with the profile, and this is actually just a modifying in the future. Um, our self-regulation isn't up to scratch, so we let it fall by the wayside in sort of 12 months time.

Or we stop thinking that we've actually got to invest time on something as this is keeping the lights on business as usual, and just start running off with our next great ideas of hooking up to the Tesla and understanding what happened with all the actual data from that Tesla. It's a new story that we're trying to move on.

Also, I'm very, very public in the press at the moment. There's a good chance that we might have been hacked. Um, it's not necessarily data to breach where we could have accidentally exposed it, left the documents in a bus stop or anything. Um, there's a lot of people out there with mal-intent who might want to watch it, just, um, hold us around some hackers, just, um, um, basically use our data for all the mains.

And then, um, we've definitely lost the trust in our customer base or finance. We've got to, we've got learning. That's going to be based on this implementation. And we also need to be able to handle those exceptions that are flagged by the system where it says, I just don't know whether this person's going to be a good hire or whether this is, um, a genuine accident or not.

We've got to review our cloud compliance processes, um, and see if they need updating. So it could be that legislation changes for GDPR. Sure I am something else in the future that might be coming up. And we've now just got to watch to just say, right. Okay. Have we got to change some of the way that we actually delete the data and have got to change the way that we anonymize the data, um, appropriate use and access or in, so who's actually viewed this video and then we've got sort of regular cadence of security views, penetration testing, a lot of things that we would normally do in delivering with the private sector.

And then as Simon said, there's going to be constant, um, vulnerability patches, and produced for any of these software platforms that we're working with. These could very much disrupt the service because we've got this kind of impetus to get them deployed so that we can make sure that our secure security vulnerabilities, um, um, exploited by anyone, but they could also have, um, or known impacts to our level of service.

Um, I'll just wind up with a thank you. Ask you the question at the moment, if I start cropping this image, is this dangerous driving or is this actually a qualified steak driver carrying out a stance? So context is key. There's got to be an element of understanding the data that we were looking at. Um, actually still having access to the whole data at the end of the day so that we can actually make some judgements there because there's a lot of fake news out there.

And a lot of fake news is people engineering, videos, um, so that, um, devices and the software coming out though these days, wherever you can kind of like stick your face on movies and pretend to be the actor and all the rest of it. So if we're in a world where people can bring the Mona Lisa to life and make her into a video, we've also just got to make sure that we, um, look out for this in the future and I'll hand over to Sarah.

Hi there. So that's, uh, that's T class acts to follow and, uh, I'll just get my, my deck shed. Um, so my job is, uh, been variously called, uh, governance risk and compliance or, um, the dark side or the dark sides dark side, because I don't think I've, I've ever had a job where people have been, uh, properly pleased to see me.

Um, and this would be no exception. So, um, I have made it, my life's work to try and remedy that situation, which is to face up to the fact that we're following on behind from, um, an awful lot of, um, enormous promise and enormous potential strategic technical, and, um, profitable advantage. Um, We've got to recognize the part that we play in organizations.

Um, one of the reasons that I joined full humanity as an organization, as well as doing my. Private consulting is because I wanted to look at that across the piece, but I don't industry view and really just following on from what these guys have been talking about, I want to kind of set up the store. I'm not at a level of granularity because I've only got roughly 15 minutes about what the governance challenge, um, actually entails.

So we have Simon's map that shows us what the strategic advantage of is. It's got, um, a lot of meat on the bones to, to illustrate it illustrates that Simon, um, has, has talked through in, in great and experience depth. Um, Simon's kind of presentation is the kind of presentation. I sit quietly the back of the room sometimes with my head in my hands, sometimes feeling quite hopeful and sometimes waiting to ask, please, can I speak to your security long?

Cause I really want to get into the meat of the bones of that. Um, because Simon highlighted GDPR, I'm gonna want to know about all these things. I'm going to know what buy web security I'm gonna wanna know about API APIs. I'm going to know, want to know about platform. I'm going to want to know about the IDM plugin.

I'm going to want to know about application security. I'm to want to know about the database. I'm going to know about, want to know by any other third parties that are involved, but for the purposes of this presentation, I'm going to focus most on my most recent, um, obsession, which is how can we equip your average firm to start to get their arms around what you use of AI.

And w why would we bother, I mean, what can go wrong?

These breaches don't all represent, um, uh, ransomware or hackers. These largely represents things that built up over times. Um, Strategic decisions to, um, forego governance, strategic decisions to stretch the time before compliance with requirements or, or simply just scale getting ahead of, um, showing up some of the foundations to bear the weight of, of progress and next phase development.

There's a lot of technical debt that sits underneath an awful lot of these things. And there's an awful lot of, uh, failure to strategically compete, um, between, uh, profit growth, data acquisition acquisition, and, uh, some of the underpinning human rights that sit under data protection and security, but it needn't be that trade-off, um, what we, what we have though is an inherent tension because we often haven't built those foundations.

So moving from a minus position to a level playing field is, is, is really. Stressful. And this specifically in our context at the moment, um, uh, the first one is, might recognize it as about higher view. High view has, um, quite an, uh, a robust, um, uh, audit at the time from friends specialists. But, you know, it covered so much of the underlying infrastructure, so much of the data processing, so much of the model operation, um, and.

Perhaps didn't cover the end to end of, of what was actually happening, which raised a whole bunch of questions, which impacted the decision to, to halt some of the video analysis for, um, hiring on the other side, in the sort of accident, assessment insurance kind of space with a tipping over into, into policing.

We have the slightly painful start of response to, uh, uh, blowing up with lemonade in Sharon's, where they mentioned the overthrows and data points. They were harvesting from videos to make a decision about coverage in a few seconds. Uh, and they reversed out of that. After questions being asked out of an abundance of concern and a admittedly, uh, easy to argue, variable variability and understanding of what was going on for the Twitter royalty at, uh, at large.

The yellow quote is about a paper produced by, um, Bieber Berhane at owl, cognitive science specialist, who worked as an intern. Um, with Google, they analyzed the a hundred most quoted machine learning papers near Epson ICML and only two of them mentioned adverse outcomes. So these things are being developed into proof of concept, which is a tight pipeline.

That's only a few months, these days without really looking at adverse adverse impacts. If you're inside of them. And if you're trying to do the right thing, I mean, what, what are your challenges? Well, we ha we have a paradox. It isn't, it isn't just one instance of AI. It isn't just one change project. It isn't just one vendor.

In a lot of cases, we have to have whole shed loads of things, or we are in a very small firm. That's needing to be nimble and needing to be agile. And the last thing they can afford to spend two, to pause and spend a lot of times. So people tell you, well, prioritize, what are you, what are your priority things to look at?

Or what are your priority things to kick the tires for? Um, and you very rarely have enough time or boots on the ground. And so people tell you to prioritize your site prioritize based on what they say based on risk. You don't know what the risk is because you haven't had time to assess them. If you haven't got enough people and around the cycle of engagement trouble, you go it's felt, it feels like grit in what, in increasing the, a highly focused continuing development machine, which.

And it's highly reasonable and we need to be innovating in the space of governance. And there are, there's a lot going on in the DevSecOps space and in the automation space, which makes this easier. But most funds are not at that level of maturity. You have to be realistic about this. And security is not the first thing and data protection oversight and ethics oversight is.

And the first thing we fund for as a startup, when you're in your seed funding phase, And it is cradle to grave. We forget about the fact there's ongoing governance needed most of the time in the business models that AI operates within. There is an explicit, um, uh, um, limitation of liability after something is into production or having been sold or delivered up the supply chain.

So that green, ongoing governance space, the exit management space and the due diligence spaces are all quite, quite difficult things to do. And the inherent risk assessment for somebody at the end of the supply chain is completely different to somebody who's just acquiring the data to train a model training model or, or run.

And these are the things of Central's that centered on during my career as being critical to, to whether we're in a position to do the right job, whether we have, whether we can, um, influence in intent to maybe go a bit further in terms of overseeing these things that potentially go wrong. Um, so there's a maturity and capability.

Do you actually understand what an ethic is? Um, I mean, we're already at that level for most foams. Um, do, do we have any body who isn't, um, stereotypical tech dude, there's a developer now there's up. So they really, I'm not stereotyping in terms of quality, judgment and value judgment, but there was a fairly narrow band of reference for a whole lot of the developer community that may miss things that are potential adverse outcomes that should be taken into account.

Risk estimation. And in terms of visitor risk, if we find stuff wrong, is it a case of JFK BI? We just need to get over the line. We've got a market advantage to take. Um, we don't have the budget for, um, gold plating. We just want to get minimum viable product into the wild right now. So then we work out where are we pushing the risk in the supply chain?

And it isn't just ethics. I mean, this is a really reductive stuff, but it points just so it lined up nicely on the slide. Please don't think this is all, I think these things entail. Um, but it's not all novelty in AI space that, so we can actually assume that the things are too novel, that there is, um, everything has an unknowable quality about risk.

It really doesn't a lot of them, the stuff that we've always been concerned about and needed to govern is in there, security, privacy, quality, safety, new regulations, yes. Around ethics. Ethics is actually reaching some level of maturity. I'm not going to get into discussions of, you know, is it utilitarianism or is it another form of ethics?

Our challenge is making space to bring experts in to have those conversations. If we are just having a conversation about how we best define effects and trying to bring people up to speed while everything is tearing on hell for leather, it will have gone live before we finished producing a report.

This, this, my focus is squarely on making space, the conversations that need to happen. And that is about engaging as early as feasible. Killer questions is at highest risk thing that we need to do right now. How much inherent risk is there? Absolute criteria, conditional criteria? Do we, descope it? Do we defer it?

Do we delegate it? Do we engage for all those different pillars of, of requirements? Um, before we get into the more traditional focus, just kicking the tires and then patting remediation, none of that last section assess and manage works unless you've got the prior ones plugging in an early enough phase of engagement.

And these are the kinds of things. I mean, by inherent risk indicators, things that it should be reasonable to know things that you should know at an early enough phase in, in development, to be able to stand up plugin, integrate requirements into whether it's waterfall development or whether it's continuous development, some things that your project manager can have as absolute red flags to say, okay, if we're not going to sort it in the next sprint or the one after, then we really need to, to throw it up the, up the chain.

And from an ethics point of view, it's becoming better defined, but there are so many lenses to look through in the places where we are lacking at the moment is access to diverse inputs from multiple stakeholders firms. Can't magic out that kind of breadth of insights. Um, law and regulation is, is changing hand over fist KPI and KRI designed for AR suffers from everything to do with risk management around AI, which is like a tail data, uh, and estimating residual risk of adverse outcomes.

Some of that fundamentally resists quantification. So it's very hard to produce metrics for those things about petite potential trade-offs in whether we can tolerate some risk to individuals around data protection. For instance, um, after delivery, um, looking at who is more or less vulnerable to potentially things that may go wrong versus something like, uh, delving into the data set to analyze proportionality to your target population, to properly de bias.

And the other aspect of this is are we just doing a show in town? Are we going to downstream party to, to provide some of the AI inputs through the supply chain and taking their word for it, that things are compliant or are we actually able to do any due diligence? The orange section is the technical testing systems code and data.

Then the other side side isn't, the blue defection is more traditional audit, focus, um, people, um, can't magic art, the skills and abilities in data science and engineering to, to, to do the technical testing and in, across all of the fronts that we need to scrutinize. So if it's 70% compliance, because we would say, because folks said, so, you know, degrees of compliance, as I said, um, level five might be that we were told it's combined.

It's really not the next level. That might be it. It is fit for purpose. We've got some evidence that exists, but nobody can show us at working the next section, right. People can show us, show us the control working. The next section is they can show us that controls work all the time. And the last final section would be you actually have an active feedback leap.

So you working on continual improvement. Um, if you piece that together and then look at the, um, tension seat introduces when you've got to do due diligence to understand this and to drive remediation, um, and understanding what portion of the risk you're managing is it, is it all of all those pillars of risk and what it will take to fix that's when you can start to have a management conversation only then.

So it drives in the idea of how early you need to get into the. And this is me taking a run at mapping, all of the moving parts that go into that kind of engagement. Now I've, I've left in for this, for this version of events, um, all of the different, uh, intersections and inputs around other elements of operational risk management, it assessment security, risk assessment, privacy, risk assessment, all of that hinges on some key nexus points around at the Genesis and custom custom-built and is a lot of the oversight and governance for AI.

Some of it is a lot more mature. We don't have enough automated monitoring. We need more, most of the continuous changing engagement for this kind of effort is quite immature. We're not really looking at post-market monitoring of models in any meaningful way that we should be. Waterfall changes more mature for engagement, but not in the AI space and feeling most of the conversations thus far has been about what could go wrong, not how we actually engage to assess how long we could possibly go in.

How do we plug into then manage it? So I've highlighted those key nexus points, which are the places where we have shortfalls in the places where we need to focus for funding, focus for engagement, doing a RACI to understand who's engaging at what point and making sure they've got time in their day to engage with us.

And they'll challenge, especially stay on assessors and automated monitoring. Those are the places where we need to focus to bring ourselves up to speed from one side to the next I've taken out all the specialists, AI stuff. And this is probably a more reasonable representation of where people are these days.

Um, data subjects, if that potentially aren't going to get. To anybody, unless it's been through legal, the board and PR and the stuff that's bubbling up is coming out of more traditional scales that might exist in the developer space, especially for smaller shops while they're developing the capabilities, the AI risk assessment, therefore degrades to the point where it's, what information people can rustle up and you move back up to the place where it really should be in terms of visibility and a little bit more maturity by engaging consultants.

But the global in's pint, the global consultant inputs to this too often tend to be a plan for a plant at two higher level to operationalize. But what we can do if we do the inherent risk assessment piece that I mentioned is quite rapidly, get to a point where we can have a meaningful conversation about priorities.

If we have an inherent risk, a high inherent risk, we're doing. Lots of staff to lots of potentially vulnerable people with lots of, um, of sensitive data or things that can potentially impact critical infrastructure or things that can potentially adversely impact the environment. And we have lane maturity.

We shouldn't be moving forward. We should be stopping until we can introduce some more maturity or fixing those gaps that have been fined. If you have medium inherent risk, um, potentially you're looking at decisions to do with insurance. Have you got low lay maturity or capability? It doesn't mean that you can't move forward, but you're going to be proceeding with caution.

You're going to be looking at those places where you've got hotspots of inherent risk and hotspots of uncertainty to mature it, cheer and fix low inherent risks. Amateurs. Maybe you're matching somebody to close that they, um, would fit in a retail space by analyzing video live video of them for in, in our scenarios.

Um, if it's only a small cohort and they're not sharing sensitive data and it can't amplify and it's not driving urgent decisions about vulnerable people that will scale rapidly, you would proceed and you, and. And parallel, but even in those high-risk scenarios, is there an ethically terrible trade-off if we're talking in the policing and national security space, people may want to argue there is.

So then you need to have some backstop because no matter what the trade-offs are, you still need to beat you to diligent. You still need to make people whole, if something goes wrong in there may need to need move rapidly. Um, while there is still high residual risk, either to grab market share in a way that the government has backed is a tolerable, um, risk for innovation, or you can legally limit liability through contractuals and you, you, there isn't regulation that demands a pause, like the prohibition clauses in the EU act, or potentially ensure to make sure that your cover your costs.

If something goes wrong and you can make people whole. Oh, you put a proportionate amount of expert prompt, responsive post-market monitoring in place for complaints handling a dispute resolution. But the fact remains that if you have not done proper Sharon's, you wouldn't know that you are potentially going live with 64% of controls is unacceptable.

So uncertainty that's 64% of controls combined is the amount that a noncompliant, the amounts are known and the amount that are a level three, four or five in terms of compliance where you haven't got an issuance that they are operating over time, or they don't exist, or they're not fit for purpose. So we need to make sure that there's a mechanism to cover those bats and to have options to do so.

And that's when we feed back into the strategic map, we take that view of the likely level of uncertainty we're going live with and the requirements for more resource to, to properly assess risk. Oh, the trade-off to post-market monitoring to making people whole rapidly while we backfill for some of that, we have to be realistic about how often that actually happens.

We then bring up that conversation at that kind of level, back into the strategic environment. And what I wanted to really highlight with this is, um, that we're all pulling in the same direction and trying to treat the same thing. I'm trying to operate in the space between, um, bolts, um, being able to influence things, but not understanding people who are at the coalface understanding things, but not being able to influence.

And those potentially impacted not being able to influence and not understanding. And in terms of our subject to securing our future. We need to navigate that space and create mechanisms without killing people, light touch mechanisms to do better, more rapidly. And we need to make people whole with more reliability, because at the moment there's a little bit too much kicking cans down the road and waiting until the volume of concerns is loud enough or waiting for regulation.

And our future won't be lost because of the singularity. It will be lost because of the governance gaps and Arizona data that layer upon each other and lead to a really uncertain future. And that's the end for me for this. And I think we're handing that back to Jen to talk about some Q and a. Thanks, Sarah.

Um, so thanks to all of you actually. Thanks Simon and rose. Um, and Sarah. Um, so yeah, so as I mentioned in the chat, uh, we can have a Q and a, uh, I don't know if I, we planning to do some more mapping or are we just going to go straight to Q and a again? Okay. Two Q and a and just so we can refer back to what we've, what we've got as much.

Perfect. Okay. Let me read, uh, I need my glasses for this one, cause this window is a bit small. It's funny on zoom. You can actually zoom the chat window, but not the a Q and a window. Okay. So this, a question here from Kevin, uh, and, uh, he's saying, I think Simon is Simon has presented a consultant's view of enabling technologies to take VDD.

It's been around for 20 years, but it's still not in daily use. Um, extrapolating its most commonly used Alexa type devices demonstrates a lack of appreciation of the devil in the detail. What is the likely fallout if this, uh, convergence view happens to be through. Uh, shall I say, shall I start with that one?

Um, yeah, so, so, so, uh, voice detects technology, um, obviously within the map, we talked about maturity. I put that one in the more mature areas, um, compared to, and it's all relative as any map is. Um, so, so yeah, look fundamentally, I agree with the commodity consideration. Th that there is that there absolutely, there are always people that, that, that, that, uh, book at any risk.

Um, but there, I would argue to some degree that there's somewhat irrelevant, um, because actually it's the, you know, to the brain go the spoils. So when you see who's framing the markets, it's the ones that are actually saying, um, we want to qualify risk as much as possible and typically that business risk, um, but absolutely to Ross's point in terms of reputational risk is factored into that.

Cause that has a monetary value and certainly public sector has a piece of that. Um, but I think the voice to text, um, uh, technology. Is most people don't even read my note and think of it as a high it's. So ubiquitous we've had serious as you say that for a very long time or a bit far from the best, but you know, Alexa devices and, uh, and Google, et cetera, uh, so much so that it's now deployed to endpoints, uh, on, on phones, et cetera.

Um, so, so yeah, no, I, I think the point that I was trying to make and I record. Uh, there's nuance in all of this. I set myself up as a bit of a fall guy with this, but really just to frame the conversation, that's going to C-suite to sign this off. Um, if, if, uh, the organizations that choose not to do this, you don't hear about, they're not making the moods.

Um, and actually, uh, the market is driven by the innovative, um, but, but, but actually it was about allowing the exposure, uh, for, for Ross and Sarah to say, well, actually there are these wider considerations and actually it's about using that map. A to frame how I can contextualize it within a business case, but also how Ross can actually also use the same from an operational consideration perspective.

And Sarah can talk about it from a, from a, from, from a wider security and ethical risk perspective, talking to the same business case, because actually my, my true opinion, isn't just go hell for leather, using all best technology and sack everybody and replace them all the drivers actually it's about saying drive as much efficiency as you can, but what you can do is you can't entirely disregarded that disregard the, um, the, the pop, the possible negative outcomes.

So that'd be my, my thoughts to that and going outside.

Okay. Um, there's some more questions. Go ahead. Sorry.

With the voice to text piece. But I think the other piece for me that, um, is really, really important for this because of things like the Alexa type devices is trying to make sure that we've got that when you talk about something like diversity and inclusion, um, there is just such a massive audience, um, where they've managed to actually just cope with different accents, different languages, different intonations, um, is one of the areas where I think we've established data available.

And that is it's a lot more, um, advanced,

um, the devil in the details.

There are obviously areas where it could go horribly wrong, but all that we can actually just do is look at the benefits that we're going to get in society as a whole, and just try and support those as they move forward. And so we've got anything that you want to add. I'm always going to be most, most squarely focused on.

Do do we have a culture and business model that creates the time to consider these things within required timeframes? Um, very practically because, you know, we've all been in a situation where saying, well, we really didn't. Don't think you should do that. And they go, well, we're going to, we don't think you should go.

We're going to, and then after five rounds of that, it's gone live. Uh, um, and it's just, it's just another hole in the layers, um, of the, um, of the foundations and that that's the biggest challenge. It's. Starting the embedding of accountability far enough up in the tree with sufficient information to, to foster understanding.

Cause I think the biggest disconnect which feeds into this is that, um, the exact, but have the ability to subtly alter the supply chain or, or put in a lever to call hope when you see something that's a strategic risk bubbling up. Um, is there understanding, I think at the moment in these novel technology areas, there's a, there's a feeling of debilitation amongst board members and they're gasping for some kind of abstracted that still substantially related to the technology view of risk.

And I think that's still very much missing and we're trying to wedge, um, re reporting on potential novel technology risk into a financial risk management, whole, a percentage probability and dollars impact, which doesn't actually enable you to manage it, which is where mapping bridges the gap quite effectively at these.

That you can drill down into. Yeah. If I could just add, I mean, um, in terms of, um, public sector and law enforcement, particularly I think, um, the public should be reassured in many ways. Uh, a, a lot of the guidance that we have is probably we disclosed, obviously a lot of conversations been around for our Facebook over the last couple of weeks where they just don't say, say, or share what they're doing with the data.

Whereas, um, w w within policing, you've got something called mopey, which is management of police information, which are published guidelines. It sounds as this is how we manage it. When we're looking at voice to text, we retain the video recording as well as potentially putting out some, some semester data from that Dunham.

Fully recognizing it's not a hundred percent accurate. And it depends on the use case for why you're actually doing that. It might just be a subject matter request and actually saying, well, here's a recording where your name was mentioned or something like that. So you want to pull out that, but equally, if it's for a murder or a account service and conviction, actually you would have humans listening to that video to make sure the transcription is correct, but equally it might be analyzing a whole bunch of video just to identify how, how many people call up to, um, uh, put in a fight police report so that they can attack.

That actually happens. Right? So actually that, that it's, it's it's use case specific. I think that context points, uh, that that roles would making it was very important, but actually with the public subjects, you know, it's actually all, pretty much all laid out there except for certain circumstances around national security that, that that's obviously kept confidential.

Um, public sectors are much more open book in terms of how it's using this technology, but it is materially different than, you know, you can, you can check the audio recording of me talking. 60 seconds and see where it's made a couple of errors and it's much more binary in terms of identifying as correction, but equally as with all these things about why the narrative it's always evolving.

I do think, um, the, uh, voice had sex is so much more mature rather than saying Mr. Liar or not. You know, we recognize that that lying tests don't work the news in six days. Um, but we've got AI. That's kind of talking out to that saying, all right, it's probably like, well, how, how much do we believe that this Dems, you know, how can you prove, prove the positive and exoplanets?

Yeah, it's an interesting area. All right. So we've got some more questions here. Um, I think we don't have long to go, but I'm sure we can, we can extend it because the next session in this window is 1130 anyway. Um, so, uh, for us, so, um, In the public sectors, some recent whistleblowers have highlighted prioritizing profit over safety.

Um, so the only name safety bill is coming, will this change our future? Um, so I mean the, if I take into account the recent sort of Facebook pieces where, um, you know, the whistleblowers basically, um, identified herself and she's, um, talking through some of the power and Humphrey committees at the moment that are looking at the online safety bill.

Um, the thing about AI, and if you're looking at, um, Facebook and all the rest of it is you can imagine how many times say that there's been, um, a video where a child's being bullied. And then this has been shared multiple times across the, the internet. Um, AI is one of the places where we should be able to really, really leverage.

Ability to look at those videos and screen them and say, right, okay, this isn't appropriate. Stop the actual share of these pace. Um, Facebook, themselves have, um, they've, they've been developing a lot of different things in the AI space for this kind of purpose, particularly after COVID. Um, they had a lot of people who were moderators and they were suddenly working at home and they couldn't necessarily view a lot of the videos that Facebook wanted them to determine was this an appropriate video to be on Facebook or not?

So they've been relying a lot more on AI to do a lot of those video screening. Um, and some of the moderators have been, um, working in the office and the moderators have been working at home and sort of, you know, paid during the Corona virus, not safe to work and look at screens. So they've been working a lot in that sector to look at recognizing where there is another instance of that video so that they haven't yet.

10 moderators looking at a video, they, from the one instance it's directed to one moderator and then they can just actually just say, great, okay, remove that video from Facebook. Now, when the online safety bill comes in, um, we are really going to need to rely on some AI and automation to be able to react fast and remove those risks.

And I think that the whistleblowers will really, really help legislation try and actually just make that before from earth a company's ethical responsibility, um, to, to say in some cases you've got to put the public best interest and keep people from harm, um, rather than focus on profit.

So when is the bill coming? I think it's still just going through and the soft part, I know that the Facebook lady was, I was already known the baby say that she was still just talking to some of the committee about it. So I'm not exactly sure, but it was in the, it was in the Queen's speech and it should be coming soon.

But as with all kind of legislation, there's a, there's an awful lot that has to be considered. Sarah. It's going to be a whilst still I think, um, the question with the online safety bill, I think isn't intended. Um, it isn't even squarely focused on the capabilities of the algorithms it's, um, the required due diligence around the online safety bill to make sure on balance it's achieving the aims is where the tie hits the tarmac in terms of people deciding what the benchmarks for harm are and, um, where people refer to for those things that aren't squarely and very specifically written into law.

What we have surrounding the online safety bill is a lot of new legislation brewing as legislation it's dependent upon giving off calm and the secretary of state or home secretary ability to. Um, evolve that definition of home and what the sanctions that would go with a positive judgment of harm would be, um, and where the, um, scope, um, spreads beyond pure illegality, um, to bring things into sanctionable, but not illegal.

Now that space makes a lot of people, very jumpy, because it is only as, um, resistant causing harm. If there's an error or a misjudgment as the quality, um, promptness and responsiveness of your root to redress by the court system or via an appeals process. And I think there's a little bit of nervousness that, um, you know, a lot of the routes to redress in terms of the court system and availability of legal aid and oversight functions.

Going in the opposite direction to being more robust and well-resourced, while we're increasing more oversight, three machines that let's face, it are not in all cases in novel areas, as intelligent as we think they are. So they throw up an awful lot of exceptions. So do, do we have the capacity in that exception management portion of the supply chain?

Similar to what I spoke about in my presentation, that that's my area for. Um, I think there's a whole raft of legislation that's going to come through. And again, we can't look at one country's legislation in isolation because obviously, um, again, this is a global vision. I do think, um, this will evolve all time and there'll be more legislation.

I do think the blanket of anonymity, um, is, is one of the underlying problems with social media in terms of all the hate you see on, on Twitter, it's from trolls that are anonymized. And actually there should be more accountability if people are paying, breaking the law and citing things and making that much more transparent.

When you sign up freedom of speech, this isn't about saying you can't say to somebody on a one-to-one basis, whatever, how do you like, um, but using a platform, uh, I'm I'm minded at the Nicki Minaj, uh, situation was saying, uh, COVID caused my, my, my friends, some of my friends, persons might something to Tesco's to grow, et cetera, and simply the reach.

Pop star just disseminating really dangerous information that might prevent people from taking vaccines. Let's say that, like we, we've got to move that one board and I think actually passing some of that onus on to, uh, very wealthy, um, technology companies, um, is wholly appropriate. And as we've seen with some of the Facebook leaks recently, um, a lot of the most.

Most incorrect information drives traffic. Uh, and actually, um, if you're just seeking profit, then you don't care about them as a profession, but there's a massive societal impact in terms of climate change, et cetera. so what about trade-off? So isn't it Simon, even, even then it's about trade-offs is that you can't have the cure be worse than, than the illness.

And nobody's arguing that the proposed cure. In terms of intent and the, the boundaries within which it's being considered for implementation is worse than the illness. But did you, just from a perspective of my daughter has horrors that she's going to be forced to use real ID for what her interactions with the internet.

And she's going to expose all of her online activities to all of her friendship groups, and that extrapolates out to the rest of her life, where she doesn't want all of her future people she wants to interact with for different reasons to see all of her online activity groups around one ID and sheet.

She thanks to her mother who is, should have given her a name like mine, Sarah Clark, which is security in theory of scarcity, because it's that woman from 24. If you sign such that a clock on the internet, um, I've given her a very unique name. Um, I do, I am not minimizing and you we've been very close to the gnarly nasty edge if child sexual abuse, material proliferation, and that kind of element of online safety.

And there are. Uh, nobody wants to be in the conversation where you're trying to stack up the value with preventing one woman from being abused because she can't, but she needs to hide, hide from her husband versus one child who we need to desperately find because they're at risk and there isn't a sweet spot here.

Um, but we have to make sure that there's not a power in balance between the people who are bringing the arguments on both sides. I certainly think that the Chinese model in terms of you have to show your passport just to get in line that'd the extreme other end and Africa and all countries and making you register since some of the, but the minute you cross the line and you're commencing a law, actual social media com should be compelled to actually share that data where you're breaking a law.

Um, and again, that's what leads sometimes other questions, but I think women Mexican. Okay. This actually a question here was Sarah. Uh, you know, um, how do you make GOC work for continuous development? Yeah, this is a great question. Isn't it? And it's, um, it's surfacing those things, which are, um, the most inhaling, the relevant, inherent risks for the particular development at the time.

There's always some front-ended effort in continuous development to stand up the requirements, um, to, to then integrate. Um, around a solution for that. So it's two things going on. It's to be it's to have the capability, to do that rapid inherent risk assessment, which takes into account the plans, surfacing their inherent risk indicators to look out for red flags, as alerts, to add into what, um, the project manager or scrum master type throws into the mix at every pause to say, have we got anything like this coming up and having somewhere to escalate it to with somebody who has means to understand, to say, actually, you know, if you're not going to sort this in the next sprint, if it's got a chance, high chance of ending up in production, we need to fix this.

We need to pause and fix this because most of the time developers just do not have the wherewithal or the influence to be able to pause rapid change like that. This. Uh, too much focus on, on, on just getting through and just getting done. And we're not blaming developers for, for, um, being a bit fast and loose with access to get something through to the next iteration, if they have no, but we would blame them if they didn't surface, it's going to end up in production.

So it's, it's those, it's the tension between those two things and having somewhere to deliver the conversation into, for someone who cares and B has the means to influence change.

And then there's an additional question here. How do you make a business case for audit or assessment?

That's a really tough one. As I was highlighting there. You need an awful lot. Well, my expert body. So you probably want to engage on, on getting your AI to market versus doing the governance for your AI. Although there seem to be quite a big swathe of people who've been working in AI, in academia who have tipped over into the ethics space.

Um, so making the cases is largely being able to visualize the pipeline and being able to visualize the pipeline that possible requirements is about being able to rapidly understand your, your inherent risks, those things that can be deferred, those things that need to be done though. Those things that need to be done now at depth.

And then you can attach because you have a rough idea how long it takes to kick the tires and who can do it. If you've got. Um, you can then match it to the hours in the day and the warm bodies available. You can do risk, risk management. You can give options to flex. You know, if we haven't got the right people on board and you, and you haven't funded me adequately to do the right kind of, um, due diligence on this, the right kind of assessment, then you know, you're going live with this degree of uncertainty.

You need to underwrite that bet by the insurance, by being sure you've got legal liability limitation, being sure that you're not, you're not going to be paying later if you don't respond though. Um, because it isn't the assurance function or the developer's decision to go live without standing risk. So you bring the potential outcomes into the forebrain.

As opposed to what normally happens, which is somebody brings you the day before it goes live and says, is it secure yet? Um, so yeah, it's the front ending that understanding of potential risk. And it's looking at it in context of the trade offs in terms of the benefit and the business case and putting the two things together.

It's a cost benefit analysis. It's what the business has been always hoping for, for a security it's enabling rapid enough early assessment to get them. Okay, thanks for that. Sarah, a good question here for assignment w what is the consideration of false positives and they impact in the, decision-making making a way to, to use AI, uh, that is, uh, on suicide prevention or making it in the restroom or want them to list?

Yeah, well, uh, well, absolutely. Uh, so, so I think, um, so th I, I think this is about the context, specific nature of things. Um, and the AI is used on CCTV cameras to, um, be able to red flag if something jumps off a bridge. Okay. Um, so we can dispatch on, I like to say, like that's a really healthy use of AI and a false positive as you check the camera and see if it was a coat thrown over, um, I don't have anything, we'll throw that coats, but you know what I mean?

And, and, and clearly a false positive you double-check, um, actually that that's really quite compelling, but clearly, uh, there was a case of a life, extra recognition test done in, in London, um, where there was a lot of pushback and I won't go into too much detail people know about it and can look it up.

Um, whether we catch a consequence of, of actually a false, positive, and look, there was a technology piece. As a police officer was reviewing that. And then they said somebody is a colored be felt, and they would be questioned by police officers saying with it, you know, once it, and actually the accuracy was immature.

So consequently, the false, false positive on that was, uh, somewhat of just having a shopping day in London with a family and then being, uh, that being kind of, um, pride grievously interrupted by the place. You can understand the hope, the sentiment behind it in terms of, so this is a wanted, um, serious criminal.

Um, but equally that false positive, I think it's a really important part. And I think it actually links to what the, the other question in terms of. So that cost benefit analysis, sometimes that cost is actually reputational and actually, um, policing took a hit on that reputational piece in terms of that technology was not mature, but that's why it was a Ted.

Well, it was a test, maybe some of the wider consideration, I mean, learn from and what I can absolutely be. She'll be pleased. Absolutely has both specifically and holistic, um, in every technology program that I've been involved with. Connected to a lot. Um, ethics is a very, um, ethical consideration of an application.

Uh, technology within law enforcement is in every board and actually widely adopted by senior practitioners, uh, as, as an important base. However, now it's, I would say it's more of an art than a science. Um, uh, in as much as there are so many ethics, uh, teams, boards, et cetera, and methodologies around that, they can look at the same problem, come up with the opposing answer.

And that's our classic kind of guest minister piece in terms of you want to get, you know, you're doing a survey, well, what answer do you want to get? And then we'll write the questions. I think there's a, there's a piece with, in terms of the maturing of the ethics process. Um, so I think we're there in terms of recognizing it has a role.

Um, but, but that links into the wider piece. What is that cost? Which ones do we identify that we assess? Because we can be blindsided.

So we don't have a lot of time, but two questions here. Uh, other than I think there's another one for Sarah. Um, let me just read this too. I think these are kind of related. Um, it is incredibly hard and this is from Matthew Adams. Um, it is incredibly hard to develop capability of the delivery team level, where they're not already islands of expertise in the map that allowed teams to develop the skills and experience they need from the inside out.

What approaches might we take the sitting there with skills, uh, specifically the, the risk point. And I think this next question is kind of related as, so can you talk a little bit about the digital competency or lack thereof or many leaders and the risk this may percent once to, oh, I'll, I'll start with the building competency within the teams.

Um, yeah, I, I, I, I feel that pain entirely and I, I very much see. My job has kind of, um, high level operational slash strategic around governance in these, in these areas as being that translation. Um, it's. Doing an upfront assessment, it's where demarcation starts and ends, but who's accountable for surfacing these things in a timely manner and therefore needing the knowledge to do so and needing the time to do so needing the escalation routes to be able to do so.

Is it starts entirely with doing this racing, working out who's responsible, accountable, consulted informed from, from the technical teams through governance teams up to, up to the executive and people at the April procure. It service partners working out where the remit starts and ends and actually making a closely documented case of about the constraints, assumptions, dependencies, risks, and issues as well.

You know, that, you know, are we just about to, to pay half of our specialist team in this, or we've got sales push. That means that they've just going to be able to surface for three months or, um, that w we've got a high profile deliverable and every dev resource is going to be on this. And no one's going to want to talk to you.

Um, if you understand that stuff upfront, you can, you can frame that awareness, knowledge, and engagement pieces of risk of its own. That it's not, again, it's not owned in the governance space and it's not owned in the dead spaces. I, and in the executive space, if you are, if you are requiring change to move at pace without the capability to produce effective oversight, that is a decision and it's a risk to manage, and it's an executive rest of manage.

And that can drive in. If you actually have a piece of paper, you want a wet signature on with us on it, it can sometimes produce the results for training and for a pause for thought. Um, and that's a constructive, um, mechanism of risk, risk management, but you do need somebody to navigate all of those areas with sufficient influence to tie those messages together.

If I get out very briefly, um, uh, I, uh, I, I let a piece of work around technology based standards across policing. And one of the things I did was kind of revisit the, the terms of reference of that, and also the governance structure and, and absolutely to Sarah's point in terms of the rates of particularly the risk of the responsible consultant, uh, The consulted or an expert, an expert practitioner.

And again, this talks to the weather, whether it be security, patching, or service improvement, and a fan service functions that continually evolving, ultimately does it meet the core mission? So if it needed expert knowledge, that was delegated out to the expert panel that says we've gone to version 6.6 6.7 6.8.

Um, and ultimately it's still consistent with the core piece. If it now allows a new, um, a new feature that can be explained in plain language to the responsible owner. Who's not a technologist is obviously much more senior organizationally, but can say, well, now we can do this thing, which is a whole, uh, in addition to what was previously done, you know, to use the example, you know, using voice to text.

But now we can identify if it's honest, well, that's not just. Better quality of voice to Texas. Now we're going to put in a new metric that says, would it be good to say if we think this person's lying based off with some accuracy, that's actually a lot of practitioner. Well, that's a senior, senior responsible owner kind of a level conversation, but you don't need to be technical to talk about that ethical question and the wider piece.

But I do think it's a, it's a, it's a really important part in terms of evolving, um, weight of these consulted, actually having expert practitioners in the loop and having that kind of due diligence is imperative.

Okay. Uh, we're getting reminders here from our, um, background. So interesting questions. Uh, okay. I think we're going to have to wrap up, uh, thanks very much again, Simon, uh, rose and Zara for joining us today. Um, they will be, um, in the networking, uh, horse, uh, if, if I'm not mistaken, uh, so hope we'll see you there, uh, the three of you and, uh, for, for our audience.

So try and catch them there. Um, but you are going to be wrapping up this session now. And the next session in this window will be at 1130 and it's going to be about, uh, the topic of this awareness matters. So join us back then at 1130 and, um, see you at the networking lunch. Thank you very much, everyone.

Thanks everyone. Thanks for.