Mathieu Glaude (00:00.00)
So Scott, it's been, I was just looking, it's been about three years since we last did a podcast together, which is kind of crazy. I think the last time we did this was in late 2022. And when I was reviewing the discussion that we had had, you had said something at that point, which had struck with me at that point. And I think led in nicely to the conversation around governance, but you said "*I can cryptographically sign a lie.*"

And so I think that statement altogether kind of cuts to the heart of what you're trying to solve, what we're all trying to solve. And so before we dive into any specifics of any projects in particular and advancements that have happened over the past few years, since our last conversation, can you maybe restate for our listeners, why cryptography alone isn't enough?

Scott Perry (00:56.843)
Right. So well, cryptography helps a lot. And first of all, thank you, Mathieu, for letting me join. I mean, you're the velvet voice of digital identity. So it's just my pleasure to be here. So cryptography can help make valid claims and, based on the nature of private and public keys. However, what you're making a claim about isn't solved necessarily by cryptography. And so what you can do, is, when you make a claim, as long as you have control of your private key, which is very key in the cryptography field, then others can validate that it came from you based on the private key pair that's attached to it. And so you can make that claim. And the other claim that you can make is that since the time that you've made the claim, there ha it hasn't been altered, because you can do a cryptographic proof to match what you're seeing today based on what was derived by cryptography.

Mathieu Glaude (02:07.10)
What would that mean? What would that mean, Scott, for just an everyday user of the Internet, maybe not being quite familiar with public private key cryptography? Like, how does that apply to just everyday use of, you know, the Internet?

Scott Perry (02:21.22)
Right. And so, you know, there's a lot of things happening in the background when you're using the Internet. There is encryption going on in transit. A lot of your data, especially passwords as such, are encrypted at rest. And so you don't really have to know as much about it. However, when we make transactions and make claims as individuals, you know, and things that are tied to me making a claim, that hasn't been solved yet.

We need to have credentials that would allow me to sign my container of claims out in the marketplace. So when people are saying, is cryptography around? When you make a payment, certainly all of the transactions as such are encrypted and encryption uses the private and public key pairs that you have. But the requirement really around cryptography is the control of a secret key. Now, the public is going to learn about that, but not necessarily have to worry about the underpinning components. The private keys will be buried inside smart wallets and you'll get enough information when you're using these wallets to get educated on the protection mechanisms that are required.

Mathieu Glaude (03:56.06)
So we basically have the technical tools to be able to, let's just say, digitally sign things, whether we're doing a post on social media, whether we want to say that I produced a piece of content, whatever the use case is, is that we have the technical tools to be able to stamp something and make sure that once it's stamped, it can't be altered, I guess, from that point onwards. But just that stamping is not enough to build trust, I guess, is where we're getting at.

Scott Perry (04:27.16)
Right, people can alter it, but when you prove it, you know, it would identify that it was altered after the time that it was signed. So that's the key thing. People can manipulate it. It's just that if you can go to the cryptographic proof, then you get the assurance that cryptography provides.

Mathieu Glaude (04:51.03)
And it seems like since we last recorded the podcast a few years ago, there's been mass adoption. I think the monthly active users of all these different AI tools has just ballooned. We're seeing the valuations of these companies having ballooned as well. But what is happening is there's more and more content or more and more claims that are coming from non-humans or perhaps just from these different AI systems.

Has the landscape changed over the past few years? It seems like it hasn't changed the types of problems we're trying to solve, but it's just reinforced the importance or the need to solve these problems.

Scott Perry (05:30.15)
Well, certainly the landscape has changed because of AI and has accelerated the need to have cryptography in any solution. You know, the typical user looks at CAPTCHA with the motorcycles and the park and the street lights and all those things. Well, AI can manipulate that and can demonstrate that it can pass these tests. So we need new tests that involve cryptography because AI cannot break the private key.

Certainly post-quantum cryptography is addressing issues around the strength of private and public keys, but AI by itself can't break cryptography and the security of a private key and the attachment of that to a public key.

And so, we're good around using all the cryptography as long as we advance ourselves to new types of cryptographic algorithms which are being developed today, sponsored, driven mostly by the National Institute of Standards and Technology. NIST is driving a lot of those new algorithms and hopefully they will be applied to a lot of the activities that we'll be doing in the next few years.

Mathieu Glaude (06:54.22)
So one of the projects that you started looking at in the past few years is the C2PA. And we've had conversations about that on this podcast before. I think we had Eric Scoutin on to talk about

that a little bit, definitely over a year ago or so. But it seems that one of the biggest issues that people are trying to solve online is just, I able to trust a piece of content? and that that's, that's a large question, but you start to get some sub questions of like, how do I know if this piece of content is AI generated or human generated?, or even how do I know that this piece of content is actually coming from the source and wasn't altered or wasn't deep faked? And so it seems like this type of problem has become a widespread problem for basically everyone.

My parents, anyone that uses the internet is faced with these problems of they don't really know how to interpret content that's being presented to them. And there's maybe been like a loss of trust definitely around that because you don't really know what you're looking at. And if it's truthful in whatever sense truthful means, means to you.

So this C2PA project, you got involved with within the past few years has kind of aimed to solve some of these problems both and maybe go deeper into this, but both from, products perspective. And I just want to try to tie this back to how do we build trust in what software is or hardware is producing by using some of these technical cryptographic implementations and then why those alone aren't enough for the product side.

But then I think this could be a very large conversation, but then how that flows to the end user, to the person, and then to the individual content creator. So maybe we could start by tying back and maybe giving a bit of a background on like what is the C2PA? What are the different elements of that? Why you got involved with it and then how it's been implementing some of these technical protocols to try to help solve these trust problems when it comes to the provenance of digital assets.

Scott Perry (09:05.15)
Right. I mean, a similar kind of theme came up a number of years ago when people didn't really understand or know, what they were eating. You know, so what advanced is requirements to put nutrition labels on the food that we eat so that we had a clear understanding of all of the ingredients, as well as some of the processes and some of the calorie counts and other types of metrics that we needed to know so that when we ate something, we at least had full knowledge of the things that we're eating.

And so that, concept was applied to digital objects because at this point, the advancement of AI and all of these tools, we do not as humans can decipher whether something came from AI or it came from another product or such. And so we don't have that information. We have to get transparency at the point of the creation of the asset.

And so what the C2BA is, it's a coalition of all of the largest tech firms in the world. So it's not like they're individual firms are developing their own proprietary solutions. They decided, we're going to combine our efforts and come up with a standard solution like wifi and USB and these things, which we can all plug into and come up with a standard to create an immutable ledger attached cryptographically to every digital object.

So in essence, you're creating almost like a blockchain that's immutable, attached to every digital object, which creates a canvas of how that object was created. And it can also act as a landscape and a canvas for others to make claims on top of it. So the C2PA is creating the base layer and we are working with generator products.

Scott Perry (11:25.18)
The reason why we call it generator products is they originate the generation of digital objects, whether it is images, videos, music, anything that can be presented in digital form, are applying the C2PA standard to frame, that canvas of a digital ledger attached immutably to that digital object. And at times, there are concerns that you could take that ledger away. But if you put fingerprints and such and store these records in the cloud, you can maintain that continuity because we need that. And now there's legislation, especially in California, that's dictating that all digital objects have that ledger or that set of provenance and authenticity information available.

Now, the C2PA is focusing solely on the products that create these and that can validate that those products actually, had generated these manifest accurately. We're not dealing with in the C2PA around claims made by people and organizations. That's handled by the Creator Assertions Working Group, which has spun off and now is hosted by the Decentralized Identity Foundation (DIF). C2PA wanted to focus only on products and that's really what my involvement got in is they wanted to create a conformance program of all of the product manufacturers that wanted to assert that they met the standards and did it in a secure way.

And so they have to apply to the C2PA's conformance program with their products and sign legal agreements and assert that they are meeting the standard, as well as demonstrate that they have implemented their solution securely because we also have two levels of assurance, One, they can assert that it is a higher and more assured level of implementation.

Mathieu Glaude (13:46.21)
So from someone who comes from the audit world and has done a lot of work with technology, internet-based companies, you've worked with tons of certificate authorities throughout the years to ensure that they were conforming to specific requirements. How has what you're describing now here with the C2PA and at least the base canvas at the provenance assertions of the origination of digital assets, like, what have you been able to transpose from your world of audit within the certificate authority world or other space? Like what applies to that? Cause I feel like often in our space and I don't think it's the same thing with the C2PA, but often people just try to reinvent the wheel when things could, you know, be taken from existing spaces and applied to something new.

I'm assuming there's a lot of overlap from the traditional space that you're operating in, towards this space now where really we're trying to create these nutrition labels. I really like that analogy. I think it speaks very well to what we're trying to do. We want to know what we're consuming. Therefore, we need to be able to read a nutrition label that we trust. But what have you been able to bring from your prior world, still current world, to this new space?

Scott Perry (15:05.20)
Well, almost all of it actually, because what the C2BA decided to do is in order to sign those manifests, the products like cameras, smartphones, they have to get a certification authority issued X509 certificate to do it. And it applies very well. And so the C2BA created a certificate policy, which is public and available and certification authorities are also members or such applicants within the conformance program. And they agree to sign legal agreements and they issue these C2PA specific claims signing certificates over to these generator products and in that way, the conformance program has control over the certification authorities and the products because those products can't get these X509 certificates from certificate certification authorities that are not in the program.

And the certification authorities can't issue these signing certificates to generator products that are not listed on the C2PA conformance conforming products list. So in that way, we have a bit of a tight ecosystem regarding ensuring that at least folks that are participating are in the program and following the requirements of the program.

Mathieu Glaude (16:46.01)
So are you seeing a lot of the existing certificate providers for DNS servers or web domains or even software, starting to see, there's a new opportunity for me maybe to have a new line of business within this new content nutrition label space where I could maybe sell different types of certificates to generator products. So for them, is it kind of just a new product line for them that just they're able to leverage a lot of their existing process and rigorness and everything to be able to just serve this new type of customer.

Scott Perry (17:23.04)
Absolutely. So, as of today, I can report there are three types of certification authorities within the program. They don't have to all be public CAs as those that are protecting Web certificates. So we do have public CAs and we just added DigiCert to our list along with SSL.com, which was the first public CA that joined our program. But we also have what I would call self-serving certification authorities. And they come in two types. One is very robust enterprise-wide certification authorities. Those like Google. Google knows how to run a CA quite well and has lots of products. And they'll be serving their products in a demonstrable way.

And then you have kind of the mom and pops that have one application that, you know, generates manifests and they want it to be able to serve themselves. And those may go under a lot more scrutiny because it does take quite a bit of rigor to be a trustworthy certification authority and meet the rigorous requirements of our certificate policy. And so, we do ask more requirements of all of our CAs and sometimes the brand new ones or the ones that are mom and pop don't know the kind of rigor that, that the public CAs have to go through as they, satisfy web trust requirements or, or those in the, the browser root programs. So, I'd say if you're wondering whether you should be a CA or not, unless you're an enterprise grade company that's issuing all these generator products, you probably want to get your certs from a public CA.

Mathieu Glaude (19:29.16)
So there's this search policy for the CAs who are, I guess, on a trusted list that the C2PA maintains. And then that gives them the authority to issue these X509 certificates to products or to generator products as you're referring to them. What is the work involved for a product to get one of these X509 certificates? What do they need to be able to demonstrate?

Scott Perry (19:57.09)
So if you're a generator product in the marketplace, first of all, you should have clear understanding of the C2PA content credential specification. And so the conformance program is starting at release 2.2, which is the current release. And we've been working with an interim solution up until then, and that will be sunsetted by the end of this calendar year.

So you better be looking at, if you want to be in the content provenance space as a generator product, you better be looking at the specification. And I think in later versions of the conformance program, we may do more attestation that you're meeting the specification, but right now, you know, the program is just getting started and the first release of the program just requires that they are asserting they're meeting it, that they sign a legal agreement. And eventually we do have implementation security requirements which are publicly posted that have varying degrees of control based on whether you want to assert yourself at a lower level of assurance or a higher level of assurance.

Higher levels of assurance use innovative attestation to validate, that you're continuously using mechanisms that we require, such as keeping your software patches up to date, and you could communicate that with certification authorities through attestation communication. And then, dynamically, they will give you certificates on an updated basis. Certainly, there will be more frequency of getting these certificates if you're at a higher level of assurance. And so you need to demonstrate from an architecture standpoint. We have a template and you have to fill it out to demonstrate how you have architected not only your application, but all of the pieces of the application that you need to apply a digital credential against it in signing cert, whether you're using even an outside signing organization to do it, that becomes part of what we call the target of evaluation. And so we're asking applicants to document what the environment is that is part of their generator product. And we're asking them to adhere to the requirements that we have for these levels of assurance.

Mathieu Glaude (22:52.21)
What are some generator products that have already completed the conformance program and have gotten these X509 certificates issued to them? I know we could talk about hardware organizations, software organizations. So I think it would be interesting to know who's already adopted this and is already on board, who are some examples. And then, how do you see this evolving maybe as a secondary question? Like what are some types of organizations that you think maybe are not there now, but would benefit greatly or would be the next ones to come on board and adopt this, whether it's hardware or software providers, platforms, creative tools.

There may be some different types of generator products that we're not even thinking about that could benefit from this. So we'd be interested to know kind of in terms of adoption, who's there now and where do you see it going?

Scott Perry (23:48.11)
Right, so what we've seen so far is a lot of the smartphone companies have come up early. And it's great when you're developing a conformance program and you want people to join. It's great when Google is the first company that goes whole hog in. And they have now 10 products, including the Google Pixel 10.

And so if you take a picture of the Google Pixel 10, it will create a manifest automtically. You don't even have to know it's happening, but you can create, you know, have that and create images that have the CR logo, which reflects that it was conformant with the C2PA. We also have, you know, smartphones from Vivo and Xiaomi. They're from China and you can see that the C2BA program is not just limited to the United States. We have applicants from all over the world.

And so we anticipate that there's a lot of products that create digital images, such as cameras, sophisticated cameras, not necessarily the smaller ones, but cameras that are used in the field for the press industry so that we, when someone takes a picture of a noted figure, they can automatically ensure that that picture, when it is taken, has provenance information attached to it. But I anticipate there'll be, the music industry is looking into a lot of products that when they create music to automatically create that provenance data, as well as video and films.

I'd say, you know, as it moves forward and the technology gets advanced to more manufacturers, then we will see innovations come as we go. It's really what I've learned out of this process. And now I am the administrator of the program. I'm finding that we need to get more of this technology in the hands of consumers.

Once you do that, then the industry comes up with very innovative ways. There's certainly a lot of need in the marketplace for certain industries like insurance, and in the press and in marketing for brand management, because there's a lot of manipulation being done in the marketplace over actors and insurance fraud claims and, a lot that can be addressed by having this provenance data attached to these pictures and other images.

Mathieu Glaude (26:44.23)
So before we get to consumers, because that's a super interesting topic and I do want to cover that. We're talking about generator products. You're talking about the mobile phone providers. They're doing this. The cameras, the platforms have already implemented this. The end user is able to see this nutrition label on a piece of content through that content credential badge.

One of the things that in my world working a lot with the verifiable credential standard is that verifiable credentials are basically a store of claims. You could call it a, I think Timothy Ruff, has a nice blog calling it, comparing it more to containers. If you're feeling that the verifiable

credential term is, is maybe misleading, but it's basically a container of claims, but you want to make sure that you're really tying it to the authority or to the system of record. And what we're doing more and more is that we're seeing how we could have links to evidence within the credential metadata. So you have attributes that are signed, but often it's the starting point to begin an engagement, but often people still need more information or need to have proofs of the evidence or just even supporting documents that may be tied to this thing altogether.

You mentioned an interesting use case with insurance companies. Do you see the C2PA stack being useful for enterprises that struggle with the forgery of documents that they issue, whether it's land titles or deeds or just, insurance, coverage or whatever, whatever goes into documents that they send to their customers.

Does the C2PA fit in there? Cause we're talking about it from, I guess we started from, on the internet, want to make sure I could trust content, but from a more of like an enterprise and B2B or even B2C within the enterprise is the C2PA a viable stack for them to really increase the assurance of documents that they're emitting that they want to make sure that they're not altered or changed after their emission.

Scott Perry (28:58.04)
Well, absolutely. I think it affects all industries that need confidence about a digital object. I mean, we've lived with paper for since the beginning of a man with a pencil, so to speak. And so but this actually this technology adds more assurance than paper. And so there was a comment I had heard in the insurance industry that if, let's say I take a picture of my beautiful car, but I use AI to manipulate my car picture showing a major dent. And it was told to me that these pictures have been submitted to insurance companies that are overloaded with claims management and they were just paying claims of up to $10,000 for these manipulated photos.

And that's real money at this point. So, I do know that one of the C2PA founding members, TruPic, has been very active in the insurance industry and promoting this technology to advance the reduction of fraud. We have title insurance in the marketplace, and all of it is, why do I have title insurance? Because there are fraudulent claims on certain things.

And so we need more trust in the information that we receive. And we need more trust on who we're interacting with. And that's, I think, a separate topic we'll get into in part of this call.

Mathieu Glaude (30:37.13)
Yeah, so you could imagine you've just described a very interesting use case to reduce the risk for the insurance company and reduce the payouts because they're able to really identify fraudulent claims if folks are submitting digitally altered images and stuff like that. But you could also imagine the insurance company that is issuing a policy or issuing whatever from their standpoint, they could also sign stuff that they're issuing that then if the person receiving the policy wants to present it to any third party, they're still able to get that nutrition label or stamp on it to know that it actually came from them. So there's a lot of similarities with what a verifiable

credential is supposed to do as well. Like is it really just ensuring that you have that provenance right from the generation of that document altogether?

Scott Perry (31:27.13)
Right, one of the things, the connection between verifiable credentials and the C2PA come with organizational and an individual attribution. So I mentioned the C2PA was very focused on X509 certificates, but in the Creator Assertions Working Group, you can use an X509 content signing and an SMIME at this point. But we are opening up the standard to address verifiable credentials because I do see in the marketplace, there are a number of initiatives that are taking place both in Europe and within the states of the United States to get signing privileges in the form of a verifiable credential in the hands of consumers.

And once everybody has a identification credential that that's tied to them, then they can use that on top of the C2PA manifest to assert that, yes, this is my picture or, I take claim to this, certainly there has to be investigation work around ownership. Cause just making the claim doesn't mean I own it. I can assert. So it's really assertions that I'm making.

And so this will build out the fabric of a new trust assurance mechanism, which includes provenance data from the products from people, as well as the legal rights associated with digital objects. And the work on top of the C2PA and the cog is happening globally with the JPEG Trust organization compounding on an ISO standard they've created to create intellectual property rights and copyrights associated with digital objects. So you can see the entire fabric of more assurance over these digital objects starting to take place and in the future will be depending on those layers of assertions about claims made to these objects.

Mathieu Glaude (33:52.13)
So when you talk about different types of assertions being made into these objects, so if we move beyond the generator products that are assigning things, there may be different types of assertions that are very contextual to a specific ecosystem or a specific industry or just to a specific person.

So is the whole idea, and when you mentioned the Creator Assertions Working Group, is the idea of how do you get the actual individual creators to start making assertions within these same nutrition labels? So you basically have the container, which is the nutrition label. It contains some signed assertions by parties who are being governed within the C2PA.

But then there may be individual creators that aren't going to be governed by the C2PA because what they're trying to say is none of the business of the C2PA type of thing, but it may be valuable for them to say something and put something within this content credential. Is that the whole idea of you're able to expand what you already have to just have very contextual attestations now find themselves within these nutritional kind of labels or elements to know what we're eating and have even more context about, when we should eat it? when we shouldn't eat it? or whatever else that we want to see.

Scott Perry (35:18.00)
Well, we want more information. So what the C2PA has created, they have their own assertions delivered to generator products, and they are called created assertions. They're created at the time of the creation of the object. The C2PA specification leaves aside containers, I guess you could say it, what they call gathered assertions can be put in, gathered over the lifetime of its life cycle.

And those claims can be made by individuals, or can be made by organizations. And so there are two flavors that we're working on in the Creator Research Working Group. One is the identity. Who's making these claims, whether it's organizations, people and such, and then what kind of claims would they make?

A lot of times, that's going to be added by industry. So we've been working very closely with the entertainment industry. They have a lot of identifiers that identify individual objects, movies and pictures and books and all these types of things. And they've been established by a number of these, what I call metadata organizations that are classifying individual identifiers for a variety of things.

So, I've been working with a group and there's a number of identifiers that can be used, you know, for works. I can be an actor, and it could be tied to me personally as the actor, or there may be different representations of me, maybe in a cartoon or I may be in a video game. And so how do I affix my different identifiers into these works that are digital that can be attached to me so I can get paid? So we're looking at mechanisms that could justify money flow. And that's why there's a lot of industries that are already interested and will be interested because we're creating really the fabric for monetary transactions to take place.

Mathieu Glaude (37:49.13)
And these third party, call it governing bodies that are the authorities or are respected within their space is kind of outside of the scope of governance of the C2PA. So I guess like C2PA is not going to say who could be, who is an actor and who's not, or who's a real estate agent and who's not, whatever example I want to use.

So is the idea that you need to have these third party governing bodies who manage their own governance and their own conformance within their own ecosystem of participants, whether or not they issue credentials or the opportunity for their members to digitally sign stuff is kind of up to them. But there is another route of trust there that if someone's able to prove that they're part of X organization or they have Y accreditation or whatever, they could then make an assertion within a piece of content, which just adds to the richness of it, but is also backed by the governance of their related field or ecosystem.

So how does the C2PA interact with that? How open is that going to be for, you know, cause it's, it's closed for the generator products for good reasons, but it's not going to be a closed ecosystem for just individual contributors of attestations.

Scott Perry (39:16.23)
Right, so it opens up past the C2PA. Once you have that immutable object, there's lots of different use cases, some that I don't think anyone in the C2BA even knows in the future how it can be applied. Certainly they wanna make it as open as possible. There is concern that there can be harms introduced by the use of the credentials and there is a component, a working group, a task force within the C2PA focused on threats and harms. We're looking at that and we are working on applications that could cause harm in the marketplace. We're sensitive about that.

But outside of that, once you have this technology in the hands of consumers, it's just like the internet. It's very similar to the internet or blockchain where, you know, we have the technology and you bring your use case to it. So these, for example, the identifiers that I had mentioned, they existed long before the C2PA, they're just getting a new avenue to apply. And I would say with greater strength and assurance associated.

Mathieu Glaude (40:42.23)
Is the C2PA going to have to have some conformance within these third party governing authorities? Because I think the content credential that CR badge or label is the, end like consumer queue that, okay, this, this is like a trusted thing. I don't know if anyone's seen these labels on pieces of content. I certainly have on images, even browsing through LinkedIn, or even, I don't know if you've generated images on chat GPT, for example, like they come stamped with this label.

I think most people will just end consumers rely on the label kind of being a trust signal and don't necessarily go into all the details. Just like if I'm on my browser, I could see that I have a secured connection and my browser is just putting a checkmark or whatever they put nowadays.

I'm not going in and reading all the different pieces of information and assertions that are in there. And so is there a fear, like you just mentioned, there's the threats working group, you want to make sure that there's, you know, garbage in garbage out type of thing, right? You don't want to impact the integrity of that, that strong brand that's trying to be built.

So although the C2PA is not going to be the governing authority for the world of all the different types of assertions that are going to be made, are third party is going to have to demonstrate some conformity before allowing their members to write into content credentials.

Scott Perry (42:14.15)
Well, I think it's going to be industry driven eventually. There is one very strong industry that is already doing that to its members, and that's in the international press. And so they have validation products and they have their own trust list that, if you're part of that community, you want to be able to be validated and you want to have your signing authority linked to that trust registry so that they're policing themselves. And I would expect that just like we expect, I do not expect the C2PA to be policing industry. Industry needs to police itself just like it does today.

The only thing that we're policing is really the ecosystem aspect that we feel we can control to create that foundation. Once that foundation is created, we are looking for industry uses to police itself and who can make those claims and such. And the technology is there.

Mathieu Glaude (43:26.07)
You mentioned the JPEG trust emerging as a rights management layer. Could you, could you expand on that a bit of how this fits within the C2PA and content credentials and within the manifest? So we've kind of covered the generator products, building a strong root of trust there through a conformance program and the issuing of certificates under some governance. We've started talking a bit about creator assertions. The third piece of the canvas seems to now be the rights management layer.

So where does the JPEG trust fit into this whole thing? How does it help complete the story? What more does it do on top of what we've described so far?

Scott Perry (44:09.00)
Right, so JPEG Trust really takes advantage of all the trust signals that come from individual generator products, as well as assertions made by people and organizations from the Creator Assertions Working Group. And then the piece that's added on the rights is really the jurisdictions, because there are a variety of different jurisdictions that have a variety of different laws associated with ownership and protection and rights of digital objects. And so it creates profiles associated with, the combination of the trust signals that are applied on these digital manifests and make determinations within, and communicating within law.

So now law, and jurisdictions have to take that and say, OK, am I going to take it the last mile and I'm going to, in a court of law, support the information that's being provided. So we're providing, in essence, a series of evidence signals that would allow a jurisdiction to rule on a claim made on rights and ownership.

Obviously, there's a number of different parties that are contributing to it. Not much different than we have today. At the end of the day, JPEG Trust is not going to tell Canada that this is Mathieu's digital object. Canadian legal authorities will look at all of the information just like they do in any case, to say, is it persuasive and immutable, cannot be changed. These are properties that are very persuasive in court of law, but it needs a cascation of these different standards overlaid upon each other to create that strong case.

Mathieu Glaude (46:28.05)
So who would be the big consumers of this type of data that will sit, like the rights data that's coming from JPEG Trust or rights data that finds its way into content credentials? Are the end consumers of a digital asset going to be really a consumer of that? Who does that matter to or does it matter to the creator? Like how does that really get consumed and add value to whoever the consumer is? curious on that.

Scott Perry (47:01.13)
Well, you know, there is issues in the marketplace that when I create a work of art or I use AI in combination with other things, will I get paid for my effort? And so creators are concerned or, you know, there are individuals like actors and such, because I'm working very closely with actors. They're concerned about synthetic actors taking their money, their due money because they are applying their digital image, a company is applying their digital image that they may or may not have the rights to.

And so what we'll be seeing really in them is a new industry born around rights, rights management and C2PA and the cog and JPEG trust are all contributing to all of that. Because with AI right now that it's, it's blurred, it's blurred. And, the anonymity of the internet, we don't know where transactions are coming from. So these are kind of efforts to try to gain some foundation around assurance and confidence around, the ownership of valuable assets and you had mentioned where is that happening?

Well, you got to look at the money situation. So if there are a lot right now, we're communicating trillions of dollars of assets and value through the internet. And we need to get a baseline additional layer of confidence to attach ourselves for jurisdictions around how money flows better. One case of point and I got involved very early stage around music industry. The music industry doesn't pay creators very well. There's two aspects of creators. There's the ones that record the music and ones that write songs. And Spotify actually, they were held accountable to pay all these folks and they were saying, I can't find them because we didn't have that flow of ownership of, in this case, songs.

And so, working with organizations like SwitchCord and a new government agency, that has been established to try to find the rights of songwriters and such, are being implemented. And so you'll see a consistent movement around and more of that happening around, rights associated with digital objects.

Mathieu Glaude (49:54.00)
Is it going to create more jobs for lawyers and administrators?

Scott Perry (49:57.16)
Wellthey have to be smarter. They also have to understand the technology a little bit more. I don't know if it'll replace it. Things will morph into a new way of bringing cases to court. There may be more cases initially, obviously with new technology, it has to kind of come to some stability point. And initially there'll probably be a lot of cases that happen through the storming period of this new technology.

Mathieu Glaude (50:28.14)
What's your experience in building conformance programs for different clients of yours? And so you mentioned you're the administrator of the conformance program for the C2PA. How do you go about doing that? And I think also to, some organizations, it may seem cumbersome to get there.

And I'm assuming that any industry group that wants to empower their members, whether it's actors or journalists or whatever, to really get their rights put into pieces of content, get different attestations put into pieces of content. They're all going to need to have some conformance to allow their own members to take certain actions or make certain assertions. So be curious to just understand how the journey has been for you setting up the conformance program, how it's being administered and how it's, maybe it is a big lift or maybe it's not a big lift, but how it's probably an evolving kind of thing over time. It's not like you just do a whole lot of work and it's done and you're good to go.

So it would be curious just hearing from your perspective as the administrator of the conformance program for the C2PA, like how do you even, how do go from zero to where you're at today?

Scott Perry (51:50.05)
Well, you know, it started as an auditor. was a participant in major ecosystems. So as a web trust auditor, and, I was part of the, internet trust around issuing security certificates to websites. And so, these browsers that require assurance around these security certificates use the audit firms to audit their specifications and they've come up with their own called Web Trust. And so, I understood all of the components of an ecosystem governing authority of a standard, which is the CA browser forum and root programs that are using those standards to apply conformance criteria to allow you to be on a Trust Registry, which is based within laptops around the world.

And so the concepts haven't changed as much, but what is going to happen is that there will be more as we decentralize control. Because the internet started, we thought everything would be empowered around one organization or one set of organizations. But we've obviously we found that everything is moving towards a decentralized mechanism and activity is happening to move control from the big companies that control a lot of the aspects of your identity and moving back to the individual to control who they are and control the artifacts that represent themselves.

Scott Perry (53:41.06)
I anticipated that that would take place. So the issuers of these artifacts, like drivers licenses or certifications from states or endorsements of digital identity for you to work with states, they will be issuing these credentials and need to both transmit and make transparent what went into actually creating these artifacts that are used for identity. So that when I'm relying upon it, I know what went into it and is it being controlled to allow it to be trustworthy? So the requirement for a public governance framework and a published conformance program holding accountable to the issuers of these credentials that are happening are really important.

And so, even before, we saw governance frameworks being built at the Trust Over IP Foundation, we created a dual model for the architecture of the Internet, one with a series of layers in technology, but also a governance standard that really has been applied to what's been happening since the beginning of the Internet. But it will have new users like the C2PA.

There was an organization that had a set of players that they wanted to control. And so I came in with the Trust Over IP Governance Meta Model and basically gave them the landscape of how they could, identify the requirements that they needed. And other organizations are doing what they need. So the Governance Meta Model doesn't specify all of the rules. Creates the areas for individual governing authorities to make their own rules against the risks that they see around the misuse of these credentials that get issued.

Mathieu Glaude (55:51.11)
Just some quick fire questions as we wrap up today. Why, why haven't Apple and X joined the C2PA?

Scott Perry (56:01.05)
Well, I'd hope that they would. A lot of organizations, they have a different posture. Sometimes they wait for other methodologies to come in. They wait for other products around, I think. I was around at the beginning of the internet and I was the external auditor for Microsoft.

And right at the clutch point of the internet, they were debating whether they, *we don't need the internet. We'll create our own proprietary walled garden. And there it is*. And I was waiting for them to say it's too big. And they did in the mid-90s. And I believe that this is something very similar, where we're looking at global, all products, all these things. We're establishing really just a foundation of things. It would seem that, Apple and X would adopt these things just because the public is going to be demanding that. And that's the other aspect.

We need to get this technology in the hands of people to create power and demand for other products to say, this is a good idea and I better invest in this, because if I don't, I'm going to be on the outside of the inside group, you know? And I see that with Apple pretty consistently. They now are involved in mobile driver's license and digital identity. And so I think it's just a matter of time as opposed to, this isn't gonna fly. I absolutely have confidence that they'll all join in.

Mathieu Glaude (57:51.03)
Are there competing standards or approaches to what the C2PA is doing?

Scott Perry (57:54.22)
I'd say that there is, I can't really speak in details. I think this is because we have, the majority of the tech firms that create content, are all aligned in there. It creates a powerful coalition. And I can tell you by working with these folks that are in the working groups at the C2PA, they're brilliant. And it's been my pleasure to serve with them and be a part of their group. And they care deeply about not only of their own company's representation, but really care about how this technology is going to be used in a safe and trustworthy way.

And so I have confidence. and now what we're seeing is other parties, that are doind investigative work, like the World Privacy Forum has put out a paper on the C2PA and, government agencies are looking at this. And so I think it's past the critical point where people say, is this a thing? It is a thing. And it's moving, especially with the conformance program rolling

out and Google and other products are, being conformed to this. I think that that's really the path of where we're at, where I think it's almost to the point where I don't see another competing standard coming in and swooping and taking its place.

Mathieu Glaude (59:35:23)
Do you think we'll see an impact on political discourse and elections through some of the things that you're working on here with C2PA?

Scott Perry (59:44.02)
You can. Certainly there are jurisdictions that are looking at certain evidence and the properties of cryptography for voting, obviously a very political question. There's always been questions even recently in the United States about the trustworthiness of the information used in elections.

Certainly, I hope because we do have confidence, you know, using cryptography, I hope that, the advancement of these types of things will allow to be used in elections. I've been working with the state of Utah that's taken a leadership position of all the states in endorsing a digital identity. Maybe that can also be used for voting, we need to get more proof of concepts out in the marketplace to demonstrate to jurisdictions that this is a safe and trustworthy technology to use.

Mathieu Glaude (01:00:56.14)
My final question, governance is kind of the missing piece here. We started the conversation with you could cryptographically sign a lie. So governance is the missing piece. We've kind of talked about how we implement it. How we take governance, we build conformity programs, and then we actually put these into operation. We talked about that with generator products and we started talking about how that would potentially look like. With third party governing parties for different type of industry assertions, we talked about the rights management side of things.

With governance being the key to really bringing that human trust, more confidence behind the assertions and the claims that are being made, how do we ensure governance at the same time doesn't become a tool of exclusion?

Scott Perry (01:01:47.03)
Well, you know, I think we need to get more education on what governance is and what it's not, you know? Governance tends to be an afterthought. And so I've been working very hard to educate. And people say, we need governance, but they don't understand what that means. And so to answer your question, we need transparency because the downfall of governance is that certain governing authorities take action and you don't know why they did it or you didn't know whether they were biased in their opinions.

We need to have transparency, accountability and fairness built into governing authorities. And you hope that that would be the case. And the ones that I'm working on, I aspire to that, make sure that there are checks and balances in there. I can't make sole decisions as an administrator. I need to get other people involved in decisions that are made, because I don't

want to be, the sole actor in causing certain things. We need collaboration within governance processes. And so does that mean it's all going to be fair at the end? That's why we have a threats and harms group in the C2PA. This technology can be used to create harm. We have to be watchful for it. I mean, we're not controlling social discourse. We're creating new mechanisms for society to use. But society has a variety of different motivations and not all of them are noteworthy or honest and everyone's trying to take their actions.

So we have to be cautious, just like we've always been, because this technology is not going to solve all of our problems by itself. And governance mechanisms isn't going to do that as well. We need vigilance, and we need oversight, and we need the drive to do the right thing in order to make these things happen in the way we expect.

Mathieu Glaude (01:04:12.00)
Scott, I really appreciate you doing this with me today. It's always a pleasure. I always enjoy our conversations. And for listeners, I think this conversation touched on some of the most fundamental questions about trust identity information just in the digital world today. And I think the work happening at the C2PA, at the Creator Assertions Working Group, and in trust registries in general isn't just about technical standards, it's really about rebuilding a foundation of trust that the internet was built without.

And I think as Scott said back on the last podcast in 2022, we're finally backfilling that infrastructure 25 years later. And it's absolutely fantastic to now actually see it happen. So thank you for everything you do. Thank you for doing this. I'm sure the listeners will really appreciate this conversation. Scott, thank you.

Scott Perry (01:05:00.10)
It's been my pleasure and thank you for having these podcasts. I've enjoyed listening to them and you've had amazing guests and I'm just privileged to be one of them today.