2023-01-19 AIM TF Meeting Notes

Meeting Date & Time

- 19 Jan 2023
  - **09:00-10:00 PT / 16:00-17:00 UTC**

Zoom Meeting Links / Recordings - **Jan 19, 2023 (I made a mistake in the Slack message. It's on 1/19.)**

Meeting: https://zoom.us/j/97604264531?pwd=NXB3S2d6bldidVVjVFlYVmpwallBZz09

Recording: https://zoom.us/rec/share/RLZ3mo50NnyAuVa7ESHumA9YLnA15PMzWc6Ucrx7qhzl2W22L18GaKoxPV7rL953.A81uHLinViF_Ae8F

Attendees

- Wenjing Chu
- Zaïda Rivai
- Sandy Aggarwal
- @Callum (BC)
- Daniel Bachenheimer
- Neil Thomson
- Judith Fleenor
- Chi Hwa Tang
- Kaliya Young
- Jacques Bikoundou

Main Goal of this Meeting

This is the AIM TF's #14 meeting.

Our main goal is to have individual member presentations on what problems/challenges they see in AI & Metaverse related to trust.

Starting in the new year, we plan to start drafting white papers which are the first deliverables of the task force.

Agenda Items and Notes (including all relevant links)

Time	Agenda Item	Lead	Notes
5 min	- Start recording - Welcome & antitrust notice - Introduction of new members - Agenda review	Chairs	**Antitrust Policy Notice:** *Attendees are reminded to adhere to the meeting agenda and not participate in activities prohibited under antitrust and competition laws.* ***ToIP Policy***: *Only members of ToIP who have signed the necessary agreements are permitted to participate in this activity beyond an observer role.* ***ToIP TSWG IPR Policy:*** *see TF wiki page.* *AI & Metaverse Technology Task Force*

5 mins	• Introduction of new members • Any general announcement, news, that could be of interest to the TF	ALL	• sankarshan AI fairness assessment standard by India TEC of DoT • Anyone gone to CES?
45 mins	Planning discussion continued: planing goals for 2023	ALL	In the last meeting on Dec 15, a lot of great questions were raised. The following is an imperfect summary of these questions, answering them clearly will help us clarify what our goals should be. For reference, the current version of the TF charter info is here. (1) What **type** of work or **role** we should do/play in ToIP and in relation to the broader ecosystem - i.e. our role: standards, how does it relate to other groups, possible collaborations with X, Y, Z... (e.g. Vikas Malhotra IEEE, Sandy Aggarwal Hyperledger...) (2) A more **clear statement of focus**. This statement should give us clear direction and scope. (3) Concrete plan of **actions and deliverables** for 2023. Wenjing Chu will share a straw-man proposal as the starting point of discussion. Here is the "one-pager" slides: Here is the Miro chart that Mary and Zaida created: https://miro.com/app/board/uXjVOkJb1Ow=/ Please complete both before our next meeting. • Wenjing Chu did a review of the TF's charter to frame the overall scope and open the discussion. • Sandy Aggarwal : (1) the platform knows who you are (2) AI agent driven persona - how to ID that. (3) regulated metaverse and how to do KYC. • Neil Thomson : the coupling of anonymity & accountability is a key requirement. f an actor in a metaverse (virtual, created or not) can collect information or take actions, they need to be tied to a responsible/accountable party. Ultimately it becomes choice for the user/participant in an online environment as to whether "anon" users and constructs (generated avatars, personas) are accountable or not. • Daniel Bachenheimer : authentication assurance levels, regulated platform is a third dimension. • Sandy Aggarwal : in games, age proof for children friendly vs. adult world - is another kind of regulated space. • Daniel Bachenheimer in strict regulation - audit trail is another dimension wrt regulation. • Sandy Aggarwal : different governance for different environment. How do you inject the governance in inception? • Daniel Bachenheimer : think an analogy to "Regulated" Platform is from the EU where you can have qualified electronic attestation of attributes (QEAA) and unqualified electronic attestation of attributes (EAA) where qualified issuers EAAs are EU regulated. • @Dan - essentially "verifiable credentials" of a different form (for a platform) • Judith Fleenor : **I think a white paper explaining the various scenarios and the different requirements would be good.** • Wenjing Chu : Identity by AI models. Two type of problems: how data is being used (ethical) more technical (deep fake and tax around identification). How to differentiate human individual from bot (AI or not). This is important for assigning responsibility etc. One proposal: summarising scenarios and use cases that describe these problems and offer solutions. Better inform and recommend other principals to consider. The document would be useful to better inform people in our community. **More clearly specified what the topic is, how it is used today, what problems can be seen from todays systems and what are potential other problems for the future**. • Sandy Aggarwal : How is identity working today and how is identity going to work if we are going to use AI. We can take different examples for different categories and go from there. • Neil Thomson: Whether AI is allowed to use behaviour, etc. to identify an individual is a "permitted and consented processing" data privacy issue, which could be covered under data privacy regulation/legislation. • Sandy Aggarwal : liquid avatar, avatar is *streaming of code*. does the avatar needs to have the ID component such that it cannot be corrupted? • Wenjing Chu : We should structure our work now. Would it be good to identify a smaller set of topics we can focus on and as a group we can decide which topics we should focus on. So we should focus on: **More clearly specified what the topic is, how it is used today, what problems can be seen from todays systems and what are potential other problems for the future**. • Neil Thomson : Brings up the concept of "Authentic Avatars" - is their behaviour traceable to a known, declared crypto/human trust root. All this conversation is stressing data behaviour and regulation. *How do I know the avatar is behaving to the rules I'm expecting it to behave*? • Wenjing Chu : User-user level: of what kind of behaviour is accepted rather than a platform. In AI and Metaverse: Makes it all more severe and interesting as these problems are already existing today but in AI and Metaverse these problems get more complex. • Wenjing Chu : finish Miro board + finish one pager. ============== From Dec 15, 2022 Minutes: Wenjing Chu : see slide here: **Zaida**: wrap up presentations and put in Miro and see what we want to see. **Callum**: Didn't do a presentation, but would be willing to do one. **Sandy**: Are we just going to do standards, or can we collaborate? Or is this just for fun? How much are we going to bring?

Is our task to be coming up with standards, what are the others doing? What exactly is the purpose of our group? Are we also establishing ourselves as a standards helping body? What is the role that we are going to play? Pulls notes on research on this.

What is the current spanning on the metaverse today? Do anything of those relate to AI and Metaverse.

Callum: documented deliverable what it means for the future

Sandy: Maybe we should bring in industry experts? In the overarching eco-system where do we sit? Part of ToIP and Linux foundation. We are focused in the Metaverse.

Wenjing: Maybe we should rethink, but originally it was set up to do two things: 1) Exploration, to get as wide and diverse and collect as many opinions as possible. We wanted to collect from experts what kind of new problems/challenges you could think of like ToIP mission or 4 layer architecture. What is the problem with the AI and Metaverse applications oppose. What problems are out there? 2) Write down recommendations, how do we recommend to the individuals to deal with these problems.

The presentation I made was done on the observation both Metaverse and AI made the Decentralised Identity (identifier) kind of obsolete, because these identities are handled in some way. Your body has plenty of information, which you cannot hide. Therefore, those issues in the current architecture pretend these issues do not exist. This would be one example. Some were more academic. Current AI systems with Metaverse setup, what can they find out about you. What do people need in order to feel trustable? Lot of academic research done already today that answer this question of how to solve this.

The white house presented a set of principles.

Next year: come back to wrap up and see what we actually want to deliver. And then we are going to summarise these challenges that are relevant and a second thing we want to deliver is a recommendation. In ToIP this can be done in two stages, high level: where do we want to be or come up with a few principles (would be very high level). We could add some principles to the list of 17 principles or write more specific recommendations. In case of the latter, which could be a technical specification, protocol, government specification, but those take much longer. It was suggested to be open and much better.

Sandy: We can say "identity in the context of AI and Metaverse" if we talk about "AI and Metaverse" thats too big, we are actually talking about "How does AI come into play" We need to come up with a definition of what we want to focus on.

Wenjing: We are not doing AI nor metaverse, we are doing ToIP. We have a picture that ToIP is proposing and the question is, if you propose a future environment, what is the stack going to look like? We want to create a trustworthy environment. Today, we are focusing on existing services. We may or may not update this stack in order to support the future emerging services. And we take AI and Metaverse as two focus points. There is a lot of work we can jump into. How to create identity? Digital assets? Avatars? AI powered agents? These could be more concrete directions to go to, it is a possibility. If this is a more productive way of jumping into something, we could absolutely switch our direction here.

Sandy: Will do a paper and will share a link.

Wenjing: There are multiple things. 1) What data to disclose, what not. If I provide content, how do I want to get paid. You need a lot of things, like biometrics, that needs a lot about me. But its much bigger than just biometrics, they know a lot more. 2) Agents: describe environments and come up how we manage.

Sandy: how are AI agents use today by for example, games. Microsoft has the working Metaverse platform Mesh. Meta when it came in didn't have legs, because it is somehow very difficult. They were using AI to create legs. How is AI going to be used? In terms of speech? Chatbots? Visuals? And how do these come to play? Is the goal of our TF to come up with a recommendation in the design principles? Then we need to know what the shortcomings are. What are the challenges. Then we can say, because we know these challenges (like the leg-problem) then we need to know what to fix. Might know some people that are specialised in the AI side, that know these problems.

Some proposed action items:

- Sandy will help invite experts who have deployed metaverse-like systems, e.g. games, to share with us issues they face.
- Sandy is also working on a paper in the Hyperledger - will share a link and invite us to contribute.
- Wenjing will write up a context/scenario as a proposal for the TF to discuss in the new year - in order to answer the question: what is the intersection of ToIP and AI & Metaverse looks like - what problems we can focus on to solve.

| 5 mins | - Review decisions /action items
- Planning for next meeting
- AOB | Chairs | - Next meeting: identify topics you want to get answer too |