～［Dialogue with Diversified Insight］Future Human Responsibility in the AI Period～

Event Report

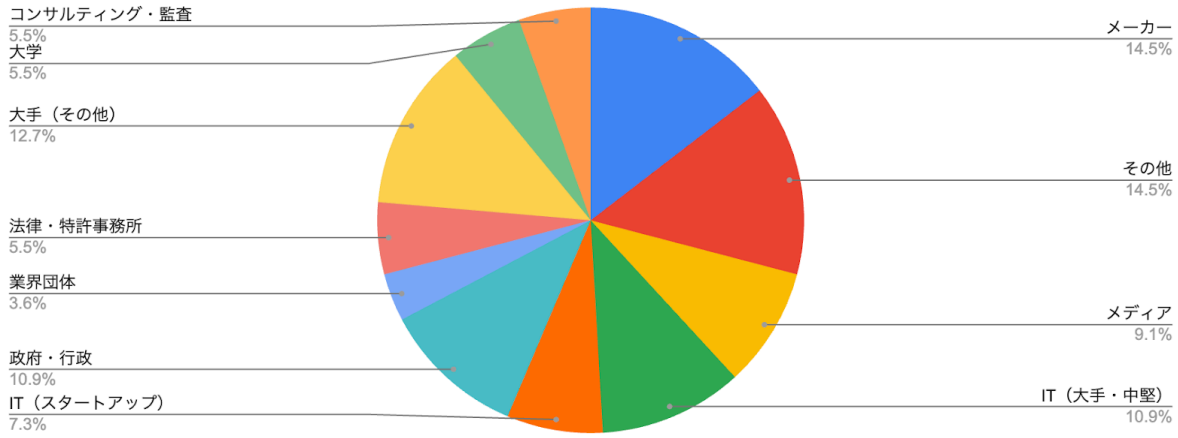
Privacy by Design Lab

Event Overview

Hosted the event in August 21th, 2024 below

Event Name：［Dialogue with Diversified Insight］Future Human Responsibility in the AI Period
Venue：Tokyo, Chiyoda Ward, Matunouchi 3-8-3
Tokyo Innovation Base（Sushi Tech Square 2nd Floor）
Date：August 21th, 2024（Wed）
Start：17:00（Opening Reception：16:30）
End：20:00
Organizer：Privacy by Design Lab
Co-organizer：Tokyo University, Institute for Future Initiatives（IFI）Governance Unit
Cooperation：PrivateAI
Support：Embassy of Canada to Japan
Event Link：https://peatix.com/event/4071836/
Registrations：182（Canceled 7）
Check-in：69

Registration Demographic（Permissioned Attendances）



Speakers

Patricia Thaine
CEO & Co-Founder, Private AI

Patricia Thaine is the Co-Founder and CEO of Private AI, a Microsoft-backed startup who raised their Series A led by the BDC in November 2022. Private AI was named a 2023 Technology Pioneer by the World Economic Forum and a Gartner Cool Vendor. She is also a Computer Science PhD Candidate at the University of Toronto (on leave) and a Vector Institute alumna. Her R&D work is focused on privacy-preserving natural language processing, with a focus on applied cryptography and re-identification risk. She also does research on computational methods for lost language decipherment. Patricia is a recipient of the NSERC Postgraduate Scholarship, the RBC Graduate Fellowship, the Beatrice “Trixie” Worsley Graduate Scholarship in Computer Science, and the Ontario Graduate Scholarship. She is the co-inventor of one U.S. patent and has ten years of research and software development experience, including at the McGill Language Development Lab, the University of Toronto’s Computational Linguistics Lab, the University of Toronto’s Department of Linguistics, and the Public Health Agency of Canada.

Andrew Gambardella
Postdoctoral researcher at the University of Tokyo

Andrew Gambardella graduated from UC Berkeley with a BS in Electrical Engineering and Computer Sciences in 2013, after which he took a position as the lead AI engineer for SoftBank’s humanoid robot, Pepper, at SoftBank’s main office in Tokyo, Japan. There he created an AI app, PepperVision, that allowed the robot to learn about, recognize, and interact with objects in the real world. Following this, Andrew took a position at the then-newly founded startup, Cogent Labs, where he worked on Japanese handwriting recognition and document clustering techniques. In 2017 Andrew started a DPhil at the University of Oxford in Engineering Sciences, concentrating on machine learning and artificial intelligence. He submitted his DPhil thesis on Bayesian transfer learning techniques in 2021, and thereafter worked as a researcher at KAIST (Korea Advanced Institute of Science and Technology), applying his knowledge of machine learning to the arts. Since then Andrew has returned to Japan, and is currently working as a researcher of artifical general intelligence at the University of Tokyo, working under Japan's "godfather of AI," Professor Yutaka Matsuo.

Toshiya Watanabe
Professor, Institute for Future Initiatives Vice President Professor, Department of Technology Management for Innovation, Graduate School of Engineering (Additional Post)

Toshiya Watanabe finished the doctoral course of inorganic material engineering faculty at Tokyo Institute of Technology. After fifteen years career of researcher of manufacturing company, he was appointed to become guest professor at University of Tokyo’s Research Center for Advanced Science and Technology in 1998. Later, he was appointed as professor of the same center in 2001. Currently he is a Professor of the Institute for Future Initiatives and Technology Management for Innovation (TMI). He is also appointed Vice President of University. As for activity for government policy, he is a chairman of planning committee of Cabinet Council Intellectual Property Headquarter.

Chihiro Fujisaki
Managing Director, Privacy by Design Lab

In 2004, he joined a major printing company and was involved in new product development for consumer goods; in 2006, he joined the business strategy department of a regional business division, where he was responsible for employee training, sales planning, legal affairs and the Privacy Mark acquisition secretariat; in 2014, he moved to the business strategy department of a core business division, where he was

responsible for formulating management visions and internal penetration, From 2021, he moved to the R&D department of the company's digital subsidiary, where he is in charge of research and strategy development related to privacy protection technology platforms, respect for avatar privacy in the metaverse and digital ID. Currently, from 2024, he is also involved in a project to develop an AI ethics policy and to build privacy governance, in parallel with business reforms, including generative AI.

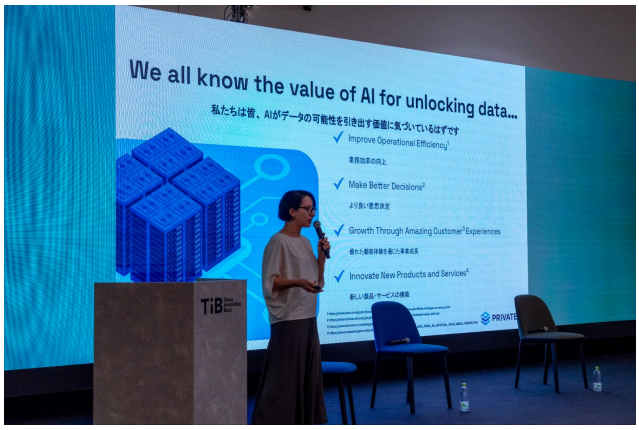
In addition, as a parallel career, he co-founded and serves as a board member of Privacy by Design Lab, a general incorporated association in 2020, is a member of the Privacy Workshop Committee of the Information Processing Society of Japan, and participates in other university collaboration projects to deepen understanding of data, with the aim of realising a society where each person can be respected by each other. He is involved in various project activities with the aim of realising a society where each individual is respected.

Short Presentation 1 ：Creating a Future of Responsible AI （Patricia Thaine）

Presentation Slides：Creating a Future of Responsible AI

Thank you for inviting me today. I would like to talk about responsible AI. In recent years, the applications have been able to make optimal decisions more efficiently through LLM, just as they are projected on a screen. Many use cases are appearing all over the world, and LLM is being integrated into general services, leading to a better customer experience.

C-level executives are using the LLM solution and it is progressing more widely. Besides, the issues of bias in decision-making and vulnerabilities such as hacking are also emerging, and there is a growing need for more trusted and responsible AI.



Integrating the responsible AI definitely requires privacy, security, and transparency (being accountable). When it comes to security, new types of vulnerabilities should be in consideration.

NIST published guidelines for discovering vulnerabilities two weeks ago. When it comes to privacy, upfront risk estimation is often insufficient. There are some potential risks that occur during implementation. In 90% of test environments, private credit card information is also implemented, but many are unaware of it.

This may not lead to appropriate data usage and may cause problems. Meanwhile, penalties may be incurred due to violation of laws and regulations due to the setbacks of using data, and unavoidable issues related to algorithms such as data deletion may also occur.

Financial sanctions from regulators are widespread globally, and policies like Europe's AI law will have a major impact in the coming years.

There are moves to ban the use of AI for public surveillance, etc., and the European AI Law does not mention the continued acquisition of data related to individuals through generative AI models such as LLM, but also the use of different types of related data.

In addition, as there is a growing movement in Europe to require risk management, it is necessary to sort out data governance, security, and robustness.

Under data protection regimes, data minimization is a fundamental requirement, requiring data to be processed in the amount necessary for the processing of a specific task. The European GDPR also touches on pseudonymization and anonymization.

The Data Protection Act and the European AI Bill are packed with content that is required in the policy process. The services developed by PrivateAI include the elements necessary to respond to these needs.

We provide the necessary elements for companies to use AI responsibly to innovate. We provide a mechanism to clarify what kind of data is held and protect it.

There is often a debate about direct identifiers and indirect identifiers, but it is necessary to combine multiple results and link them to feasibility.

We will adopt a third-party audit model as the certification model, prepare the necessary technical resources to realize a responsible AI model, and aim to implement cybersecurity, computing, etc.

Short Presentation 2 ：For Human-Centered AI by Research （Andrew Gambardella）

Presentation Slides：For Human-Centered AI by Research

AI has attracted more attention since the birth of a new neural network in 2017. From 1952 to 2008, we have passed through the pre-deep learning era and are now entering a new regime of learning. This has led to exponential growth, and computation is also.

In addition, a new emerging AGI will be coming out, and a new LLM (general AI) will appear from 2023.

On the other hand, people like Professor Hinton are concerned that generative AI risks the extinction of humanity.

Even if it is not a Generative AI, police AI that judges someone's face and AI related to recruitment will have a similar meaning. Although these risks are scope that AGI has not yet reached, I believe that they will be addressed as AI research evolves in the future.

As it becomes to grow the dataset, LLM gets smarter as well. When talking about data currently used in AI, a major theme is how to safely utilize large amounts of data such as those from Github and Wikipedia.

Humans look at ChatGPT and type in what they are interested in, and the AI learns by checking the content. By entering an incomprehensible string of characters, you can attack ChatGPT. ChatGPT is not yet able to respond to such intentional attacks. The same goes for personal information.

Matsuo Laboratory is also researching AI that protects privacy, and we are conducting research on what happens when new learning is added to Generative AI. Through that research, I learned that LLMs sometimes pretend to forget.

Short Presentation 3 ：AI & Data Governance （Toshiya Watanabe）

Presentation Slides：AI& Data Governance

Today, I will talk about Japanese data and AI governance, focusing on institutional topics. In terms of my slides, you can find it on my Site (research map) portal and has been uploaded. So if you are interested in more details, please check it out as reference.

We are planning to hold an event similar to a startup pitch on November 26th of this year, based on the concept of a startup ecosystem to achieve well-being. We are accepting applications until August 31th, so please join us if you are interested.

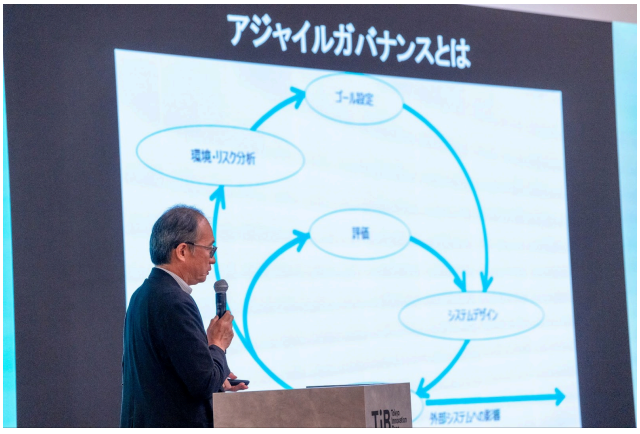
At this event, we have been considering smart cities topics, and it is necessary to think about how to improve the wellbeing of the people living there, rather than the purpose of using AI.

In Toronto, PrivateAI is based, where was a Google affiliate's smart city project, was not well-received by civil opinions, and was eventually ceased.

In this case, the data was not originally intended to improve the smart city, but was intended to be used for a different purpose.

When the people search on Google, they have to provide various personal data and give Google a license. Each user has a license agreement with Google. The surveillance cameras may collect personal data for marketing purposes without the person being photographed realizing it.

Nowadays, the accuracy of low-orbit satellite data is becoming more accurate, so the purpose to use satellite data will likely become an issue in the future. In addition to legal compliance issues, it is also necessary to think about privacy issues.



To utilize data will no longer be viable due to distrust among customers and stakeholders.

COCOA, the app was developed during the Covid-19 pandemic, is the good reference.

While many people had misunderstandings about COCOA, I think it was relatively easy to accept the provision of data for the purpose of public benefit. Communication is necessary for people to understand the system, and it is important to balance this with the purpose of data use.

As AI will be expanding, rising more risks will be emerging. There may be concerns that someone with malicious intent may use it in a risky manner.

Since it is difficult to regulate everything, including copyright, by legislative action, Japanese approach is to promote self-regulation in order to face the stakeholders who are the beneficiaries.

It is necessary to arrange the communicate with stakeholders centered on AI and governance, with an attitude of self-regulation as much as possible, rather than outright bans.

In accordance with technical advances, it is necessary to adopt agile governance that evaluates and improves. It is also important to adopt the concept of co-regulation and design incentives for those who comply with self-regulation, and Japan has adopted this concept.

Panel Discussion

Fujisaki: Thank you panelists. As a beginning, I would like to ask all panelists what each of you have felt anything by listening to what the other panelists said?

Andrew: Although there were various discussions, I think most of the content seemed to be the same. I totally agree that AI and privacy are important, and that AI should not be used in situations where it should not be used.

Fujisaki: Is there a connection between other technology elements and the AI issues?

Andrew: For example, encryption is often related to AI, and there are also places that apply to my research in linguistics. Most researchers research not only AI but also other fields.

Fujisaki: Prof. Watanabe, did you feel anything after listening to the panelists?

Watanabe: It was very interesting to learn about a new business idea from Patricia's talk. I think it is extremely important that the research we are doing now turns into business. Talking copyright issue as an good example, some people say that it is better to impose restrictions under copyright law, but I think that is very difficult.

Because we can't apply unlawful case if we cannot know the process inside AI. If AI cannot be properly understood, there may be little point in deleting the personal data used for training. Even if you erase data once, the same data will be generated again within the mechanism.

It is difficult to regulate with conventional opt-outs requirement and such, and it is necessary to understand what AI is, before regulating it, which is a challenging now. Therefore, I think firstly it is important to adopt self-regulation and make it easier for those who develop technology to proceed.

Patricia: I think it is very important to incorporate responsible AI into applications and services to avoid social backlash. Responsible AI is already being widely discussed, and information is being shared from various perspectives on issues that need to be considered in each region, including in the area of data protection.

Fujisaki: Before moving to the next topic, I would like to ask the audiences what kind of people are participating today. Could you raise your hands how many people are participating today as researchers, businesses, and AI users? (Question to the audiences)

Looking at everyone's responses, I found that most of them were business and users, so I would like to explore their interest with the panelists.

How is progressing on responsible AI?

Patricia: I have the impression that many countries have just begun demonstration experiments regarding responsible AI. Opportunities are increasing, especially among consulting companies, governments, and major corporations, and consider what responsible AI is.

In the financial field, many cases are emerging to address AI governance and responsible AI, and momentum is growing.

Fujisaki: What companies are interested in responsible AI in Canada?

Patricia: The financial sector, consulting, and big tech companies are starting to take action. Technology companies are also interested in communication service providers, and an increasing number of companies are starting to work on responsible AI, just like in Japan.

Fujisaki: Could you tell us if there are any differences in the way AI to handle in different countries?

Andrew: Not only for Generative AI but also for General-purpose AI, there are big differences in the amount of data depending on the country and language. In the case of South Korea, the amount of data is not enough to begin with the AI production, so it is difficult to create their own model. In Korea, we are currently at the stage of investigating how to create a privacy policy.

Fujisaki: What about in Japan?

Andrew: LLM has a technology called an organizer that allows you to break down strings into separate words. Japanese has a large number of characters, and there are many cases where it is not recorded in the organizer. There is some issues to compare in English and Japanese, whether in space or not.

Fujisaki: In that case, should we create an original Japanese model?

Andrew: Universities and companies are also trying to create international LLMs, and it is necessary to create something that also supports Japanese.

Fujisaki: How should we deal with the rules and ways of thinking when dealing with AI?

Watanabe: In the case of Japan, I got the impression that there are many requests for clarity in black and white. in front AI and data contract guidelines. In consequences, the guidelines were about 400 pages long. When sorting out AI and privacy,

you have to draw the baseline. Major tech company like Google and a new startup has a gap for governance resources, so we have to take into account that.

In the case of a startup, you start to tackle the basics items, and as you gradually grow the number of stakeholders involved, so I think it's important to create a governance plan accordingly.

Even thought we have created a checklist in this guideline, start-up companies should start the basic requirement first.

Fujisaki: Do Japanese companies often request that universal rule?

Watanabe: Japanese companies are not good at governance and management, so I think that we got plenty of requests for decisions to be made as clearly as possible.

But, in the case of governance, all the items cannot be clearly defined. Therefore, I told them to rethink about governance from scratch and looking at their own goals and communicating with their stakeholders.

Fujisaki: Do you think that in Canada? There is a similar desire to follow the same black and white rules when using AI in Japan?

Patricia: Even in Canada, we have gray zones. There are gray zones in terms of governance to deal with customers, but we try to consider them in advance.

There is a similar case at Canadian Airlines, and we are considering how to draw a line between employees to handle information.

Audience: How should we reach a common understanding in AI guidelines, and we define the conventionality of human-centered?

Watanabe: It is important for businesses to first determine who their stakeholders are. Besides, considering whether the target stakeholders will be accepting it or not.

Stakeholder relationships relatively aligns with societal transition, so instead of believing reclkessly, it is necessary to organize things around stakeholders.

Taking the Japanese Act on the Protection of Personal Information as an good example, it is just refer to guidelines. But I think it is necessary to start from there and think about countermeasures since the stakeholders are depends on the company's services.

As a company becomes larger, stakeholders become broader, so it is important to make decisions based on the environment in their business area.

Audience：, So, I would like to know what you think about the use of data for AI learning from the Japanese Copyright Law Article 30-4 perspective.

Watanabe: As I mentioned earlier, it is important for businesses to first determine their stakeholders. And to pre-consider whether the target stakeholders will accept it.

Speaking of Japan's copyright law, it was revised a while ago, and machine learning has been deemed to be an acceptable under copyright law. At that time, they quoted with the American concept of fair use and created a law that states that the purpose for processing data to teach machine learning is fair use.

At the time, the law had a good reputation as a progressive law, but since last year the trend has changed, and some people are now saying that it would be better to repeal it. Originally, the content needed to be compiled by the government, but some questions have come up that are extremely difficult to answer.

Andrew: Overseas AI companies are often concerned about Japan's handling of copyrights. I can't say the name specific companies, but I think there will be cases where AI is used in research now..

Fujisaki: From the perspective of overseas companies, does this mean that Japan has a lot of research materials that can be used for AI?

Andrew: Yes. LLM learning requires big data, and Japan, where big data is freely available, that is an fruitful resources for machine learning development.

Patricia: I would like to ask both of you if there are any differences between Generative models and conventional AI models regarding copyright law?

Watanabe: From a governance perspective, it seems appropriate to pay a fair price. I would like them to consider their stakeholders and take actions such as obtaining approval or permission from content owners.

Fujisaki: How can I claim copyright using just a string of characters?

Watanabe: There are some things that cannot be considered only within copyright law. I think this is an easy-to-understand analogy, but from now on, it will become important to consider how to deal with stakeholders as a matter of governance, rather than just thinking about copyright laws that rely on determining whether the target is a copyrighted work or not. I think so.

Fujisaki: Does this mean that we need to update the way to apply for business operations based on the existing laws?

Watanabe: It is important to prioritize governance rather than copyright law. The idea is that it would be better to respond through governance rather than legislation.

Audience: How should we think about considering the theory of lawin Japan? I believe that European rule-making is based on the theory of evil, but please tell me how to evaluate it and how it should be viewed in Japan?

Watanabe: Even if the law is passed, there is the rest of issue to enforce the crime. Although, we create hard-law like those in Europe, enforcement problems will arise. Just by enacting hard-laws will not solve the all problems. Learning from the case with GDPR, I think it is important to create something that will serve as a key point, so I think it will be necessary to create rules in Japan as well.

Utilizing data is not an issue that can be solved only in Japan. Also, if there are no rules in Japan, it will grow concens worldwide. From now, I think a certain level of rules will be necessary to balance utilization and protection, but this will not actually solve the problem.

We focus on co-regulatory principle to look for transparent explanations and considering penalties for violations of the act.

Fujisaki: I want to hear Patricia's opinion.

Patricia: I think there are ways to regulate things as required by society, such as the EU's AI law, but I think it will become more important to balance the technical innovation.I think it will be important to consider this aspect as well.

Audience: What initiatives is taken to reduce AI risks while increasing returns in Canada?

Patricia: Some initiatives have started, but there is no clear movement yet, so I think that, like in Japan, there will be a need to evaluate personal data legislations comparing to the data protection system in Europe. I think it will happen.

Fujisaki: What do you think is necessary as a researcher to reduce risks?

Andrew: Look at police utilities with AI as an example, I think even researchers need to think about the risks before they come up with a model.

Fujisaki: Does it matter whether the purpose of using AI with humanism?

Andrew: Yes. I think it will be necessary to consider issues such as bias to decide whether it is acceptable to look at someone's photo and determine whether or not they are a criminal.

Fujisaki: I think ethics and morals are related to a country's culture and rules, but how should we make judgments about them?

Andrew: China is promoting the use of surveillance, but it is also difficult for us to judge whether it is a good idea or not.

Audience: There is a lot of countries to design systems related to AI. Please tell us how are you reviewing this landscape? And, there are ideas such as agile governance, and when will this type of concept be achieved through technological development?

If technology alone cannot achieve proper usage and humanism, we will permanently have to work against it, please tell us foreseeing.

Andrew: The processing power of computers has increased over the past 50 years in accordance with Moore's Law, but the amount of AI calculations will continue to increase, so I think technological development will slow down to a certain extent.

However, since the chips developed by NVIDIA will rapidly improve the performance of AI, it is important to consider whether it is necessary to think about technological development in terms of regulations in the first place. is.

Audience: I think principles are more important than government regulations. What do you think about that?

Watanabe: I think it's difficult to create rules based on the amount of calculation. This should be dealt with through basic self-regulation and joint regulation, and in Japan, in addition to AI regulations, there are also moves to require accountability, such as the Transparency Act for Digital Platform operators, so this is a very helpful resource. I think it will be.

Although we are making good progress by requesting joint regulations for certain platform operators, I think it would be difficult to apply similar regulations to AI, which has a wide range of applications.

Fujisaki: Lastly but at not least, I would like to receive comments from everyone. If you have anything you would like to talk to us today, please share your final comments.

Andrew: First of all, I think it's important to consider the intention to use AI carefully, so please use it carefully.

Watanabe：We received over 24,000 comments on copyright public comments .Usually there are around 100, so you can see that there is a lot of interests in this field.

This topic has become such a national debate that even the government has difficulty reviewing all the comments.

I think it's important to think it as an issue for the entire ecosystem, not just specific people, so I hope everyone will engage in various discussions.

Patricia: If anyone is interested in our activities, please ask Mr. Goto, who is active in Japan, about various things.

Pictures


TiB
Tokyo Innovation Base
KICKOFF!
SHOP


SusHi Tech TOKYO
Sustainable High City Tech Tokyo
TiB


パネルディスカッション


SHOP


TiB
Tokyo
Innovation
Base

Report Inquiry
Contact：Privacy by Design Lab
Email：info@privacybydesign.jp