

PATENTS AND TRADE SECRETS: RISK OF LOSS OF RIGHTS WHEN USING ChatGPT?



Seminar Kraus & Weisert "International Patent Law: Recent Trends In Artificial Intelligence"

Munich, September 12, 2023

Speaker: Dr. Johannes Graf Ballestrem, LL.M.



STRUCTURE

I. INTRODUCTION

II. RISK OF LOSS OF RIGHTS WHEN USING
ChatGPT?

III. SAFETY PRECAUTIONS WHEN USING AI



Introduction



I. INTRODUCTION

- The term "artificial intelligence" was first used by John McCarthy in 1955/56 and described as:

“conjecture that every aspect of learning or any other feature of intelligence can in principle be so precisely described that a machine can be made to simulate it”



I. INTRODUCTION

- For successful "machine learning", AI tools must be fed with data
- Precision of problem solving relies on the quantity and quality of data collected
- AI learns and improves from the input data (*training data*)



I. INTRODUCTION

- Opportunity: Ease of work for patent offices and patent attorneys in the search for prior art
- AI tools can help to accurately and comprehensively sift through all sources of information
- Can the input of trade secrets into AI tools for the purpose of determining the prior art lead to their disclosure and subsequently to a patent application no longer being allowed?



I. INTRODUCTION

- EU Law:

DIRECTIVE (EU) 2016/943

Article 2 – Definitions

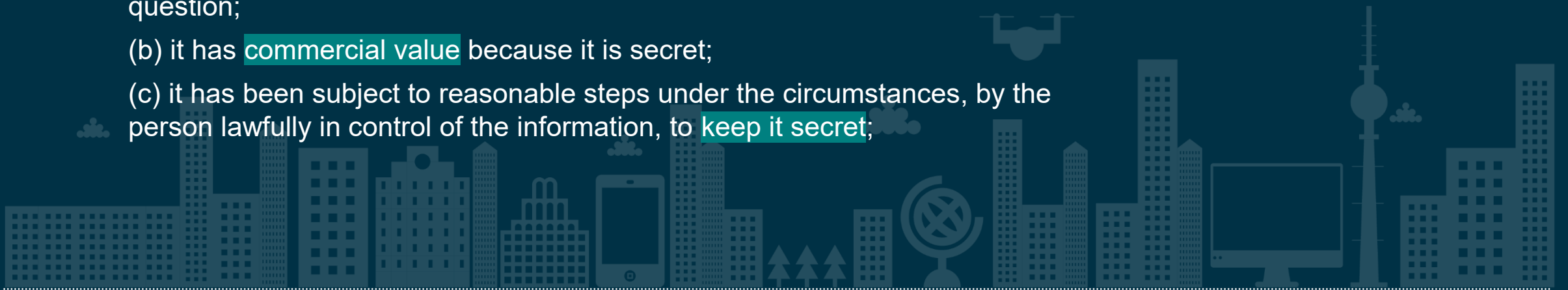
For the purposes of this Directive, the following definitions apply:

(1) ‘trade secret’ means information which meets all of the following requirements:

(a) it is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;

(b) it has commercial value because it is secret;

(c) it has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret;



I. INTRODUCTION

- Japanese Law:

Unfair Competition Prevention Act (Act No 47 of 1993)

Section 2

(6) The term "trade secret" as used in this Act means technical or business information **useful for business** activities, such as manufacturing or marketing methods, **that is kept secret**, and is **not publicly known**.



I. INTRODUCTION

- US Law – trade secrets are protected by state and federal law. To constitute a trade secret, such information must meet two criteria:
 1. the information must derive **economic value** from **not being known**
 2. the owner must keep the information **secret** using **measures** that are reasonable under the circumstances



I. INTRODUCTION

Sec. 3 German Patent Act / Art. 54 EPC

(1) An invention is deemed to be new if it **does not form part of the state of the art.** The state of the art is held to comprise **all knowledge made available to the public** before the date governing the filing or priority date of the application by means of a written or oral description, by use or in any other way.

(2) ...

(3) ...

(4) ...

(5) ...



I. INTRODUCTION

BGH – Dec.12.04.2022, X ZR 73/20

- The plaintiff claimed that the inventor of the patent at issue had sent technical drawings to a subsidiary before the priority date
- Could this lead them to become prior art and therefore not patentable?
- In the case of commercial development or testing activities, the public accessibility of knowledge must be denied as long as the knowledge is only accessible to persons involved in these development and testing activities.
- Even if trade secrets are not treated confidentially and therefore do not fall under the Trade Secrets Act, this does not necessarily make them prior art. They still can be patentable.



Risk Of Loss Of Rights When Using ChatGPT



II. RISK OF LOSS OF RIGHTS WHEN USING ChatGPT?

Does entering trade secrets into ChatGPT lead them to become prior art?

- Problem comparable to entering trade secrets in online search engines
- The EPO also uses online search engines for its prior art searches

(epo guidelines for examination 2023 – Part B Ch. III No. 2.4)



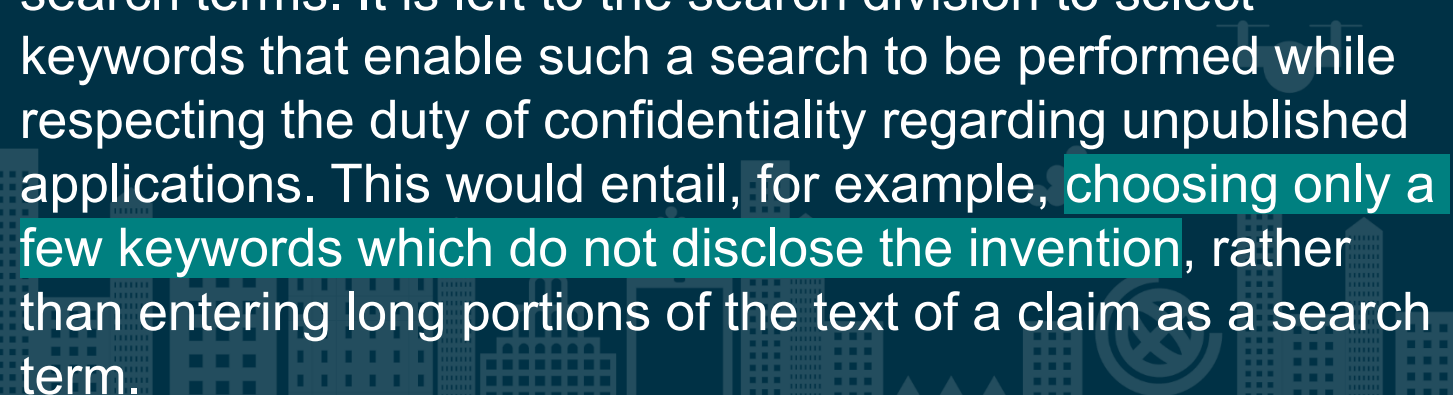
II. RISK OF LOSS OF RIGHTS WHEN USING ChatGPT?

Guidelines for Examination of the EPO

Part B – Chapter III-3

2.4. Search on the internet

The European search can also cover internet sources, including online technical journals, online databases or other websites [...] but must take great care not to disclose confidential information through the inadvertent use of search terms. It is left to the search division to select keywords that enable such a search to be performed while respecting the duty of confidentiality regarding unpublished applications. This would entail, for example, choosing only a few keywords which do not disclose the invention, rather than entering long portions of the text of a claim as a search term.



II. RISK OF LOSS OF RIGHTS WHEN USING ChatGPT?

Does entering trade secrets into ChatGPT lead them to become prior art?

Let's ask ChatGPT!



II. RISK OF LOSS OF RIGHTS WHEN USING CHATGPT?

SA SAMUEL

Does entering trade secrets into ChatGPT lead them to become prior art?

CHATGPT

I am not a legal expert, but generally speaking, sharing trade secrets or confidential information in a public forum like ChatGPT could potentially impact their status as trade secrets. However, whether this would lead to them becoming prior art would likely depend on various legal factors and the specifics of the situation. It's advisable to consult with a legal professional for accurate advice on intellectual property matters.

Message



II. RISK OF LOSS OF RIGHTS WHEN USING ChatGPT?

About ChatGPT

- OpenAI is also aware of the security risks
- As one can see ChatGPT also reminds users not to disclose confidential information
- Also, the OpenAI T&C address this topic



II. RISK OF LOSS OF RIGHTS WHEN USING CHATGPT?



OpenAI

Research ▾ API ▾ ChatGPT ▾ Safety Company ▾

3. Content

(a) **Your Content.** You may provide input to the Services ("Input"), and receive output generated and returned by the Services based on the Input ("Output"). Input and Output are collectively "Content." As between the parties and to the extent permitted by applicable law, you own all Input. Subject to your compliance with these Terms, OpenAI hereby assigns to you all its right, title and interest in and to Output. This means you can use Content for any purpose, including commercial purposes such as sale or publication, if you comply with these Terms. OpenAI may use Content to provide and maintain the Services, comply with applicable law, and enforce our policies. You are responsible for Content, including for ensuring that it does not violate any applicable law or these Terms.

(b) **Similarity of Content.** Due to the nature of machine learning, Output may not be unique across users and the Services may generate the same or similar output for OpenAI or a third party. For example, you may provide input to a model such as "What color is the sky?" and receive output such as "The sky is blue." Other users may also ask similar questions and receive the same response. Responses that are requested by and generated for other users are not considered your Content.

(c) **Use of Content to Improve Services.** We do not use Content that you provide to or receive from our API ("API Content") to develop or improve our Services. **We may use Content from Services other than our API ("Non-API Content") to help develop and improve our Services.** You can read more here about how Non-API Content may be used to improve model performance. If you do not want your Non-API Content used to improve Services, you can opt out by filling out [this form](#). Please note that in some cases this may limit the ability of our Services to better address your specific use case.

(d) **Accuracy.** Artificial intelligence and machine learning are rapidly evolving fields of study. We are constantly working to improve our Services to make them more accurate, reliable, safe and beneficial. Given the probabilistic nature of machine learning, use of our Services may in some situations result in incorrect Output that does not accurately reflect real people, places, or facts. You should evaluate the accuracy of any Output as appropriate for your use case, including by using human review of the Output.

5. Confidentiality, Security and Data Protection

(a) **Confidentiality.** **You may be given access to Confidential Information of OpenAI, its affiliates and other third parties.** You may use Confidential Information only as needed to use the Services as permitted under these Terms. You may not disclose Confidential Information to any third party, and you will protect Confidential Information in the same manner that you protect your own confidential information of a similar nature, using at least reasonable care. Confidential Information means nonpublic information that OpenAI or its affiliates or third parties designate as confidential or should reasonably be considered confidential under the circumstances, including software, specifications, and other nonpublic business information. Confidential Information does not include information that: (i) is or becomes generally available to the public through no fault of yours; (ii) you already possess without any confidentiality obligations when you received it under these Terms; (iii) is rightfully disclosed to you by a third party without any confidentiality obligations; or (iv) you independently developed without using Confidential Information. You may disclose Confidential Information when required by law or the valid order of a court or other governmental authority if you give reasonable prior written notice to OpenAI and use reasonable efforts to limit the scope of disclosure, including assisting us with challenging the disclosure requirement, in each case where possible.

(b) **Security.** You must implement reasonable and appropriate measures designed to help secure your access to and use of the Services. If you discover any vulnerabilities or breaches related to your use of the Services, you must promptly contact OpenAI and provide details of the vulnerability or breach.

(c) **Processing of Personal Data.** If you use the Services to process personal data, you must provide legally adequate privacy notices and obtain necessary consents for the processing of such data, and you represent to us that you are processing such data in accordance with applicable law. If you will be using the OpenAI API for the processing of "personal data" as defined in the GDPR or "Personal Information" as defined in CCPA, please fill out [this form](#) to request to execute our Data Processing Addendum.

II. RISK OF LOSS OF RIGHTS WHEN USING ChatGPT?

THE SAMSUNG INCIDENT / OTHER SAFETY-RELEVANT BUGS

- Samsung allowed its employees to use ChatGPT for professional purposes
- The entire source code of an application was entered into ChatGPT for debugging purposes
- ChatGPT was used by Samsung employees to summarise meeting notes and create a presentation
- In another case, ChatGPT users were shown requests from other users due to a bug which disclosed the requests / prompts



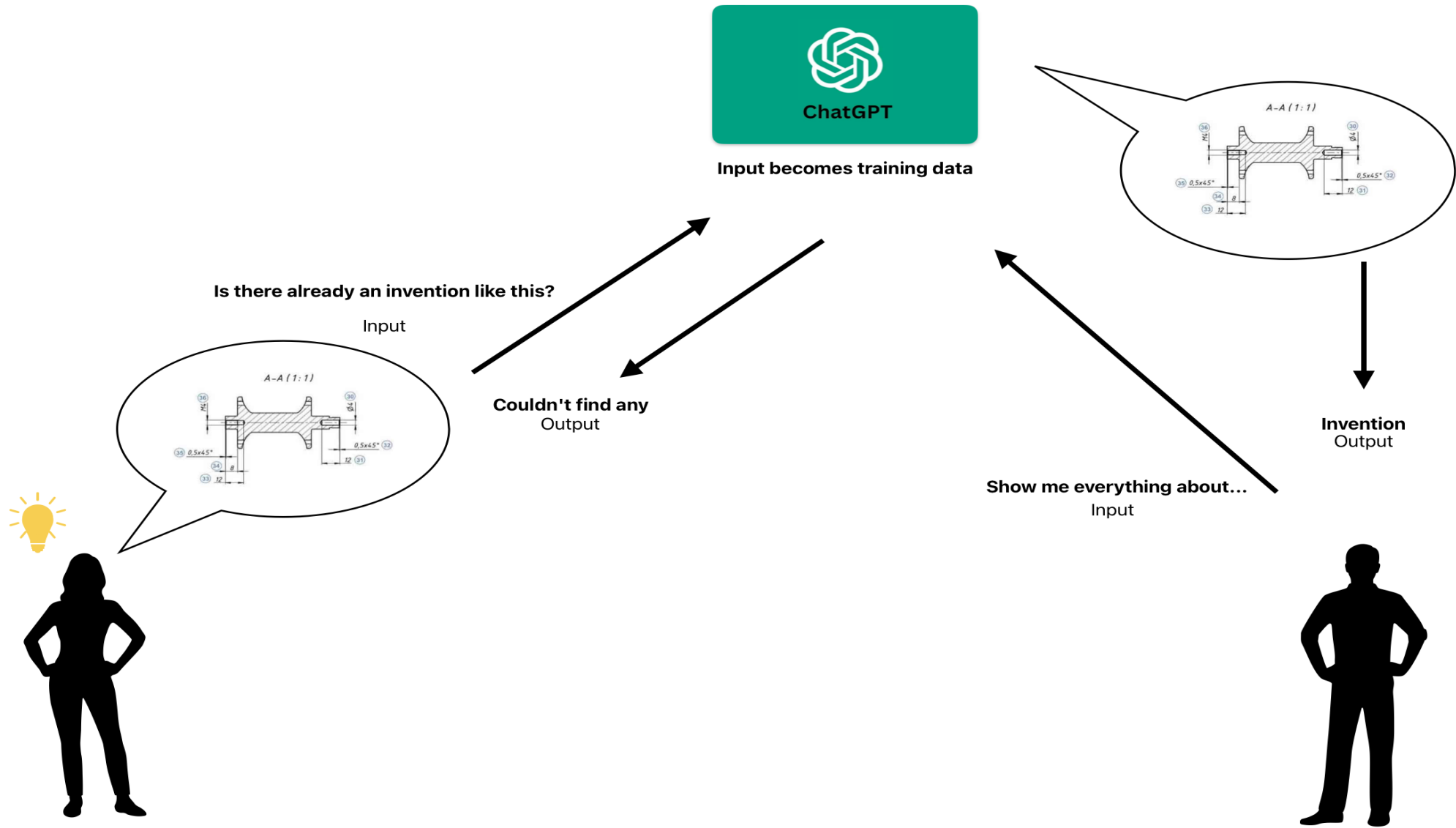
II. RISK OF LOSS OF RIGHTS WHEN USING ChatGPT?

Trade Secrets and Patents

- In German law, disclosure of trade secrets is “the disclosure of the trade secret to third parties, not necessarily to the public”.
- In patent law terms, information is "publicly available" ... "if even a single member of the public is able to access and understand that information and if there is no non-disclosure agreement in place (NDA)".
- Due to the effect of the training data, the use of ChatGPT can in principle be seen as disclosure of the trade secret, as it potentially becomes accessible to third parties (other users).



II. RISK OF LOSS OF RIGHTS WHEN USING CHATGPT?



II. RISK OF LOSS OF RIGHTS WHEN USING ChatGPT?

ChatGPT – *API* or *ChatGPT-Enterprise* to mitigate the risk?

- ChatGPT or other AI tools may be able to comprehensively and precisely describe and display prior art
- High awareness of personal data, but not tailored to trade secrets
- After the Samsung incident announcement of a business version and inclusion of the possibility to disable chat history
- In the API application of ChatGPT and ChatGPT Enterprise, data is not used for training purposes
- But: security gaps and bugs are still possible



II. RISK OF LOSS OF RIGHTS WHEN USING CHATGPT?



Research ▾ API ▾ ChatGPT ▾ Safety Company ▾

Search Log in ↗

Get started ↗

OpenAI – T&C

Model training FAQ

How does OpenAI train its models?

OpenAI trains its models in two stages. First, we learn from a large amount of data. Then, we use data from ChatGPT users and human trainers to make sure the outputs are safe and accurate and to improve their general capabilities. [Learn more about our training process.](#)

What sources of data are used for training OpenAI models?

OpenAI uses data from different places including public sources, licensed third-party data, and information created by human reviewers. We also use data from versions of ChatGPT and DALL-E for individuals. **Data from ChatGPT Enterprise and the API Platform (after March 1, 2023) isn't used for training our models.**

Need more help?

If you have further questions or require assistance, please reach out to our support team via our [Help Center](#).

II. RISK OF LOSS OF RIGHTS WHEN USING CHATGPT?

OpenAI Research API ChatGPT Safety Company Search Log in Get started

Compare ChatGPT plans

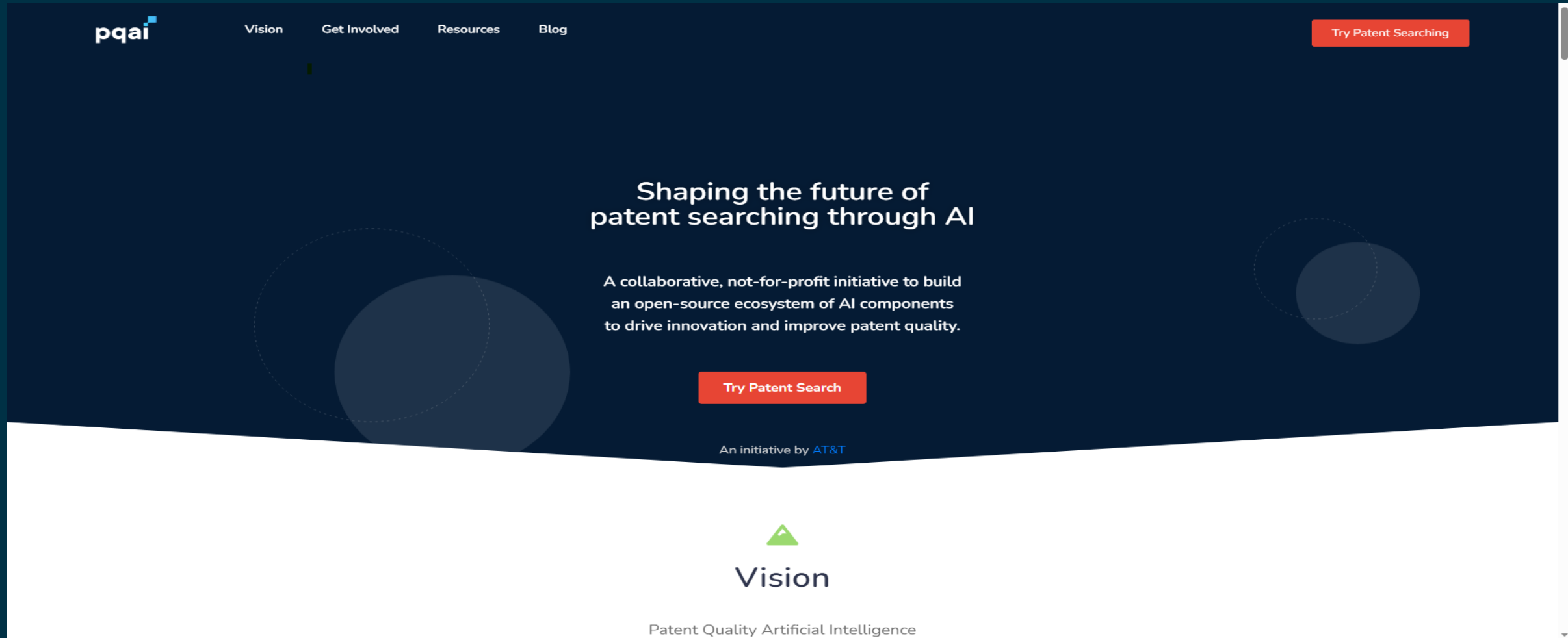
Free	Plus	Enterprise
\$0 per person/month	\$20 per person/month	
Try it now ↗	Upgrade now ↗	Contact sales
Everything in Free, and:	Everything in Free, and:	Everything in Plus, and:
<ul style="list-style-type: none">✓ GPT-3.5✓ Regular model updates	<ul style="list-style-type: none">✓ GPT-4*✓ Advanced Data Analysis*✓ Plugins*✓ Early access to beta features	<ul style="list-style-type: none">✓ Unlimited high-speed GPT-4*✓ Longer inputs with 32k token context✓ Unlimited Advanced Data Analysis✓ Internally shareable chat templates✓ Dedicated admin console✓ SSO, domain verification, and analytics✓ API credits to build your own solutions✓ Enterprise data is not used for training

*Usage capped at 50 messages every three hours

*Actual speed varies depending on utilization of our systems

II. RISK OF LOSS OF RIGHTS WHEN USING ChatGPT?

AI-driven Prior Art Search – pqai (<https://projectpq.ai/>)



The screenshot shows the homepage of the Project PQ AI website. The background is dark blue with abstract circular patterns. The top navigation bar includes the 'pqai' logo, links for 'Vision', 'Get Involved', 'Resources', and 'Blog', and a red button labeled 'Try Patent Searching'. The main content area features the headline 'Shaping the future of patent searching through AI' and a sub-headline: 'A collaborative, not-for-profit initiative to build an open-source ecosystem of AI components to drive innovation and improve patent quality.' Below this is another red button 'Try Patent Search'. At the bottom, it states 'An initiative by AT&T' and features the 'Vision' logo (a green triangle) and the text 'Vision Patent Quality Artificial Intelligence'.


pqai Vision Get Involved Resources Blog [Try Patent Searching](#)

Shaping the future of patent searching through AI

A collaborative, not-for-profit initiative to build an open-source ecosystem of AI components to drive innovation and improve patent quality.

[Try Patent Search](#)

An initiative by [AT&T](#)


Vision
Patent Quality Artificial Intelligence

II. RISK OF LOSS OF RIGHTS WHEN USING CHATGPT?

How PQAI maintains user privacy?

By [PQAI Staff](#) | In [FAQ](#) | [Leave a comment](#)

When you use PQAI for running prior-art searches, you can rest assured that PQAI **provides you complete privacy.**

Unlike most search engines, which track everything you do, **PQAI never tracks or saves your search data.** We believe that it is very much needed for a platform like PQAI, which is used by many inventors to validate the novelty of their ideas.

When you enter a search query on PQAI, it goes to our server in the cloud on a secure, encrypted link. The server finds the results matching your query from its database, and sends them off back your way. **After this, no traces of your query are left on the server.**

(This policy of never storing user search queries is also mentioned on PQAI's [search page](#) – see the link at the bottom of the page.)

Please note even though we don't track user data, we do store few anonymous traffic statistics such as number of requests. This helps us scale our servers appropriately to handle the traffic, deter abuse, and understand how people find value on our platform.

How do we train our AI?

Another question is whether our AI learns from user behavior? The answer is – no. The fact that we don't track or save search data makes it impossible for us to train our AI on it.

But that leads to another question: how do we train it then? The answer is: patent office examination data.

We download the examination data that is routinely published by the USPTO on their website, then we process it to create training datasets for our AI. Many contributors from the open source community have helped us in this process.

II. RISK OF LOSS OF RIGHTS WHEN USING CHATGPT?

All Prior Art / All The Claims – Patents As An Open-Source Project

All Prior Art
Algorithmically generated prior art

Prior Art **Publications** About Contact

Publications

Publications, each of 10,000 inventions

Current total:
4,220,000 inventions

[Current torrent](#)

[All Prior Art Volume 1](#)
[All Prior Art Volume 2](#)
[All Prior Art Volume 3](#)
[All Prior Art Volume 4](#)
[All Prior Art Volume 5](#)
[All Prior Art Volume 6](#)
[All Prior Art Volume 7](#)
[All Prior Art Volume 8](#)
[All Prior Art Volume 9](#)
[All Prior Art Volume 10](#)
[All Prior Art Volume 11](#)
[All Prior Art Volume 12](#)

Search ...

All The Claims
Algorithmically generated claims as prior art

Claims About Publications Contact

1461189017-69dc6a61-7dae-4dd5-b591-5a18c6996c0e

Search ...

1. A filtering chip conveyor comprising:
a conveyor tank arranged to retain cutting fluid containing chips,
a continuous conveyor belt at least partly disposed inside the conveyor tank, the belt being arranged to rotate and to turn at a tail end and at a discharge end, with a space between upper and lower flights of the belt, so as to transport chips on the upper flight towards the discharge end, to be discharged off the conveyor,
at least one filter box arranged between the upper and the lower flights of the belt,
at least one filter plate arranged in the filter box, the filter plate comprising a filtration region having a plurality of openings for permitting cutting fluid to pass through the filter plate while not permitting chips whose smallest sectional chip dimension is larger than a predetermined maximum chip dimension, to pass through the filter plate,
wherein:
the at least one filter plate has a thickness of less than 0.3 mm,
the openings include an array of profiled orifices etched through the filter plate, the etched orifice profile being such that the smallest sectional

Safety Precautions When Using AI



III. SAFETY PRECAUTIONS WHEN USING AI

- Although OpenAI does not store any data entered for training purposes within the framework of the API applications, there are overarching security concerns (Samsung incident, bugs, etc.)
- Companies that want to use ChatGPT need to implement compliance policies and training
- Use ChatGPT Enterprise Version or API
- Disable prompt history
- Caution (but inherent anyway): AI can always produce incorrect results



Thank you



Contact



Dr. Johannes Graf Ballestrem, LL.M.
Partner
Germany

+49 221 5108 4394

johannes.ballestrem@osborneclarke.com

Dr Johannes Graf Ballestrem is a patent litigator with a strong focus on technology involving mechanics, electronics, information technology and 'access to data' claims. He has outstanding experience in litigation concerning printer consumables, automotive supplies, remanufacturing and software implemented inventions.

Johannes has specialized in patent law for over 15 years. After working in the patent litigation department of a leading international law firm in Dusseldorf, he joined Osborne Clarke and became partner in 2019. During his career, he has taken part in a wide range of patent litigation cases in the field of telecommunications, mechanics and software. Johannes also regularly advises in M&A transactions and licensing. He has particularly deep experience in the automotive and energy sector.

Johannes represents clients before the civil courts as well as in arbitration and participates in parallel validity proceedings before the European Patent Office, the Federal Patent Court and the Federal Supreme Court.

You can find the answers to the most frequently asked questions on the subject of Patent Litigation in Germany [here](#).

