CRAIG (00:00):

Hi, I'm Craig Smith and this is Eye on AI.

CRAIG (00:13):

This episode is sponsored by [Paperspace](https://www.paperspace.com/), which provides the tools for end-to-end management of machine learning workflows. It comes with dedicated GPUs in the cloud. Check them out at paperspace.com I mentioned in the last episode that I'm working on an AI-enabled audio editing tool. In fact, I'm just the Guinea pig for [Ken Church](https://www.eye-on.ai/podcast-015), a pioneer in NLP who I've had on the podcast before. Ken created the tool as part of his work at [Baidu](http://www.baidu.com/), the Chinese AI giant. It's a work in progress, but I want to thank Ken and Baidu for their efforts. It's making my life a lot easier.

CRAIG (00:57):

This week I talked to [Casimir Wierzynski](https://www.intel.ai/bio/casimir-wierzynski/#gs.wtdw9b), a senior director in Intel's AI products group. Cas talked about his work in privacy, taking me on a tour of the latest strategies that promise to unlock the data necessary to liberate a AI. He talked about hardening encryption against the code-cracking power of quantum computers and about his work in [connectomics](https://en.wikipedia.org/wiki/Connectomics) with salami slicers for the brain that are making it possible to map the neural networks of our minds. I hope you find the conversation as amazing as I did.

MUSIC (01:34):

[STOLEN GIN, SECOND TO THE SUN](https://www.amazon.com/Second-to-the-Sun/dp/B07ZDCSMZC)

CRAIG (01:40):

Can you give a little bit of your background, where you grew up, what kind of a family you came from? I'm always curious about whether people grew up in academic families.

CASIMIR (01:50):

So I'm Casimir Wierzynski, people call me Cas for short. My current role at Intel is in the office of the CTO for the AI products group. I come from a family of humanists. So it's kind of funny that I'm in a tech role now. My mom's an attorney, my dad's a journalist. Actually that journalism background kind of informed some of the privacy work that I've gotten into recently. So I studied electrical engineering in college and ended up on Wall Street for a while as a derivatives trader. That is in a way an act of AI in itself because you know trading is all about decision making under uncertainty and you can think of that as kind of a nice working definition of AI. In a way, I mean, getting machines to do that instead of people. After a few years of of doing that, I kind of craved, you know, going back into AI and kind of studying it for real.

CASIMIR (02:37):

I went back to grad school to get a PhD. It seemed like a really promising model for AI was the human brain itself and I kind of ended up slightly to my surprise, studying neuroscience because if you want to kind of figure out how the brain was really doing things, you had to put on a pair of gloves and start disassembling animals and poke brain cells and see what's really going on in there. There are a lot of theories. I kind of describe it as theories in search of data. So to get the data I recorded from rats brains as I taught them tasks. In the day they would learn and then at night they would sleep and I was trying to understand this connection between learning and sleep and what's the computational function of sleep. And it turns out to be quite a deep topic.

CASIMIR (03:20):

After that I, I kind of got pulled into this really interesting project around neuromorphic engineering.

CASIMIR (03:26):

So this is this idea that you can try to build computer chips that actually mimic the brain. You have parts on the chip that kind of spike and send action potentials to each other just as neurons do. And that kind of led me back into engineering and back into how do you build artificial systems that are intelligent. Now at Intel, my role in the CTO office is a little bit broader in the sense that we're looking for kind of the major trends in AI coming along. And those could be at the level of, you know, new materials, new transistors, you know, what are the physical substrates of computation likely to be to topics around specific algorithms and how are people really going to do the number crunching around AI all the way up to kind of bigger topics. Like what are the ways in which AI systems are going to be deployed in the real world and what are the concerns there? One of those that we identified a couple of years ago was this, and it's still a much of an issue now, is how do you reconcile the fact that these AI systems, you know, they have so much promise, we want to unlock all of this kind of potential of AI and find all, all the, all this good stuff in the data around us. And AI systems are fundamentally shaped by data. But these data are increasingly private and sensitive and you know, how do you, how do you kind of reconcile those two

MUSIC (04:42):

INTERLUDE

CRAIG (04:54):

Before we talk about the data piece, can you talk a little bit about neuromorphic computing and the slicing of brain tissue and photographing with an electron microscope, in which you can actually see neurons and even the

CASIMIR (05:13):

The vesicles,

CRAIG (05:15):

Vesicles captured between the synapses. Can you talk a little bit about that project?

CASIMIR (05:20):

Yeah. So that field is called connectomics. It's kind of a funny name, but it's like you have a genome. How do you kind of do a systematic characterization of some entire biological system? So the prevailing hypothesis in neuroscience is that the way the brain computes is really very much a function of its connectivity. So the connectivity form defines function, right? The way things are connected tells you how things work. But then that kind of begs the next question. Okay. Well, how specifically are things connected in the brain? The rat brain, the human brain, you know, since [Cajal](https://en.wikipedia.org/wiki/Santiago_Ram%C3%B3n_y_Cajal) himself in the late hundreds was doing studies under a microscope and staining specific cells and kind of following where they go, there's clearly been an interest in, in tracking connectivity. But from the point of view of let's say an electrical engineer or a computer architect who actually wants to get a real detailed wiring diagram, like what specifically is connected to what, those data have been really hard to get and certainly hard to do in a systematic way.

CASIMIR (06:21):

So, you know, kind of fast forward to around 2007, and people like [Jeff Lichtman](https://en.wikipedia.org/wiki/Jeff_W._Lichtman) at Harvard developed these techniques, what's like a salami slicer, an automated salami slicer for brain tissue, except these slices are 30 nanometers thick, so would not make a great sandwich. But, this is really the level of resolution that you want to resolve connections in the brain. So, Jeff has this amazing technology for doing the automated slicing. These little slices end up going on a plastic tape, you know, almost like reel to reel tape from a recording studio. And then he passes this tape through this automated electron microscope machine. So you end up with these super high res images of successive slices of brain. So that's step one. Already, that's like a heroic undertaking. But now you're left with this really interesting computational problem.

CASIMIR (07:15):

In principle, all the information about connectivity is in these slices because you can see the outlines of brain cells, the cell membranes, and you have enough resolution to see where two membranes come together, a synaptic bouton they call it. You even have enough resolution to see inside the synapse, the little vesicles that contain the neurotransmitter that kind of pass chemicals from one brain cell to the other. So it's amazing resolution. If you can imagine tracing the outlines of all of these things on one slice. And then on the next slice, again, you trace all the outlines of what you saw. You could kind of connect all of those outlines together and it would start to look like a 3d skeleton of, of the neurons and the glia and all the parts of the brain. I've had the privilege, the real fun as a neuroscientist to help on the computational side of things.

CASIMIR (08:09):

Collaborating with Professor [Nir Shavit](https://en.wikipedia.org/wiki/Nir_Shavit) at MIT. How do you speed this up? Because you know, again, if it takes the age of the universe to do it, then it's not practical. So we kind of set ourselves this goal. If the computer could keep up with the microscope itself, that would be a great threshold because then your data don't kind of get backlogged. You can keep up. So that was a task. I think we may be getting close to that threshold by doing clever things around kind of systems engineering and making full use of all of the goodness in the Intel processors and so on.

CRAIG (08:44):

And how thick are the slices?

CASIMIR (08:47):

It's probably on the order of 20 nanometers, something like that.

CRAIG (08:50):

And how thick is a neuron?

CASIMIR (08:53):

Oh, what's funny, like a neuron is actually huge on that scale. So a neuron's soma, the cell body of a neuron, is typically around 20 microns. So that would be like 20,000 nanometers compared to 20 nanometers.

CRAIG (09:07):

I see. So you build up a thousand layers to see the 3D image of one neuron.

CASIMIR (09:16):

That's right. That's a good way of thinking about this.

CRAIG (09:18):

Yeah. Yeah. And, and is there a visualization then or is this all being done in numbers? I mean, do you create a visualization then when you stack these so that you can see in sort of a computer aided design program and you can look at the the neuron?

CASIMIR (09:38):

You can create these [beautiful visualizations](https://www.pinterest.com/pin/239394536412770440/?lp=true). One thing I think that's kind of underappreciated about the brain is just how tightly packed all of this wiring and brain cells are starting with Cajal. I think that what led him to be able to do so much tracing of neuroanatomy just using staining and a microscope, he figured out this technique. He and [Golgi](https://en.wikipedia.org/wiki/Camillo_Golgi) figured out this technique that only a few neurons would get stained. And so that way you could kind of see because of the empty space between them, you could actually visualize what neurons look like. But they're very tightly packed. A little bit like my, my closet at home where I have my router and wires just kind of jammed in that closet. So the cool thing with the visualizations we can do with connectomics is that you can just say, okay, let me just turn on half the brain cells and see an overall gestalt of how they're connected. But then later on you also have the information in digital form. So you can do all the kind of cool statistics like between this brain area and this brain area, how many brain cells on average does one cell contact and can kind of build up statistics like that, which you need to do science.

CRAIG (10:47):

Yeah. And you were talking about, in the human genome project, that a lot of the research at the beginning was just getting the process down. I know you said that you worked on octopus brains and mouse brains and different parts of the human brain. If you get the process locked down, how long would it take to image an entire human connectome?

CASIMIR (11:16):

Let me try to put some numbers around it. So the most recent project that I saw was to slice a cubic millimeter of brain, and that took about a month. Now that's on a single slicing machine, but it did run more or less 24/7. Again, your reference to the human genome project is spot on because there was this initial kind of protocol for doing sequencing called [Sanger sequencing](https://en.wikipedia.org/wiki/Sanger_sequencing). And there was some effort to get that to work on a single machine reliably. And then once you get it on the single machine, then they kind of ended up filling gymnasiums full of Sanger sequencing machines. So you could imagine one month for a single cubic millimeter. So you know, it kind of goes linearly from that, right? And one day it would be 30 machines and so on. What's interesting is that the bottleneck now is still actually the computational step, not the slicing step.

CASIMIR (12:06):

So that's why we would love to get kind of over this threshold where we can analyze as quickly as it comes off the microscope.

CRAIG (12:13):

I see. Yeah. But, but are you confident that in 10 years that process will be solved efficiently? And then it's just a matter of hardware and time?

CASIMIR (12:26):

I am, yeah. I think mouse brain is definitely in sight in the next decade. You know, the fly, [Drosophila melanogaster](https://en.wikipedia.org/wiki/Drosophila_melanogaster), you know, kind of our friend, the fruit fly has basically been done at this point, at the connectomics level. So we're kind of moving our way up the evolutionary ladder.

CRAIG (12:43):

Yeah, that's fascinating.

MUSIC (12:57):

INTERLUDE

CRAIG (12:57):

Now on the work on privacy, can you, can you describe your work there and the project?

CASIMIR (13:03):

One of the things that motivates me about this whole field of privacy is the fact that there've been cases in human history where denying people's privacy has been, you know, there's a human right around privacy and that's something that motivates me. So my dad came from Poland.

CRAIG (13:19):

When did your family come to the States?

CASIMIR (13:21):

Late fifties. They left Poland in 1945 but first to Europe and then to the U S and later. But I still had cousins and uncles and so on in Poland, during martial law, during the regime. And you know, I remember people had to register their typewriters with the government.

CASIMIR (13:39):

So I, I lead a team right now that specializes in this area, a kind of emerging area called privacy preserving machine learning. And under that privacy preserving machine learning umbrella, there is a set of technologies that can be used to get insights from data without explicitly having to look at the data in detail.

CASIMIR (14:00):

I know that seems a bit counterintuitive and there are some magical cryptographic techniques used to do that, but that's the overall goal. And there's kind of two reasons why you'd want to do that. One is basic security and privacy and making sure that you don't have breaches of data and so on. But another reason is that now you can kind of enable these entirely new applications where - say that you had a group of hospitals that wanted to share their data in some way in order to build a more reliable detector of brain tumors in MRI scans. Statistics is just such that the more data you have, the more accurate you can be. But then clearly there's an issue with sharing patient data. So there's cases where people want to pull data, but for excellent reasons they can't. And so now you, you know, using these privacy preserving techniques, you can unlock that whole space. And it's not just healthcare, it's also in financial services. If you wanted to detect nefarious activity fraud, things like that. Banks clearly want to do this, they clearly want to operate collectively to do that. But then they have these very real privacy concerns around data.

CRAIG (15:05):

Yeah. Can you break that down into the elements of data privacy or privacy preserving software?

CASIMIR (15:14):

So, it's an emerging field, but already there's some core technologies and they're at various stages of readiness for, for the real world. So let's say you want to pool data. The example I just talked about where people want to collectively operate on data without explicitly having to share it. There's techniques called federated learning or multi-party computation. So that's one bucket. Another bucket is in this idea of can you compute on encrypted data? So can one party receive data that's encrypted from somebody and without ever decrypting it, do some kind of math on those data. And then still give an answer to somebody back, even though they never saw the underlying data. So that technique that that's kind of the most magical in my mind, that's called homomorphic encryption. There is another important set of techniques around privacy. So if you look at a dataset and you build some kind of statistical model that that learns about this dataset, you don't want to overlearn in some sense, you don't want to memorize individual details from that data set. You actually want to extract the bigger irregularities out of that. And so differential privacy is a technique that helps you achieve that.

MUSIC (16:30):

CHORD

CRAIG (16:30):

Can we talk about each of those in turn? Maybe starting with federated learning, which is strategy where, where the algorithm, the machine learning model is sent out to places that are holding the data and they're trained on the data in those places. And then the updated model or the, the parts of the model that have been updated are returned to the center. Can you describe that?

CASIMIR (17:02):

Yeah, yeah. It's actually kind of straight forward, although it's cool that it works. So imagine you have several people who hold data and it's private, so we call them the Federation. It sounds a little bit like Star Trek and this is your Federation and then just start with some initial blank slate version of the model and every member of the Federation gets that blank slate. Then each of them on their private data and their private data never leave their premise, but they figure out what adjustments do they need to make to the model in order to have that model work better on their data specifically. So each of them kind of figures out how they would change the model to make it work better for them. They share all those updates with some kind of central coordinator and then this coordinator basically adds all those suggested updates together. Now you get a new candidate model and that new candidate model again gets shared with all the members of the Federation and then you iterate again. They then compute another set of adjustments. They kind of go back and forth over time. What you end up with is a model that will satisfy everyone's data. So it's as if you had kind of worked with the pool dataset, but you never worked with any of the data directly.

CRAIG (18:09):

Yeah. And what you're transferring back and forth is not the entire model, but the weights that have been updated or some other aspect of the model that's changed.

CASIMIR (18:19):

That's right. Yeah. So it's the kind of the parameters of the model and you can even get fancier and say, okay, because some of these models have hundreds and millions of parameters, but in each round, these suggested updates may only touch a small proportion of those parameters. So you'd only really just kind of send the deltas, you know, the changes.

CRAIG (18:35):

Is there any difference in performance between a model trained in a federated way and a model trained on a cohesive data set?

CASIMIR (18:45):

That's a great question. So we've been testing that empirically. Did a study about a year ago with a doctor at the university of Pennsylvania or radiologist there. There's a kind of a standard data set called BraTS, which is a bunch of images. The task is to try to segment brain tumors from MRI images. Those images were collected at different institutions. So one thing you can do is kind of say, okay, well if I pretend like I had done this, I had trained this model in a federated way where I take all the examples from one institution and I put it in one bucket and you know, I can kind of bucketize, I can actually explicitly test this idea of whether training federated gets you close to the same performance as just having all the data. And in that case it worked extremely well. So there are still some interesting research ideas around is. So the challenge happens when different members of the Federation have wildly different data, then this question becomes more acute and you want to test it a little bit more. We've done some research on my team to come up with strategies where you adaptively change the rate at which you do this updating process to adapt the fact that there may be very big differences across institutions.

CRAIG (20:00):

And there's a famous anecdote of computer vision system looking at X-rays to detect fractures. And researchers found that what it was actually looking at were markers on the X-ray that identified which hospital it came from. And some hospitals had a higher rate of fractures. And so the machine learning algorithm was pretty good at predicting fractures. But actually what it was doing was identifying which hospital the scan came from. So in federated, how do you correct for that or how do you identify those kinds of biases?

CASIMIR (20:40):

Yeah. So that's a great reason to do federated learning. Even if you only cared about your own. Let's say you had a single hospital, they feel like they have enough data to kind of serve their own needs. But even there, there's a really good reason to, to kind of expand your dataset by doing federated learning, because then you can make sure that, you know, the model that you have actually generalizes to the actual underlying task and not something spurious. So yeah.

CRAIG (21:14):

And then on homomorphic encryption, which is fascinating, can you describe that? And, and last time we spoke, you used an example of polynomials as the encryption. If you could describe that.

CASIMIR (21:31):

Sure. Yeah. So homomorphic encryption scheme is a, is a way of encrypting numbers or a way of encrypting data, kind of following the Greek etymology. So homomorphic means having the same shape. So when when you move data from the, the un-encrypted world into this encrypted space, the data still kind of have the same shape relative to each other. You're still preserving some structure among the data relative to each other, but you're of course obscuring what the actual data are because it is, you know, encryption. So in particular, like a single number in the plain world in this encrypted world becomes a very high order polynomial. So you remember from high school like polynomials or things like 2x + 3x squared - 2x cubed, except in this case, the powers of X would go all the way up to like let's say 4,096. But you have these very large polynomials in the encrypted world.

CASIMIR (22:27):

And then if you add two numbers in the encrypted world and then bring them back into the real world, you'd get the sum of the two things that you brought over. So it's, it's a way that you can operate in the encrypted world, in mathematical ways that correspond to operations in the real world, except you never actually see the underlying data. So let's make it a kind of concrete example. So a hospital takes a scan, they use their private key to encrypt this scan. Now it's a bunch of polynomials. They send it to some cloud-based radiology service. That radiology service is operating just purely on polynomials. They have no idea what the underlying data are. The polynomials come back to the hospital, the hospital uses it's key now, and only they can unlock this thing and get back the diagnosis that they were looking for.

MUSIC (23:23):

CHORD

CRAIG (23:23):

And then differential privacy. Can you describe that a little?

CASIMIR (23:27):

Sure. So let's think of the example where you have, let's say predictive text on your phone where you know, you start to type a word and then your phone predicts what's the next word? So that kind of prediction model, you take a bunch of text message data and you try to build a model that says, okay, if the previous word Apple, then the next one may be pie. You know, very likely the problem is that if you have in your dataset where people say, you know, my credit card number is, and then the very next thing they'd say is their credit card number. You don't want that level of granularity to show up in your model. Right? So you don't want somebody else typing 'my credit card number is' and then suddenly it pops out your number. So to avoid that, some people call it fuzzing the data or adding a little bit of noise to the training data so that that forces the machine learning process. It'll still learn the overall statistics of English and basic syntax, but it won't have enough statistical power to see these tiny little details like individual people's information. That's an example of differential privacy.

CRAIG (24:31):

Yeah. And so if you fuzz the data or you introduce too much noise, then the model doesn't work. Right. So there is some way of determining how much noise to put into the data to protect the privacy but allow that data to work.

CASIMIR (24:50):

That's right. Yeah. So there's probably two or three dozen papers out there on aspects of how do you get the most utility out of some model while still preserving the privacy that you need. So there is going to be a bit of a trade-off between privacy and utility in this space. Although I think in practice people are finding that there is a sweet spot in a sense and actually some amount of fuzzing can make the model better because one of the overall goals of machine learning is: I've only looked at a subset of the data, but I really hope that the model that I build applies to data I've never seen before. So this is this idea of generalization, that concept of generalization is completely in line with this idea of not overly memorizing different parts of your data set because those are, those are not germane to the task that you're training for.

CRAIG (25:43):

Right. And a lot of people don't realize that machine learning models can actually memorize or or hold data in the hidden layers that can be queried if you know how to query and extracted after the training. There was a study about exactly that, retrieving social security numbers or credit card numbers and other identifying features that had been in the trading data set and even after the training data set is removed, that information was retained in the model. Is that right?

CASIMIR (26:22):

Yeah, so this is called an extraction attack and there's actually a kind of a nice confluence here with homomorphic encryption in the sense that this, this kind of attack that you just described, you can think of two scenarios. One is where the attacker actually has access to the model where they can kind of see all parameters of the model and how it was built and so on. That's called a white box attack. And then then there's another version of this where the attacker can, can use the model in the sense that they can send stuff to it and get answers back, but they can't look inside to see how it was built. And extraction attacks are possible in both of those scenarios, but they're a lot easier if you actually have access to the details of the model. So homomorphic encryption can actually be a way to protect the details of the model. The example that I gave with homomorphic encryption before was where I was trying to protect the privacy of the data that I fed to the model. But you could also turn it around, you could actually encrypt the model and thereby protect the confidentiality of the model itself.

CRAIG (27:29):

Yeah. And all three of these sound pretty powerful. Is there a reason why you wouldn't want to just choose one as opposed to blending them or stacking them?

CASIMIR (27:40):

Yeah, so differential privacy actually addresses a slightly different problem than homomorphic encryption in the sense that differential privacy addresses the ability to tie a specific set of information to a specific individual. Whereas homomorphic encryption and federated learning are more about confidentiality. And there, they're kind of defining it as operating on data but not seeing what the underlying data are. So those are subtly different but they are actually kind of different problems and we just now went through an example where you might want to do both in the sense that you might want to use homomorphic encryption to prevent someone training data to see what the underlying data are. But then you'd want to use differential privacy to make sure that that model hadn't learned details of the training set. They are slightly different problems.

MUSIC (28:49):

INTERLUDE

CRAIG (28:49):

From a layman's point of view, this sounds like a little bit of overkill. I mean are there really people out there with the level of sophistication required to query machine learning models, for example, to extract data? Is this more about researchers just being doubly sure that the systems they are building are secure?

CASIMIR (29:20):

Well I think of it as kind of like the Robert Frost poem where you know, good fences make good neighbors. If we can make nice mathematical guarantees that I've done this machine learning operation and you cannot learn anything about the data, the amount that you can learn about individuals and the data is kind of mathematically bounded. I feel like this is the right thing to do just in the that when you go to the supermarket and you can see the list of ingredients on the box of cereal, right? That gives confidence that now I can go out and buy any box of cereal and know that it's going to have certain properties. I think this is the kind of foundational work that AI will need in order to kind of, you know, to kind of grow the overall AI market

CRAIG (30:00):

And are there developing standards around this so exactly as you described so that people in hospitals, when they sign a release form that their data can be used, that there'll be, you know, a level three security protocol and that you look that up and it's, you know, a combination of homomorphic computing and differential privacy and some, some other things. Is it becoming standardized in that way or would you think it will become standardized?

CASIMIR (30:32):

I think aspects of it will be, so my prediction, my vision, and in some ways my hope is that, remember in the early days of the web that you would go, you know, HTTP, you know amazon.com you'd fill in some stuff, you'd fill in your credit card number. And then after a while people said, Hey, you know what, like we probably shouldn't be sending credit card numbers around. And so then they, for certain very, you know, sensitive things, we'll have this thing called HTTPS you know, and that's going to be like kind of the secure web interface. And then people gradually got trained to say, okay, I'm going to look for the lock on the browser. But it was only just a few pages that would be guarded that way. And then after a while people said, Hey, if you can kind of secure this one page, why don't you just secure all the pages?

CASIMIR (31:11):

So, everything now is like HTTPS, right? So I feel like for machine learning, the, the idea that people are going to be operating on raw data is just going to seem quaint and weird and slightly indecent. So to get to that point of HTTPS, you need a couple things. You need to make all these technologies more usable, right? So that the people who are doing the data science and so on don't have to worry about how big the polynomials have to be in some weird space. And you also need some level of interoperability and industry consensus around around the underlying technologies. So that is starting to happen for some things like homomorphic encryption, people on my team and are working with other industrial partners to work with the right standards bodies to get that process started, to kind of standardize aspects of homomorphic encryption. There is already efforts in other standards bodies around federated learning. So I think this will kind of come together.

MUSIC (32:07):

CHORD

CRAIG (32:14):

Intel's a chip maker, it's a hardware company. How much of this is going to reside on the hardware on the chip or is this research to enable solutions that, that Intel can participate in in other ways? Yeah.

CASIMIR (32:31):

So one thing that we haven't talked about yet is the fact that some of these techniques require extra compute. They are computationally intensive. Intel has seen this situation before in the early two thousands when encryption became much more commonplace or there was a kind of an encryption standard called [AES](https://en.wikipedia.org/wiki/Advanced_Encryption_Standard), people were using it a lot. We said, Hey, you know what? Let's actually, let's add a new instruction to the, you know, Intel processor line to accelerate this particular part of the encryption scheme. Just to kind of speed that up. So we've, we've done that before and I feel like for some of these protocols we will probably do that again, where we'll need to kind of provide hardware support to speed up these very specific calculations.

CRAIG (33:14):

Yeah. I know you're, you're not a chip designer, but there are these part of the chip or a protocol within the chip, these trusted execution environments. Is this related to that or is that a completely separate function in the privacy space?

CASIMIR (33:32):

I think I consider it another kind of paint on the palette, so to speak, for a privacy preserving machine learning. So the technology that you're referring to, these, these trusted execution environments are ways that you can, for example, dedicate a certain amount of memory that you're working with on your computer to say, okay, this memory is going to stay encrypted. Whenever the processor needs to access that memory, it's going to access it only in its encrypted form. And then once it reaches the inner sanctum of the processor, only then are we going to decrypt it, do some kind of operation and then very quickly reencrypt it. So there's a way to speed up that process and make it much more efficient. That's my non chip designer version of what a trusted execution environment is. So that's definitely part of the, the toolkit that we can use.

CRAIG (34:18):

Right, right. And, and the, the bit where it's un-encrypted so the calculation can take place and then reencrypt it presumably that could remain encrypted using homomorphic encryption. Is that right?

CASIMIR (34:32):

You could, yeah. You actually, you could use both, a kind of a belt and suspenders approach when you have encryption inside one of these trusted enclaves. Yeah. let's say two different parties have intellectual property that they want to protect. One party owns a model and then then the other party has sensitive data that needs to operate in that model. You could use homomorphic encryption to protect the patient scan, let's say, and then you could use the enclave to kind of encrypt the model. So you have now you're kind of protecting two different parties at the same time.

CRAIG (35:04):

Yeah. There's been a lot written about the advent of quantum computing and how that will obsolete all of the encryption protocols that exist because of the power of the quantum computer. How does that relate to these three different buckets that you refer to? Am I wrong on that?

CASIMIR (35:30):

No. The crypto community is looking very closely at quantum computers and how to handle that. There's actually a process at the [NIST](https://www.nist.gov/) used to be known as the Bureau of Standards where they are looking at what would be the recommended new cryptography systems that people should use to make them so-called post quantum or kind of quantum resistant. The cryptography techniques that I've been talking about so far are post quantum already, so you're already kind of safe from ...

CRAIG (35:57):

All three? Differential and homomorphic encryption and federated learning.

CASIMIR (36:03):

So of the three that you just mentioned, strictly speaking only homomorphic encryption is an encryption scheme. Yeah, so that one is the one with the kind of the polynomials that we were talking about. Yeah. This refers to a family of cryptography schemes called lattice based crypto schemes and some of the, those are post quantum schemes and actually there are people at Intel who are actively suggesting to NIST what should be the next adopted standard. Some of those are a lattice-based as well.

MUSIC (36:35):

CHORD

CRAIG (36:36):

You were talking at the beginning about how unlocking data can lead to all kinds of new applications and one of the obstacles right now is privacy and security. Presumably once that's solved then all of these new and wonderful things can happen. One of the things that's being talked about from a consumer point of view with regard to data privacy and data protection is the ability to control your personal data and receive remuneration for its use. Is that part of your world at all? It's looking at how strategies can be applied to personal data and then different ways that individuals could contribute data or sign releases on data and be compensated.

CASIMIR (37:32):

Yeah, we definitely think about these technologies. They exist in a world subject to economic laws, right? So we definitely think about the kinds of applications that you're discussing. For example, federated learning could be a way that people who have private data silos could monetize those data without explicitly sharing them with anyone.

CASIMIR (37:52):

And that's, that's a very interesting possibility because then then it creates the markets and kind of, I'm a former trader, right? So I love market mechanisms around allocation of resources and I think that would be a fantastic development for the field.

CRAIG (38:05):

Yeah. I had a conversation with Dawn Song from Berkeley about all of this and she's working on on solutions of for allowing users to control and monetize their data and also to to identify and track how much an individual's data actually contributes to the training of a model. And my question was, well, how much from an individual's point of view Is that really worth, because certainly Mark Zuckerberg and Jeff Bezos are two of the world's wealthiest men because they figured out that they can collect all of our data and monetize it. But when you split that data up in the individual pieces, it's tiny. The ability to monetize that is tiny. So is there any, do you have any thoughts about that? Even one thought that I had on a, on a monthly or annual basis, it's insignificant, but maybe over the course of a lifetime. Then when you reach 65 there's this bucket of money to help you through retirement, which is all of the accumulated money from the use of your data through your lifetime. Or one thing that Dawn talked about is you could have interest groups that pool their data revenue for various causes. And I'm just curious whether you've thought about any of this stuff.

CASIMIR (39:36):

So the context of my thoughts has been lately mostly around kind of immediate customer problems that we're seeing. So we haven't gotten to the level of kind of individuals whether they should sell their individual data or not. You know there are already kind of data sharing agreements in place where again, looking at health care, like you know, a pharma company wants data from a hospital and then they get armies of lawyers together and they come up with some very large check and it's a pretty complicated process. I think to facilitate those kinds of business to business type interactions would be a really great place to start. I know [Jaron Lanier](https://en.wikipedia.org/wiki/Jaron_Lanier) has also been [in the New York Times](https://nyti.ms/30d0B8P) about individuals should sell their data. I think that's actually a pretty complicated topic. There's plenty of a commercially and societaly important business to business cases that we'd like to work on sooner.

CRAIG (40:35):

That's it for this week's podcast. I want to thank Cas for his time. If you want to learn more about Cas' work, you can find a transcript of this episode on our website, Eye on AI. Also check out Paperspace at paperspace.com. They have a terrific blog that tracks the latest AI trends and are doing amazing work. We love to hear from listeners, so feel free to contact us with comments or suggestions.

CRAIG (41:09):

The singularity may not be near, but AI is about to change your world, so pay attention