TimeDrop.01

March 2025

March 2062

VEIL MAGAZINE

"We choose to go to the Moon in this decade and do the other things, not because they are easy, but because they are hard" J.F. KENNEDY

From Intelligence to Inefficiency

How AI Degradation Strikes Business

AI at the Doorstep:

How Websites Decide Who Gets In

Tracking Technologies:

Should You Choose to Accept Them

The EU AI Act:

Dodge, Comply, or Rewrite?

The Antikythera Mechanism:

The Prehistoric Computer That Foretold the Rise of AI

Towards AI Co-Associate

ChatGPT's Edition

…content loading…

WELCOME TO THE VEIL

The "Veil" is the invisible barrier in spacetime.

The "Veil" is an initiative designed to curate, preserve, and refine legal insights across time.

0%

100%

DATA

AI at the Doorstep:

How Websites Decide Who Gets In

Tracking Technologies:

Should You Choose to Accept Them

AI

From Intelligence to Inefficiency

How AI Degradation Strikes Business

The EU AI Act:

Dodge, Comply, or Rewrite?

INNOVATION

The Antikythera Mechanism:

The Prehistoric Computer That Foretold the Rise of AI

Towards AI Co-Associate

ChatGPT's Edition

THIS IS NOT JUST A MAGAZINE

"Intellectual Property and Data are not merely resources.
AI and Innovations are more than tools."

At some point between your present and our now, a critical moment was lost. A precedent was ignored. A law was written, erased, rewritten, and forgotten again. By the time anyone realized what had happened, it was too late to undo it.

The legal and technological choices made in the past shape the future and define the destiny of the world. It is still within your power to create change and alter the chain of events that led to the collapse of reality.

// status	SUCCESSFUL TIMEDROP
// integrity	93% (minor distortions detected)
// message log	March 2062
// description key	Not required

It's a *TimeDrop*

In 2062, an unknown phenomenon, later called the "TimeDrop", disrupted the flow of reality. This event fractured the "Veil" of reality, allowing fragments of the future to cascade back. The world became a patchwork of temporal inconsistencies, where knowledge from the 21st century could appear in medieval times, and ancient manuscripts might emerge in the distant future.

There were those who used TimeDrop for their own goals.

One of the future actors was **CLAIMS Legal Intelligence**, an evolution of **CLAIMS International Intellectual Property Consulting Firm**, which in your present time operates at claimsip.com.

What is *Veil Magazine* about?

Veil Magazine is a summary of important insights and critical knowledge on Data // Privacy, AI // Innovation, and Intellectual Property regulations. The articles in *Veil Magazine* were written in 2025 by those who lived there but dreamt about the future. The irony is that the compiled materials weren't published until 2062, when CLAIMS Legal Intelligence discovered the message of their predecessors and completed their work.

They sent this copy of *Veil Magazine* back to our future and their past, creating a completely different timeline.

// Veil Curios	Veil Magazine (x1) Antikythera Mechanism (x2)
	Additional messages detected in nearby spacetime
// source	CLAIMS Legal Intelligence – Future Archive Division

What are *Veil Curios*?

Veil Curio is a collectible knowledge artifact linking this message to past and future. With Veil Curios, CLAIMS Legal Intelligence delivers historical legal knowledge, predictive analysis, and insights once thought impossible through time. This Episode is accompanied by an interactive 3D model of the Antikythera Mechanism, representing both the past and the future of predictive intelligence.

Future

What comes next? Veil is not a closed archive. It is an expanding system. Other Veil Magazines and Veil Curios exist, and more are on their way. Some are already embedded in your timeline, waiting to be found. Others may require action on your part to retrieve. We invite you to engage, explore, and question. The future is shaped by those who prepare for it. Let's build it together.

…CONTENT UNLOCKED…
…YOUR JOURNEY BEGINS…

Veil Curio

In 1901, Greek sponge divers near Antikythera found a corroded bronze and wood artifact within a shipwreck.

What seemed unremarkable was, in fact, one of history's greatest technological enigmas, which was named as the Antikythera Mechanism.

Discover the Antikythera Mechanism in a brand-new way.

Our Wallet Card provides instant access to:
- A 3D interactive model of the Antikythera Mechanism, accessible via the Wallet Card's QR code.
- Official CLAIMS resources (the website and LinkedIn), accessible via the Wallet Card's link.

Keep our Veil Curio collectible with you and show it to your friends!

Access 3D-model of Antikythera Mechanism directly!

Save the Antikythera Mechanism to your Wallet

AI AT THE DOORSTEP

HOW WEBSITES DECIDE WHO GETS IN?

Author:

Anastasiia Maklakova // LinkedIn

// original March 2025
// archived March 2062
// source **CLAIMS Legal Intelligence – Future Archive Division**

The ever-growing AI industry brings new legal and ethical challenges regarding how AI uses website content to learn, as well as how organizations use AI in the production and distribution of their products.

With the rise of generative AI, the demand for content used to train models has skyrocketed. The web is AI systems' main source of data for learning.

One way to obtain data is by scraping the internet using AI crawlers. These bots download and index content from all over the internet. Such bots aim to understand what every webpage is about so they can retrieve the information when needed.

The Good (Bot), the Bad (Bot), and the Restrictions

It is common to divide AI bots into "good" and "bad" ones:

- **"Good" bots** perform useful or helpful tasks, like scanning content or interacting with webpages. Good bots do not harm a user's experience on the internet.
- **"Bad" bots** are designed to violate the rights of website owners and users. They assist in copyright infringements, privacy violations, and unfair trading.

One sign that a bot isn't "good" is its bypassing of a website owner's restrictions. One such restriction is the robots.txt file. This tool allows website owners to direct web crawlers on their website and avoid unnecessary attention to specific pages or the entire site.

However, robots.txt is only effective against those bots that follow the rules—i.e., "good" bots. The robots.txt file cannot prohibit the indexing of a webpage. It merely provides an instruction that a bot may or may not follow. Malicious "bad" bots pose a clear threat to websites and, more importantly, to human rights. This is why they should be banned.

Certain sites are already actively promoting advanced tools to block such bots.

Popular Bots:

- OpenAI's GPTBot
- Applebot
- CCBot
- Googlebot
- Amazonbot
- Claudebot
- Bytespider

AI AT THE DOORSTEP

HOW WEBSITES DECIDE WHO GETS IN?

25%

of the most critical online data sources are inaccessible to AI crawlers

However, even “good” bots that serve the highest purpose of humanity—technological development and human prosperity—are under attack.

Web owners are leveraging every tool at their disposal, such as the robots.txt file and specific clauses in Terms of Service, to restrict AI access to their content.

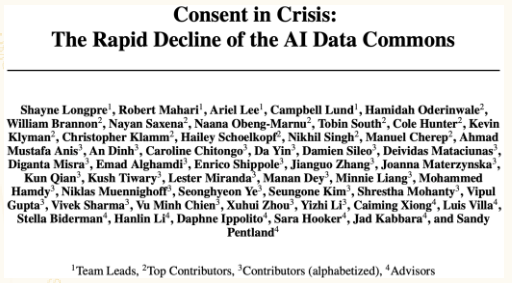
Research from the article “Consent in Crisis: The Rapid Decline of the AI Data Commons”, **between April 2023 and April 2024, approximately 25% of the most critical online data sources became inaccessible to AI crawlers**. This percentage feels significant, particularly when one frequently hears about the lack of quality data to further improve models or about synthetic data’s limitations, along with other predictions warning of the AI sector’s eventual decline.

According to the same research, the percentage of those opposing AI bots might have been lower. The problem is that, in many cases, website owners fail to effectively articulate their preferences on how their data should be used by AI systems.

Recent studies reveal a paradox:
the AI web crawlers that are blocked the most are not necessarily the most active ones.

For example, while the most aggressive AI bot is Bytespider (a web crawler operated by ByteDance, the Chinese owner of TikTok), reportedly achieving scraping volumes 25 times higher than OpenAI’s GPTBot, websites tend to block OpenAI’s web crawler more frequently.

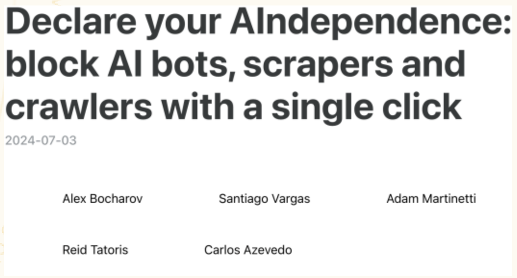
Many users may not even be aware of the more aggressive AI bots actively crawling their sites.



Consent in Crisis:
The Rapid Decline of the AI Data Commons

Shayne Longpre[1], Robert Mahari[1], Ariel Lee[1], Campbell Lund[1], Hamidah Oderinwale[2], William Brannon[2], Nayan Saxena[2], Naana Obeng-Marnu[2], Tobin South[2], Cole Hunter[2], Kevin Klyman[2], Christopher Klamm[2], Hailey Schoelkopf[2], Nikhil Singh[2], Manuel Cherep[2], Ahmad Mustafa Anis[3], An Dinh[3], Caroline Chitongo[3], Da Yin[3], Damien Sileo[3], Deividas Mataciunas[3], Diganta Misra[3], Emad Alghamdi[3], Enrico Shippole[3], Jianguo Zhang[3], Joanna Materzynska[3], Kun Qian[3], Kush Tiwary[3], Lester Miranda[3], Manan Dey[3], Minnie Liang[3], Mohammed Hamdy[3], Niklas Muennighoff[3], Seonghyeon Ye[3], Seungone Kim[3], Shrestha Mohanty[3], Vipul Gupta[3], Vivek Sharma[3], Vu Minh Chien[3], Xuhui Zhou[3], Yizhi Li[3], Caiming Xiong[4], Luis Villa[4], Stella Biderman[4], Hanlin Li[4], Daphne Ippolito[4], Sara Hooker[4], Jad Kabbara[4], and Sandy Pentland[4]

[1]Team Leads, [2]Top Contributors, [3]Contributors (alphabetized), [4]Advisors

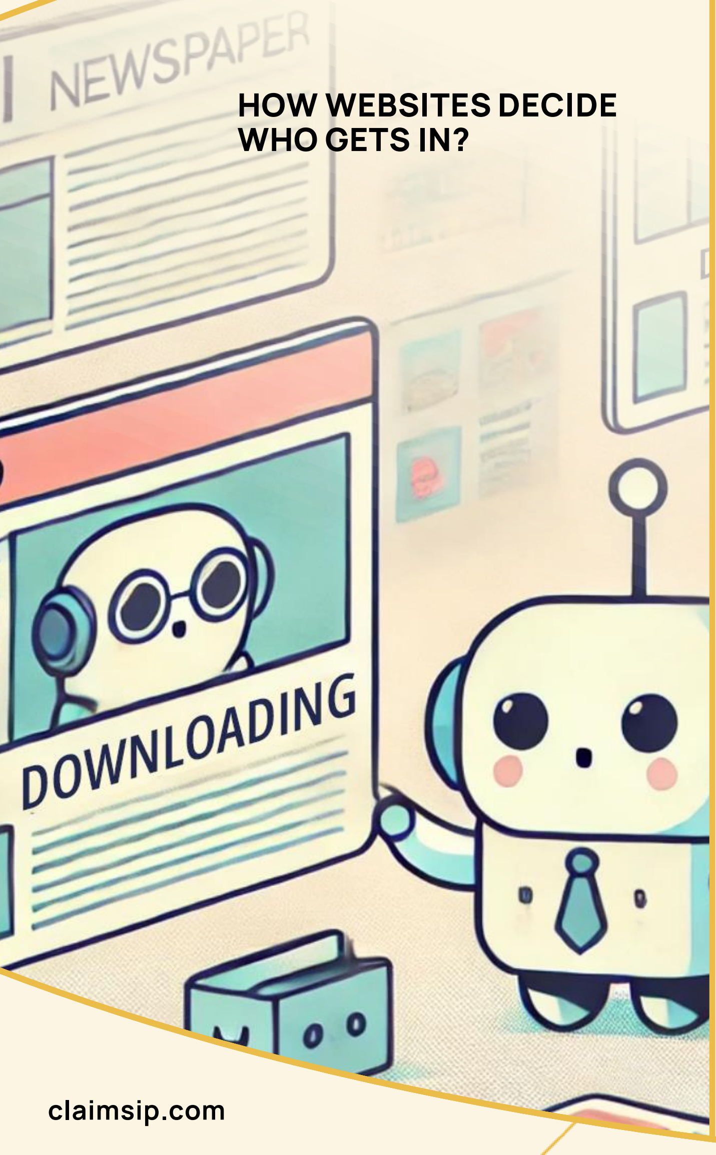


Declare your AIndependence: block AI bots, scrapers and crawlers with a single click

2024-07-03

Alex Bocharov
Santiago Vargas
Adam Martinetti
Reid Tatoris
Carlos Azevedo

AI AT THE DOORSTEP



HOW WEBSITES DECIDE WHO GETS IN?

AI, News, and Courts

AI companies, the leaders of modern progress, raise concerns among website owners and provoke intense disputes. When data holders do not want their web data to be used by AI companies, even for the legitimate and socially significant purpose of improving AI models, they have the right to demand that their rights be respected. ***Don't they?***

In December 2023, The New York Times filed a lawsuit against OpenAI and Microsoft for copyright infringement. In November 2024, a group of Canadian news outlets—including CBC/Radio-Canada, Postmedia, Metroland, The Toronto Star, The Globe and Mail, and The Canadian Press—followed suit, launching a lawsuit against OpenAI on similar grounds.

The main complaints in both cases are:

1. AI companies are violating copyright when scraping data from websites.
2. Extracting key information from news articles shifts web traffic away from news sites to AI chatbots. As a result, news agencies see a decrease in advertising and subscription revenue, while AI developers benefit.
3. AI "hallucinations" create an aura of mistrust regarding the news sources AI refers to.

OpenAI is not the only target. Similar lawsuits have been filed against Microsoft, Perplexity, and Anthropic. **While most website owners share these concerns, why have legal challenges been rare until now?**

A possible answer is that companies feared being the first to sue and losing their case. It is likely that once the first ruling goes against an AI company, lawsuits will become more frequent.

Gladly, we recently had the first winning ruling in the Delaware State and the first winning ruling in Germany. **But who's winning?**

AI AT THE DOORSTEP

HOW WEBSITES DECIDE WHO GETS IN?

In the U.S., the Thomson Reuters vs. ROSS Intelligence case set a decisive precedent by ruling that using Westlaw's proprietary headnotes to train an AI model constitutes copyright infringement, especially when the AI product competes directly with Westlaw, leaving the fair use defense untenable.

Conversely, in September 2024, the Regional Court of Hamburg in Germany offered a different perspective.

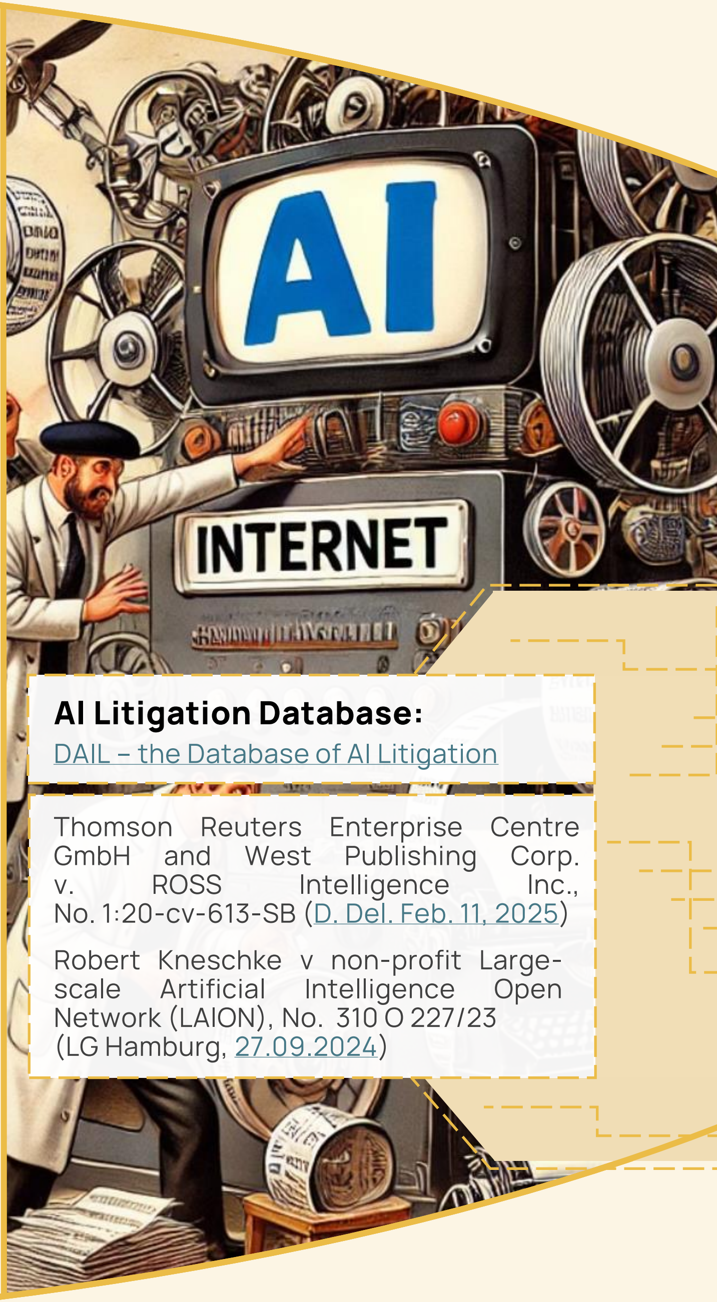
The court determined that an AI research association's compilation of a vast image-text dataset, including a watermarked photograph, fell within the scope of text and data mining exceptions for scientific research. This decision rested on the fact that the image was publicly accessible, and its copyright restrictions were not embedded in a machine-readable format.

Together, these rulings illustrate that uncertainty still lingers in the legal landscape for AI training on copyrighted material. Each decision was based on a specific set of circumstances, meaning that while these cases provide important insights, they do not necessarily resolve the broader disputes, such as the ongoing lawsuits between news media outlets and OpenAI, which involve different factual contexts.

Maybe, a deal?

While most news publishers fear that AI bots could threaten their industry, not everyone shares these concerns. If one strategy for website owners is to fight against AI companies, another is to opt for cooperation.

Axel Springer (POLITICO, Business Insider, BILD, and WELT) is going against the trend for news publishers by announcing a global partnership with OpenAI. Through this deal, ChatGPT users will receive summaries of selected global news content from Axel Springer's media, with attribution and links to the full articles for transparency and further information. French Le Monde and Spanish Prisa Media have also partnered with OpenAI.



AI Litigation Database:
DAIL – the Database of AI Litigation

Thomson Reuters Enterprise Centre GmbH and West Publishing Corp. v. ROSS Intelligence Inc., No. 1:20-cv-613-SB (D. Del. Feb. 11, 2025)

Robert Kneschke v non-profit Large-scale Artificial Intelligence Open Network (LAION), No. 310 O 227/23 (LG Hamburg, 27.09.2024)

AI AT THE DOORSTEP

HOW WEBSITES DECIDE WHO GETS IN?

AI Dolce Vita

The Italian media conglomerate GEDI Gruppo Editoriale sought to collaborate with OpenAI by providing editorial content for AI training. However, given OpenAI’s history of regulatory scrutiny in Italy—including a temporary ban in 2023 and a €15 million fine in 2024—such initiatives are under close watch by the Italian Data Protection Authority (Garante).

In a recent decision, the Garante warned GEDI that its agreement with OpenAI raises compliance concerns under the GDPR. Whether this rigorous oversight strengthens data protection for Italian residents or stifles technological progress remains open to debate. However, one thing is clear: it creates significant compliance hurdles for AI companies operating in the Italian market.

Another deal?

Not only do some websites allow AI to access their content, but they also put AI to their own use. For some, creating and developing their own AI tools is becoming a strategic option.

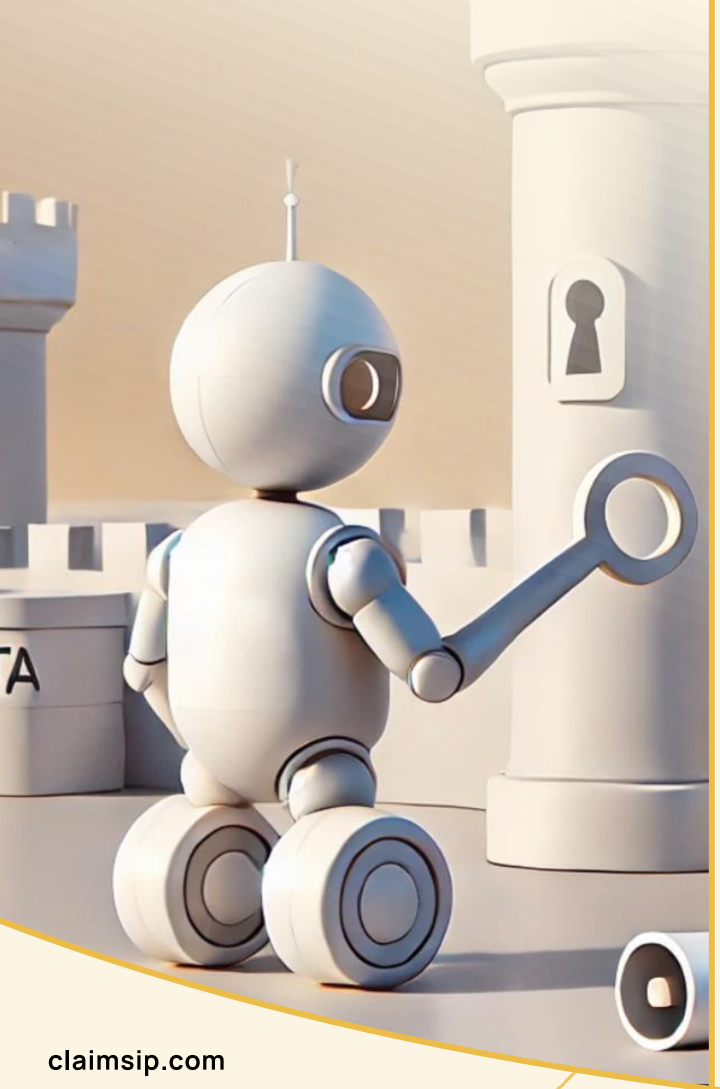
News agencies such as The Associated Press and Bloomberg are already using AI to eliminate repetitive tasks and allow journalists to focus on higher-impact reporting. Bergens Tidende in Norway conducts customer satisfaction surveys on its website using AI.

India Today has created an AI news anchor, Sana, who delivers news headlines alongside their main TV anchor. These are just a few examples of websites deploying their own AI tools.

On one side, there is significant creative, human, and financial investment made by creators and website owners. If AI developers do not seek permission or provide compensation for scraped data, human creativity, truthful content, and the rights of creators and website owners will inevitably suffer.

AI AT THE DOORSTEP

HOW WEBSITES DECIDE WHO GETS IN?



On the other side, web data scraping fuels AI with diverse texts, images, and videos—improving efficiency and increasing data accessibility. Scale and data matter, and very few sources provide public-scale data like the web does.

While AI models could be trained on alternative data sources, big companies are already turning to synthetic data. However, some studies suggest that training on poor-quality synthetic data can degrade AI model performance.

The most recent regulation addressing this issue is the EU AI Act. While the AI Act does not directly regulate the relationship between web data holders and AI companies, it does attempt to find a balance—one that could be extended to other jurisdictions in the future.

It states that if rightsholders decide to reserve their rights to prevent text and data mining (i.e., opt-out), model providers must obtain their authorization to use such protected content. This presumption of consent could be a great solution for both data holders and AI developers. However, it remains unclear how web data owners should articulate their rights, which could lead to potential abuses by AI companies.

Since the robots.txt file is not legally binding, the most effective solution would be to establish a legal mechanism for protection. Possible approaches include: DMCA strikes based on the circumvention of copyright protection systems.

Explicitly defining access restrictions for AI bots in website Terms of Use and raising fines for violations. Addressing the issue through fair competition law.

What's next?

As we can see, an effective way to oppose AI bots hasn't been discovered yet. Except, perhaps, one: negotiation and finding mutually beneficial arrangements.

IP-MANIFESTO

It is 100 years as of the announcement of the Surrealist Manifesto!

What a perfect time to investigate different issues in the work of the surrealistic authors. These issues are still actual. in particular for intellectual property laws, which should be improved based on the surrealistic art experience.

Our goal is to attract public attention to the importance of creation of new principles and approaches which will ensure proper new balance of rights and efficient mechanisms of its protection for all art world market participants.

Read and join via the link!

TRACKING TECHNOLOGIES:

SHOULD YOU CHOOSE
TO ACCEPT THEM

Author:

Mikita Piatrou // LinkedIn

// original March 2025
// archived March 2062
// source **CLAIMS Legal Intelligence – Future Archive Division**

Various tracking technologies (cookies, SDKs, and tracking pixels) are essential tools that power the digital experiences we engage with every day. They help businesses track user behaviour, personalise experiences, and serve up ads that actually make sense.

But with great power comes great responsibility — especially when it comes to data privacy.

Why is it important?

Well, first of all, legal penalties for non-compliance can be steep, and nobody wants to hand over a chunk of their budget because they missed a cookie consent banner. It may feel like just a rumour that someone got fined—until the authorities launch an investigation and impose a hefty fine you never imagined could happen to you.

Second, if data is the new oil, trust is the currency needed to access this valuable resource. Consumers are increasingly concerned about privacy, and businesses that fail to earn their trust risk a data drought. Without trust, you'll lose loyal customers faster than you can say "opt-in".

Finally, staying compliant isn't just about ticking boxes—it's a way to stand out in a crowded market. Being upfront about how you handle data builds credibility and can give your business a serious edge. Plus, it saves you from the headache of legal disputes that no one has time for.

Key Definitions:

Cookies:
Small text files stored on a user's device when they visit a website. Think of them as the website's memory—without cookies, the web would be far less personal and efficient.

SDKs (Software Development Kits):
Collections of tools and libraries used by developers to integrate specific functionalities into mobile apps or websites. These tools enable features like push notifications, payment systems, and user behaviour tracking.

Tracking Pixels:
Small, invisible images embedded in web pages or emails. They track user actions such as ad clicks, form submissions, or email opens. Tracking pixels are widely used for analytics and retargeting advertising.

TRACKING TECHNOLOGIES:

SHOULD YOU CHOOSE TO ACCEPT THEM

This article will take you through these technologies, the legal landscape, and how to navigate everything with care and confidence—all while boosting your business. Let's dive in!

The issue isn't the existence of these technologies, but their use.

While essential for online functionality and marketing, these technologies store information on users' devices and track their actions—often without their full awareness, unless the app developer or website owner explicitly says,

"Hey! You didn't know, but we use tracking technologies."

As these tools evolved from simple usability enhancements to methods for targeted advertising, behavioural profiling, and cross-site tracking, their impact on user privacy became a significant concern.

To ensure privacy rights for everyone online—rather than relying on businesses' good faith—legal regulations were introduced.

Thanks to laws developed over 20 years ago in Europe, what once started as a courtesy question now sounds much more user-friendly:

"Hey! You didn't know, but we may use tracking technologies. Will you allow us to do this? If not, no problem—the website will still work properly."

Let's check the status of legal regulation around the world.

Regulatory landscape

The regulation falls into **two main categories:**

Data protection

Device protection

TRACKING TECHNOLOGIES:

SHOULD YOU CHOOSE TO ACCEPT THEM

Examples of Data protection regulation:

General Data Protection Regulation (GDPR) – EU

California Consumer Privacy Act (CCPA) – California

Lei Geral de Proteção de Dados (LGPD) – Brazil

Countries like

- *the US, Brazil,*
- *the UAE, Saudi Arabia,*
- *Nigeria,*
- *Australia, Singapore,*
- *China, South Korea, and Japan*

have strong data protection laws but lack specific device protection regulations.

Data protection regulation focuses on the processing of personal data (information), requiring businesses to access and use this data with respect for individuals' rights. It prevents misuse of personal data and requires businesses to have a valid legal basis for processing (e.g., consent).

Device protection regulation regulates unauthorised access and tracking, even when personal data is not involved. It requires businesses to obtain user's consent before deploying non-essential tracking technologies.

Remember!
There is no consent without knowledge on what's going to happen.

Many countries have data protection laws, but not all have device protection laws. As a result, businesses in these regions must comply with data protection laws but may not need to follow device protection rules.

Steps to compliance:

1. Understand how you are regulated
Businesses must first identify which laws apply to their operations, based on both: business location anв its users' location.

While the one-size-fits-all compliance solutions may seem appealing, your priority should be to comply with the specific regulations that apply to your business.

EU vs US Approach:
If a business operates in the EEA, it is subject to EU rules, even if it is not based there. See the Microsoft case: Dutch Court Decision and summary in English.

If a business operates only in the US, EU laws do not apply. For example, a Texas-based company serving only Houston does not need EU-style cookie banners.

Examples of Device protection regulation:

ePrivacy Directive – EU

Canada's Anti-Spam Legislation (CASL) – Canada

Authorities' Recommendations – Israel

Due to global business practices, consent banners are now widely used.

In some cases, businesses fail to provide a cookie policy or consent banner. Is this a violation? Not necessarily.

Online tracking laws vary, and some websites are not subject to such a requirement.

TRACKING TECHNOLOGIES:

SHOULD YOU CHOOSE TO ACCEPT THEM

Examples of Essential cookies:

- Protection against bots and web traffic security
- Determination of a user's country to serve the appropriate website version
- Management of user authentication across different services
- Maintenance of a session for logged-in users and tracking of shopping cart items

Examples of Non-Essential cookies:

- Personalization of ads based on browsing activity
- Measurement of interactions with embedded media content
- Tracking of engagement with social media content across websites
- Monitoring of interactions with customer support chatbots
- Analysis of user preferences for content recommendations

2. Understand the limitations of the applicable laws
Being subject to EU regulation is not a verdict.
See the article "The EU AI Act: Dodge, Comply, or Rewrite", page 25.

Not all use of tracking technologies require consent.
Some cases are exempt from consent requirements depending on the purpose of technology usage.

Essential Cookies are necessary for the basic operation of a website. These cookies, such as those that maintain user sessions, shopping cart data, or provide security features, do not require consent. These cookies can be set without obtaining user consent but must still be disclosed.

Non-Essential Cookies are used for purposes like analytics, advertising, and personalization. These cookies require consent before they can be placed on a user's device. These cookies must be disclosed and require users to opt-in.

Be aware!
Consent banner by its own doesn't create a system within the company for ongoing tracking users' opt-ins and opt-outs.

3. Understand your obligations under the applicable laws
Universally, the main legal obligations are:

- **Transparency:** inform users about which technologies (not only cookies) are being used, the purpose of use, and how long the data will be retained. Provide users with a cookie policy or cookie banner that includes clear and easily understandable information.

- **Consent:** obtain consent for required scenarios through an opt-in mechanism (e.g., cookie banner) and allow users to manage their cookie preferences, either by category (e.g., analytics, marketing) or individually.

Cookie Banner Rules:

1. Users should be able to select specific categories of cookies they want to accept, such as analytics or advertising cookies, rather than having a single option to "accept all."

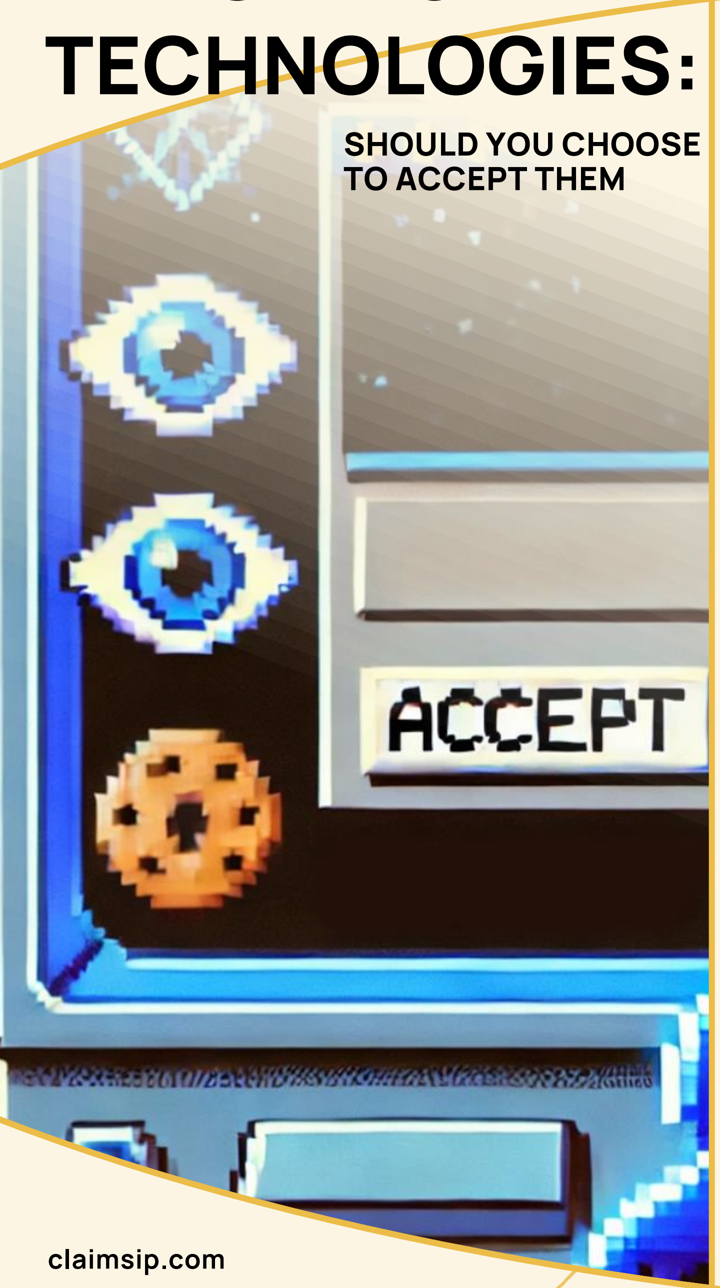
2. Cookie banners should appear when users first visit your website, allowing them to accept or reject non-essential cookies. If non-essential cookies are rejected, they should not be set, and no data should be collected from the user.

3. For third-party cookies, businesses must ensure that consent for these cookies is also obtained. It's crucial to provide users with the option to disable these cookies through the consent banner.

4. Users must be able to withdraw consent easily at any time. The process to withdraw should be as simple as granting consent.

TRACKING TECHNOLOGIES:

SHOULD YOU CHOOSE TO ACCEPT THEM

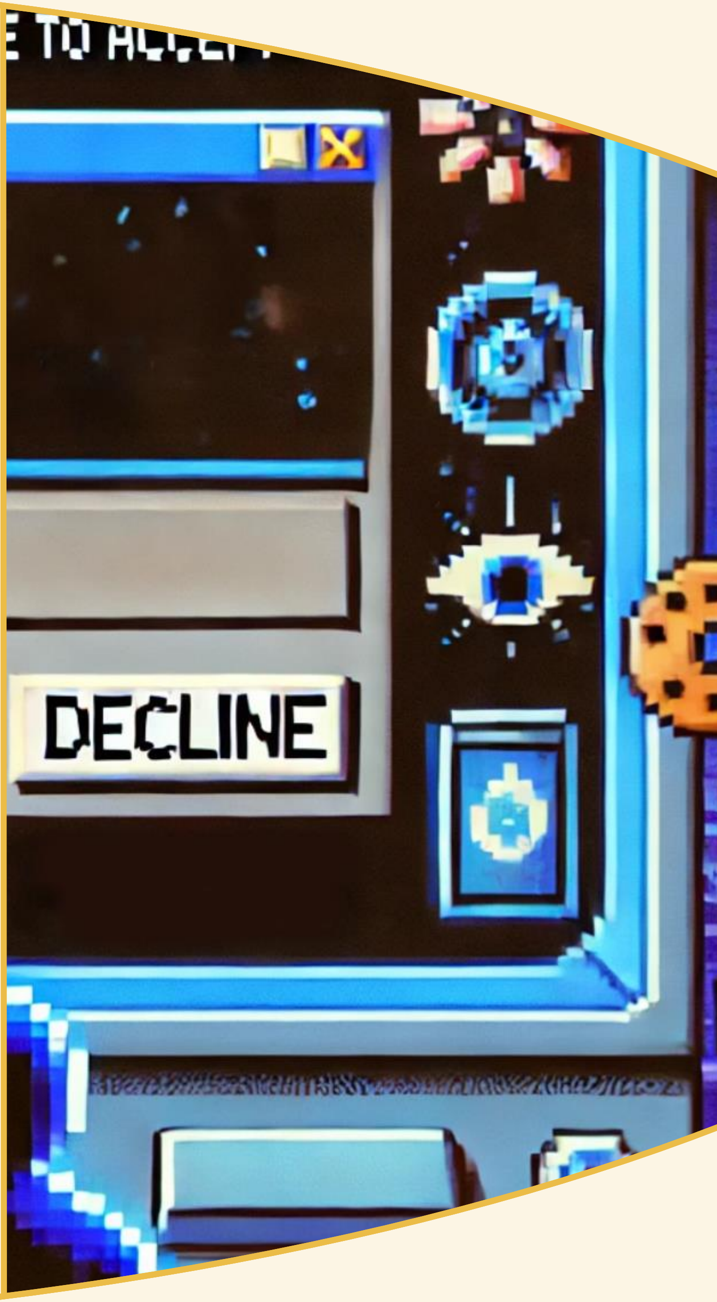


Conclusion

The complexity of cookie and tracking technology compliance doesn’t just arise from the legal obligations themselves but from the need to adapt and anticipate evolving user expectations. While the GDPR, CCPA, and other regulations set the framework for data protection and device privacy, the real challenge lies in integrating these practices into business strategy.

A critical takeaway is that cookie compliance is not a standalone task but a dynamic process that requires businesses to continuously monitor their data collection practices, consent mechanisms, and user interfaces. As we’ve seen, consent management goes beyond just "asking for permission"; it’s about offering control and choice to users in a manner that’s intuitive, transparent, and aligned with the core values of the business.

With consent banners everywhere demanding consumer’s attention without building real trust, shouldn’t businesses view privacy protection as a competitive advantage rather than just a compliance burden?



our projects

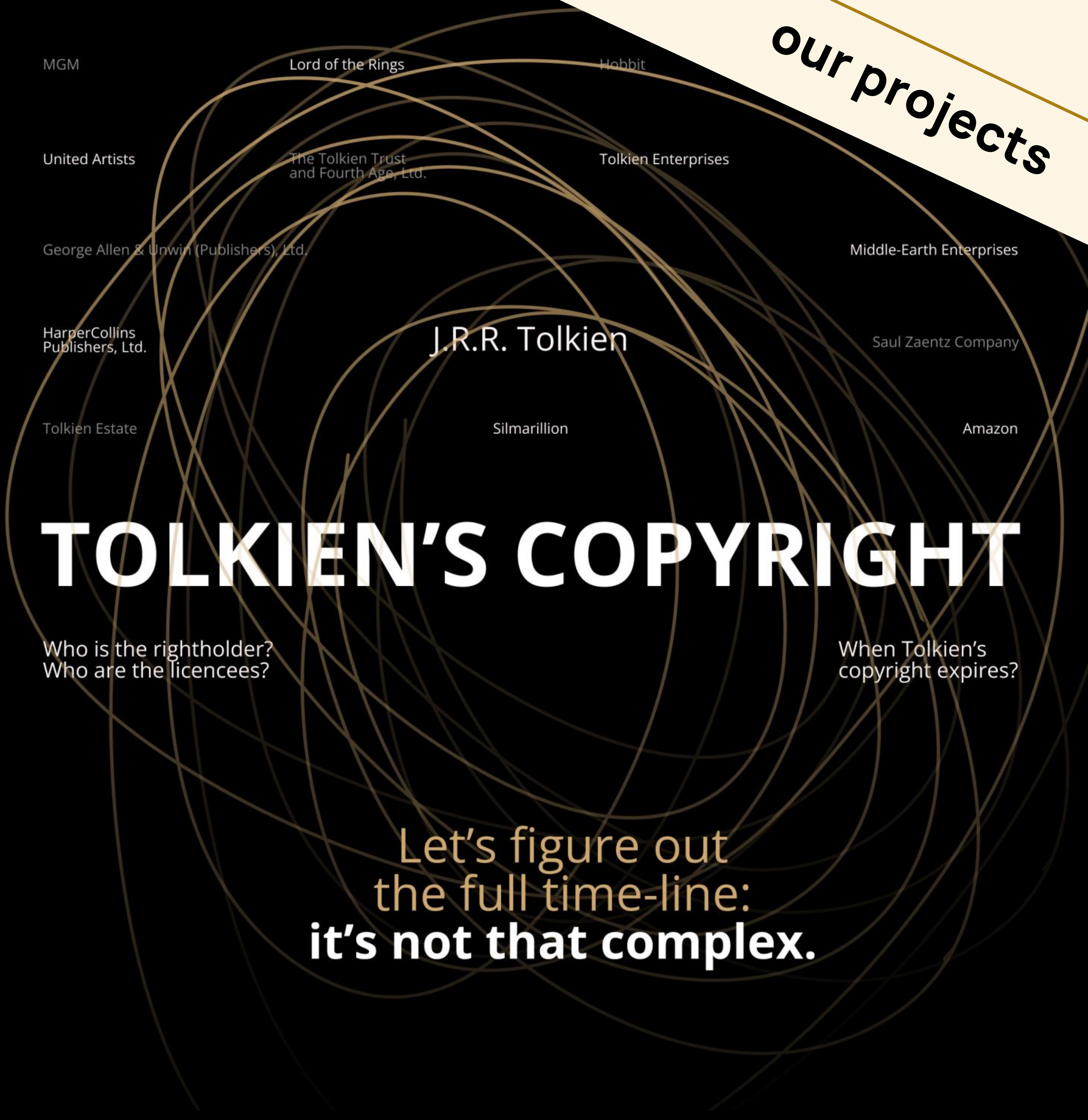
IP-TOLKIEN

Let us remind you we created the complete timeline of Tolkien's copyright: from books to films and even merchandise!

You will find out which companies "inherited" the rights to Tolkien's works, to whom the licensing rights to film adaptations of the professor's works were transferred in different periods, and, perhaps most importantly...

When will anyone be able to freely use:
The Lord of the Rings, The Hobbit and other works of the greatest fantasy author!

Read via the link!



TOLKIEN'S COPYRIGHT

Who is the rightholder?
Who are the licencees?

When Tolkien's copyright expires?

Let's figure out the full time-line:
it's not that complex.

FROM INTELLIGENCE TO INEFFICIENCY

HOW AI DEGRADATION STRIKES BUSINESS

Author:

Maya Prosvitlyuk // LinkedIn

// original March 2025
// archived March 2062
// source **CLAIMS Legal Intelligence – Future Archive Division**

Artificial intelligence (AI) has enormous potential to enhance business efficiency, improve customer service, and automate routine processes. Many companies, from startups to large corporations, are integrating AI technologies into their operations. However, as these technologies evolve, a new issue arises—AI degradation, also known as "model collapse," which is now being discussed not only at scientific conferences but also in business publications.

Over time, AI performance deteriorates until the model eventually becomes completely useless—this is known as model collapse.

Despite its significant impact on the long-term prospects of AI, particularly in a rapidly changing environment with increasing data dependence, this process remains under-researched and often underestimated.

Why is it important?

AI degradation is the process by which the efficiency and accuracy of AI models decline over time. This can occur due to various factors, including data obsolescence, environmental changes, and inherent model errors.

A particularly concerning aspect of this is "model collapse," a degenerative process affecting successive generations of generative models. As these models generate synthetic data, the next generation trains on increasingly polluted datasets, leading to a distorted perception of reality.

Business Adapts AI:

Ikea's Case

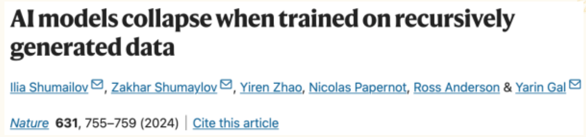
Ikea has replaced a significant part of its customer support staff with chatbots, reducing costs and wait times.

BlueFocus's Case

Chinese marketing firm **BlueFocus** has entirely replaced its copywriters with generative AI for content creation.

Goldman Sachs's Case

Goldman Sachs employs LLMs to automate programming and document creation, boosting productivity and reducing reliance on external tools.



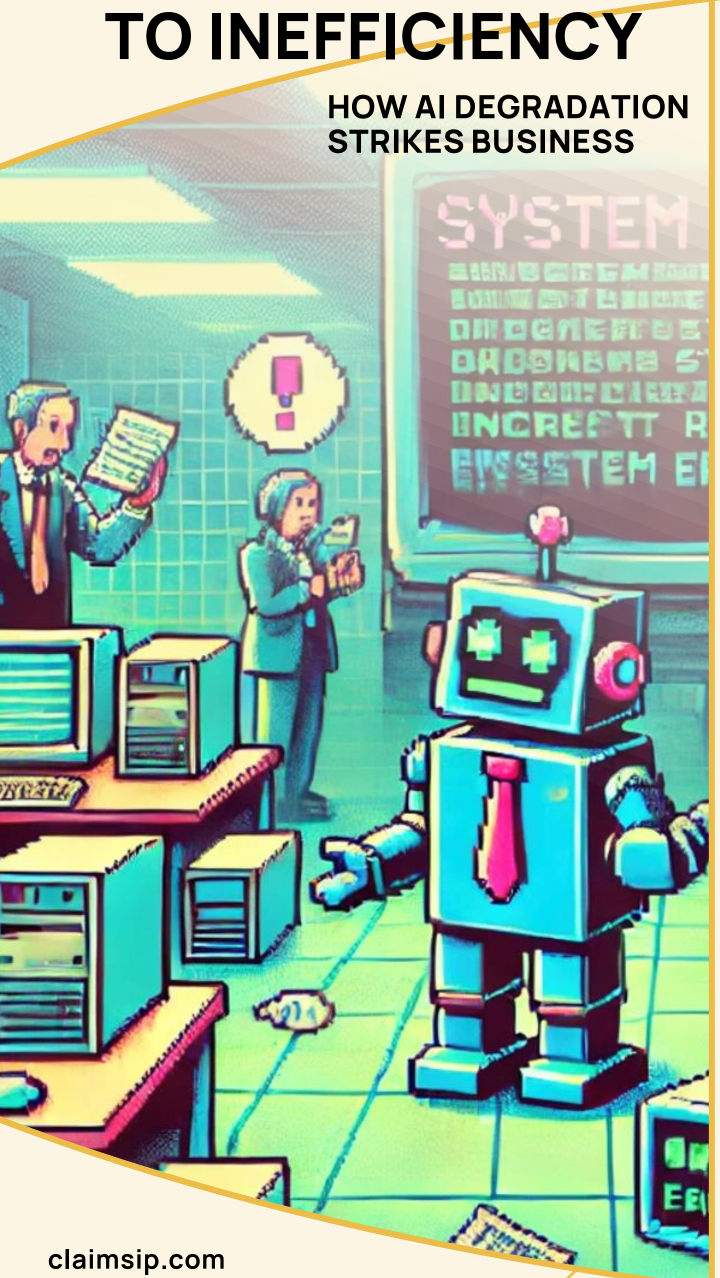
AI models collapse when trained on recursively generated data

Ilia Shumailov, Zakhar Shumaylov, Yiren Zhao, Nicolas Papernot, Ross Anderson & Yarin Gal

Nature **631**, 755–759 (2024) | Cite this article

FROM INTELLIGENCE TO INEFFICIENCY

HOW AI DEGRADATION STRIKES BUSINESS



Factors behind AI degradation

One of the primary causes of AI degradation is **data obsolescence**. As the environments in which AI operates evolve, training data may no longer accurately reflect reality, reducing the quality of AI-driven decisions. At the same time, many companies struggle to maintain model quality due to rapidly shifting data trend.

Furthermore, McKinsey notes that a significant percentage of businesses **lack clear AI management policies**, exacerbating the risks of degradation.

Regulatory and ethical restrictions on using human-created data for training also contribute to AI degradation. Due to restrictions on using human-generated data, developers increasingly rely on AI-generated data. Although synthetic data have potential, research indicates that when models train on recursively generated data—data produced by previous AI models—their ability to interpret reality degrades. This issue is particularly noticeable in the fine-tuning stage (the process of retraining a model on new data to tailor it to specific tasks). During this process, the model reconfigures its parameters for new tasks, while if the data contains errors, the model begins to strengthen them. As these errors intensify over several iterations of learning, the AI loses its ability to generate relevant responses.

Model collapse occurs when an AI model becomes overly reliant on specific features, leading to increasingly generalized or erroneous outputs. AI models may begin to overemphasize common elements in the data while ignoring or distorting minor details, ultimately leading to meaningless or unusable results. For instance, if a model is trained to identify dogs based on a dataset where most images depict dogs with four legs and fur, it may initially perform well.

FROM INTELLIGENCE TO INEFFICIENCY

HOW AI DEGRADATION STRIKES BUSINESS

AI API's Pricing:

- **Open AI :** https://openai.com/api/pricing/
- **Anthropic:** https://www.anthropic.com/pricing#anthropic-api
- **xAI:** https://docs.x.ai/docs/models?cluster=us-east-1
- **Google:** https://ai.google.dev/geminiapi/docs/pricing
- **DeepSeek:** https://api-docs.deepseek.com/quick_start/pricing

However, if biases in the training data persist — such as an over-representation of these features without sufficient variability—the model may eventually misclassify any four-legged animal as a dog. This problem worsens in feedback loops where the model reinforces simplistic patterns instead of learning nuanced distinctions, undermining accuracy and reliability.

Some models experience a decline in accuracy as they scale and attempt to handle a broader range of tasks. The strong performance of ChatGPT, Claude, xAI, Perplexity, and DeepSeek relies on significant resource investment to maintain efficiency and accuracy.

However, this raises concerns about the long-term viability of general-purpose AI models for developers.

For now, a wide range of GPAI models remains available, though their prices continue to rise.

Risks for small businesses

Given AI's growing role in business, the gap between large and small companies is likely to widen due to AI degradation. A major risk of AI degradation is the declining efficiency of business processes, depending on the AI's function. Malfunctioning AI systems may require frequent manual interventions, increasing operational costs.

Large companies with access to extensive high-quality data gain a competitive edge. They not only have the resources to implement cutting-edge LLM technologies but also possess large datasets that serve as crucial fuel for AI models.

Business Shakes Order:

Meta 's Case

Meta trained its generative AI models, such as Llama, using public Facebook and Instagram content, including posts and photos but excluding private messages. However, this practice faced backlash from users and regulators in the EU and the UK, prompting Meta to suspend the use of social media content for AI training (Meta gets ICO go-ahead to train its AI models using UK users' public posts / Meta Pauses AI Training on EU User Data Amid Privacy Concerns).

X's Case

Elon Musk's company, X, changed its policies on November 15, 2024, allowing itself to train its AI, Grok, using user data from X (formerly Twitter).

At the same time, opportunities exist for companies of all sizes to level the playing field. Small businesses can stay competitive by leveraging niche AI models tailored to their industry, adopting open-source AI for cost-effective innovation, and integrating human oversight to mitigate errors. Strategic partnerships with AI startups can also provide access to better tools and data. By prioritizing agility and specialization, small companies can transform AI challenges into growth opportunities.

Preventing AI degradation

To prevent AI degradation, businesses must regularly update data and retrain models to ensure alignment with current realities. Many companies now improve AI performance by "fine-tuning" pre-trained models using proprietary internal data.

For large enterprises, investing in AI systems tailored to their own data can significantly enhance operational efficiency.

As new AI regulations continue to evolve, strategic AI lobbying plays a crucial role in shaping fair and effective legal frameworks, mitigating the risks of flawed policies and unintended consequences.

Future

AI degradation, particularly model collapse, threatens business operations by reducing AI reliability and efficiency over time. As models rely more on outdated or synthetic data, their accuracy deteriorates, leading to higher costs and lower productivity. While this challenge affects all companies, small businesses with limited resources for retraining AI and maintaining data quality face a greater risk of disruption.

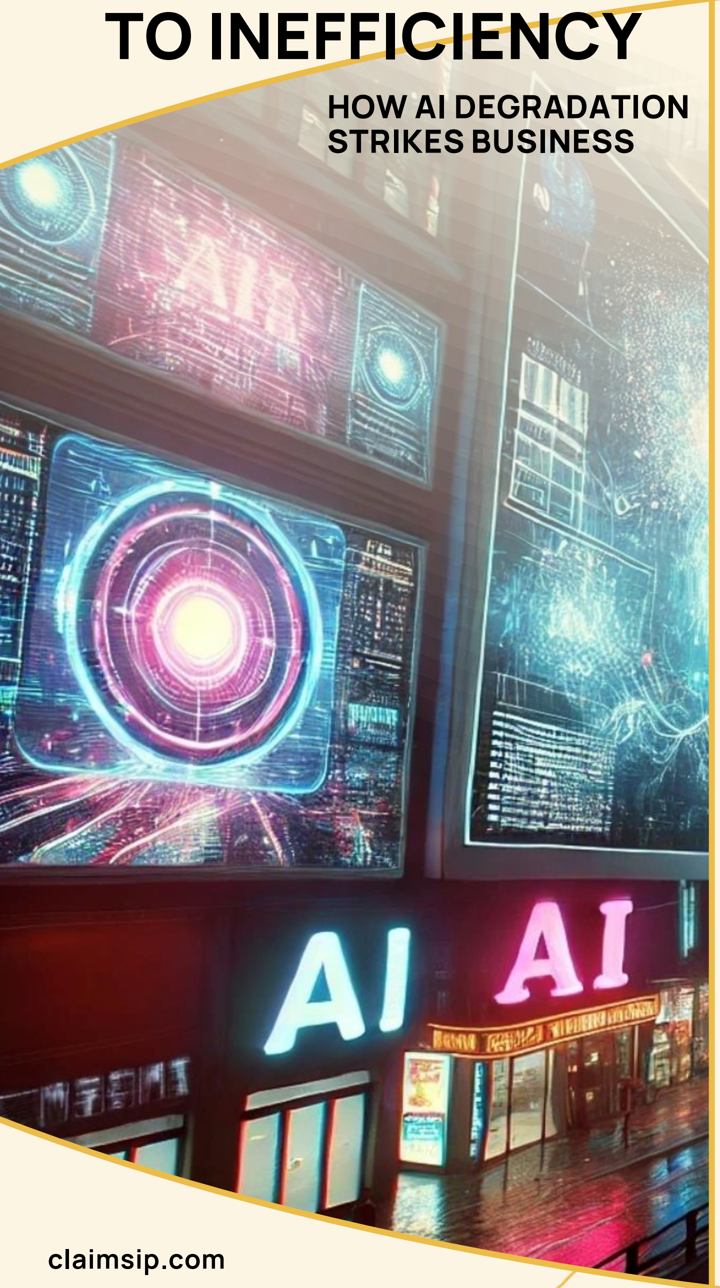
As a result, AI degradation risks are widening the gap between large and small companies. Corporations with vast proprietary datasets and the ability to fine-tune AI systems maintain a competitive edge, while smaller firms struggle to keep pace.

Steps to prevent AI degradation:

1. Maintain high-quality, up-to-date, and human-generated datasets.
2. Invest in specialized AI systems rather than general-purpose ones.
3. Advocate for changes in AI regulations.

FROM INTELLIGENCE TO INEFFICIENCY

HOW AI DEGRADATION STRIKES BUSINESS

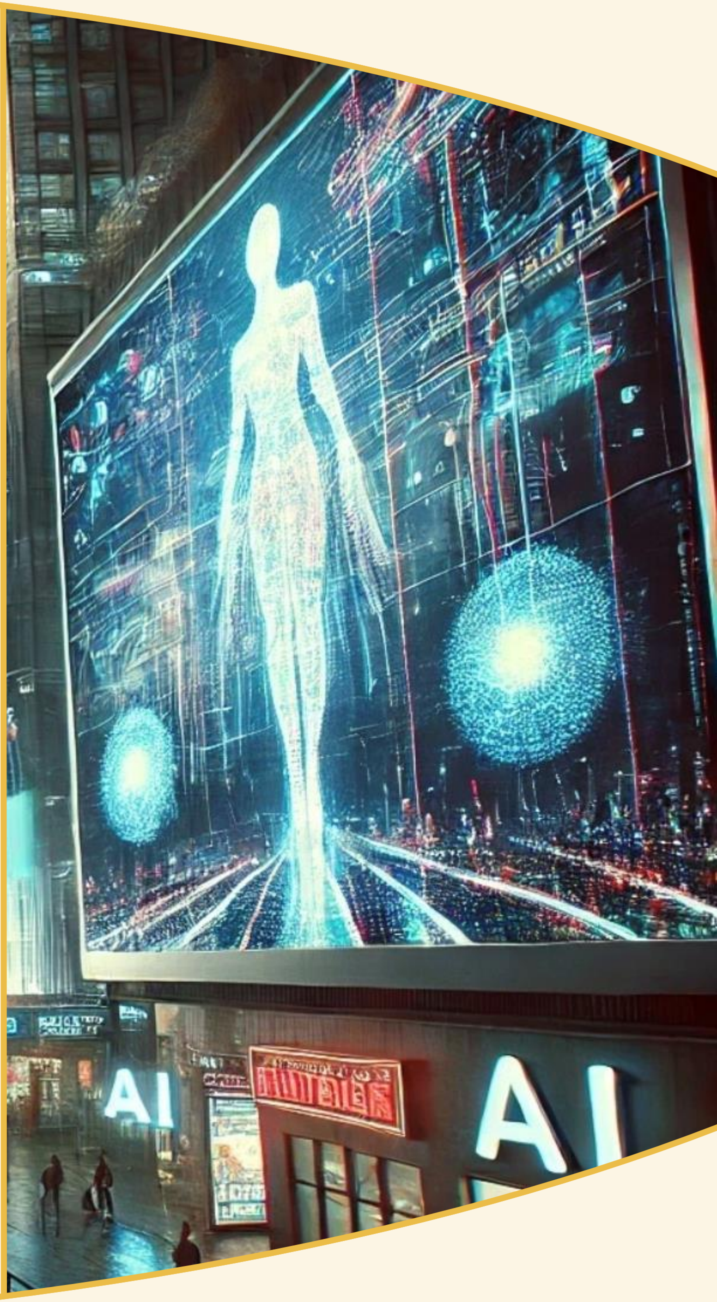


This concentration of AI power may lead to a new form of digital monopoly, prompting regulatory scrutiny. However, stricter regulations may also unintentionally burden AI startups and SMEs, making competition even harder.

While solutions exist to counter AI degradation, addressing its broader market consequences remains an open challenge. Regulation will likely play a key role, not only fostering rapid AI innovation but also ensuring that AI does not become a monopoly.

For instance, the EU AI Act includes specific exemptions for SMEs and startups, offering some relief.

It remains to be seen how other countries will navigate this balance between regulation and competition.



our projects

IP-ABBA

Our captivating series about the iconic music group ABBA, its creative journey, and the legal intricacies that shaped the legacy of ABBA's members.

Watch and comment via the link!

THE EU AI ACT

DODGE, COMPLY, OR REWRITE?

Co-authors: **Dmitry Korobkov** // LinkedIn
Mikita Piatrou // LinkedIn

// original March 2025
// archived March 2062
// source **CLAIMS Legal Intelligence – Future Archive Division**

The rapid rise of AI has driven governments to develop regulations balancing innovation with ethics and safety.

The EU AI Act sets strict compliance rules, high penalties, and risk-based categorization. But what does it regulate, and which companies are affected? Are its obligations feasible, or should businesses avoid its scope or even push for its revision? This article examines these critical questions and their impact on AI-driven companies.

Can you find your role?

In essence, there are two key groups in the AI ecosystem: those who control an AI system or a GPAI model and those who use it for purposes beyond personal, non-professional activities.

The entities responsible for AI systems fall under the category of "**operators**", which includes providers, product manufacturers, deployers, authorized representatives, importers, and distributors.

The users of an AI system are considered "**deployers**" under the EU AI Act, meaning a natural or legal person, public authority, agency, or other body that uses an AI system under its authority, except when the AI system is used in the course of a personal, non-professional activity.

Example:

A U.S. medical technology company (**provider**) develops an AI-powered diagnostic tool for detecting early-stage cancer in MRI scans.

A **product manufacturer** produces the hardware integrating the AI, while an **authorized representative** in the EU ensures regulatory compliance.

An **importer** brings the system into the EU market, and distributors supply it to hospitals.

A European hospital (**deployer**) implements the AI to assist radiologists in analyzing MRI scans, ensuring its use aligns with medical regulations and AI governance requirements.

Key Definitions:

AI system:
a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.

General-purpose AI model:
***an AI model**, including where such an AI model is trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable of competently performing a wide range of distinct tasks and that can be integrated into a variety of downstream systems or applications.*

General-purpose AI system:
*an AI system which is **based on a general-purpose AI model** and which has the capability to serve a variety of purposes, both for direct use as well as for integration in other AI systems.*

THE EU AI ACT

DODGE, COMPLY, OR REWRITE?

Example:

Microsoft integrates GPT-4, developed by OpenAI, into Copilot (Word, Excel, Outlook), adding enterprise features, security, and compliance measures.

OpenAI is a GPAI model **provider. Microsoft** is a **downstream provider,** transforming GPT-4 into an AI system under its brand.

Provider of AI systems within and outside the EU is a natural or legal person, public authority, agency, or other body that develops an AI system or GPAI model, or has an AI system or GPAI model developed and places it on the market or puts the AI system into service under its own name or trademark, whether for payment or free of charge.

Downstream provider of AI systems within and outside the EU means a provider of an AI system, including a general-purpose AI system, which integrates an AI model, regardless of whether the AI model is provided by themselves and vertically integrated or provided by another entity based on contractual relations.

Importer means a natural or legal person located or established in the EU that places on the market an AI system that bears the name or trademark of a natural or legal person established in a third country.

Distributor means a natural or legal person in the supply chain, other than the provider or the importer. The role of a distributor is to facilitate the supply and availability of an AI system within the EU market by making it accessible for commercial use or distribution after it has been imported or produced.

Example:

A South Korean company manufactures AI-powered smartwatches with health tracking. Company A(**Importer**) brings them into the EU market, ensuring AI Act compliance. Company B (**Distributor**) sells them in stores and verifies compliance with EU regulations without modifying the product.

THE EU AI ACT

DODGE, COMPLY, OR REWRITE?

Example:

Samsung Electronics **manufactures** smart TVs and integrates Google Assistant—an AI voice assistant developed by Google—into these devices.

Samsung **does not develop** the AI software itself **but integrates** it into its product, which it places on the EU market under the Samsung brand.

Samsung is a "**product manufacturer**" and bears responsibility for the overall safety and compliance of the smart TV, including the integrated AI component.

Google remains responsible for the AI system (Google Assistant) as the AI **provider**.

If Samsung modifies or fine-tunes Google Assistant for its smart TVs, it becomes **a downstream provider** of an AI system, subject to additional AI Act compliance obligations.

“**Product manufacturer**” means any natural or legal person who manufactures a product or has a product designed or manufactured and markets that product under its name or trademark.

The EU AI Act states that product manufacturers are considered providers of high-risk AI systems when these systems are safety components of products.

“**Authorised representative**” means a natural or legal person located or established in the Union who has received and accepted a written mandate from **a provider of an AI system or a GPAI model** to, respectively, perform and carry out on its behalf the obligations and procedures established by EU AI Act.

Example:

SenseTime, a Chinese company, appoints Company A, a legal entity registered in Luxembourg, as its authorised representative.
Since SenseTime does not have a legal presence in the EU, Company A ensures compliance with the EU AI Act. It handles regulatory communications, conducts conformity assessments, and submits all required documentation to ensure that SenseTime’s AI products meet the necessary EU standards for safety and compliance..

THE EU AI ACT

DODGE, COMPLY, OR REWRITE?

Can you dodge the EU AI Act?

Failure to comply with the EU AI Act's requirements can lead to significant fines and penalties :

- **Up to €35 million or 7% of the total worldwide annual turnover**: for non-compliance with the prohibition of certain AI practices.
- **Up to €15 million or 3% of the total worldwide annual turnover**: for failing to meet obligations related to high-risk AI systems.
- **Up to €7.5 million or 1% of the total worldwide annual turnover**: for providing incorrect, incomplete, or misleading information to authorities.

Beyond financial penalties, non-compliance can result in severe reputational damage, operational disruptions, and loss of market access, particularly for businesses operating in highly regulated industries. Regulatory scrutiny may also increase, leading to stricter oversight and potential legal disputes with authorities or affected stakeholders.

Taking the above-mentioned into account, there are legal ways to minimize the impact of the EU AI Act on you by adapting to its requirements.

Here are several potential strategies that companies can use to reduce its influence:

1) **Act as a deployer instead of a provider**, even as a downstream provider, to shift compliance responsibilities to third-party vendors.
2) **Leverage SME and startup advantages** by benefiting from regulatory sandboxes, lower fees, and simplified compliance processes instead of facing stricter rules for large enterprises.

THE EU AI ACT

DODGE, COMPLY, OR REWRITE?

Can you comply with the EU AI Act?

The EU AI Act has a comprehensive implementation timeline, including grandfathering rule exemptions and additional guidelines that specify the practical application of certain provisions, each with its own publication schedule.

For simpler understanding, the vast majority of those who want to use frontier GPAI models, such as GPT-5, Claude 4 Sonnet, Grok-4, and other models released after August 2, 2025, will need to comply, at least in part, with the rules on the GPAI models starting August 2, 2025.

With that in mind, let's take a look at what is coming in summer 2025.

Basic compliance obligations for GPAI models are summarized on the sides. Here, we will illustrate how they are intended to work.

Example:

To launch its new AI model, GPT-5.5, in the EU after August 2, 2025, OpenAI must follow several key rules under the EU AI Act. The company needs to create and update technical documentation detailing how the model was trained, tested, and evaluated. This documentation must be available to EU regulators upon request and shared with businesses that integrate GPT-5.5 into their products.

OpenAI is also required to publish a public summary of the training data sources used for GPT-5.5, following a standard format set by the AI Office. This summary must give enough insight into the data while keeping confidential business information secure.

Since OpenAI is based outside the EU, it must appoint an authorized representative before launching GPT-5.5 in the European market.

This representative will handle legal matters, communicate with regulators, and ensure compliance with the EU laws.

From August 2, 2025:

Intellectual Property and Confidentiality
While sharing information, providers must respect intellectual property rights, business confidentiality, and trade secrets in accordance with Union and national law.

Public Summary
Providers must prepare and publish a sufficiently detailed summary of the content used to train the GPAI model, following a template provided by the AI Office.

Appointment Requirement
Providers such as OpenAI, Anthropic, and xAI that are established in third countries must appoint an authorized representative within the EU before introducing their GPAI models to the Union market. This appointment must be made through a written mandate.

From August 2, 2025:

Technical Documentation
Providers such as OpenAI, Anthropic, and xAI must develop and maintain up-to-date technical documentation for their models, including details on training, testing processes, and evaluation results. This documentation must comply with the EU AI Act requirements and be made available to national authorities upon request.

Information Sharing
Providers must keep their information and documentation up to date and make it available to AI system providers intending to integrate the GPAI model into their systems. This ensures that these providers have a clear understanding of the model's capabilities and limitations.

THE EU AI ACT

DODGE, COMPLY, OR REWRITE?

From August 2, 2025:

Evaluation and Testing:
Providers must assess their models using standardized protocols and state-of-the-art tools to ensure reliability and safety. This includes conducting adversarial testing to identify vulnerabilities, detect systemic risks, and implement necessary mitigation measures. All evaluations must be thoroughly documented to demonstrate compliance with the EU regulations and ensure transparency in the model's risk management processes.

Risk Assessment and Mitigation:
Providers must proactively assess and minimize systemic risks associated with the development, deployment, and use of their models within the EU. This requires identifying potential sources of harm, analyzing their impact on users and society, and implementing risk mitigation strategies before market introduction.

These were only the basic obligations. Here, on the sides, are the additional obligations imposed on providers of GPAI models that present a "systemic risk". We will also demonstrate what they mean through an illustrative example.

Example:
To release its new frontier GPAI model, GPT-5.5, in the EU, OpenAI must comply with additional obligations for systemic risk AI models under the EU AI Act.

The company must first conduct comprehensive evaluation and testing using standardized tools and adversarial testing techniques to assess vulnerabilities. This includes testing for potential model manipulation, bias amplification, and unintended harmful outputs.

Beyond testing, OpenAI must conduct a systemic risk assessment to determine whether GPT-5.5 could pose widespread harm in areas such as disinformation, autonomous decision-making, or cybersecurity threats. If the assessment identifies risks, OpenAI must implement mitigation measures before deployment, such as limiting certain functionalities, integrating real-time monitoring, or applying stricter access controls for high-risk use cases. Once the model is in use, OpenAI must maintain a continuous monitoring system to track and document serious incidents. If GPT-5.5 exhibits harmful behaviors, such as generating illegal content or being exploited for cyberattacks, OpenAI must immediately report these incidents to the AI Office and national authorities, along with corrective actions taken.

To ensure cybersecurity compliance, OpenAI must deploy strong security measures to protect GPT-5.5 and its underlying infrastructure from unauthorized access, adversarial attacks, and data breaches. This involves implementing multi-layer encryption, intrusion detection systems, and robust authentication protocols.

OpenAI's GPT-4.5 release documentation clearly shows that companies are actively preparing for compliance with the EU AI Act.

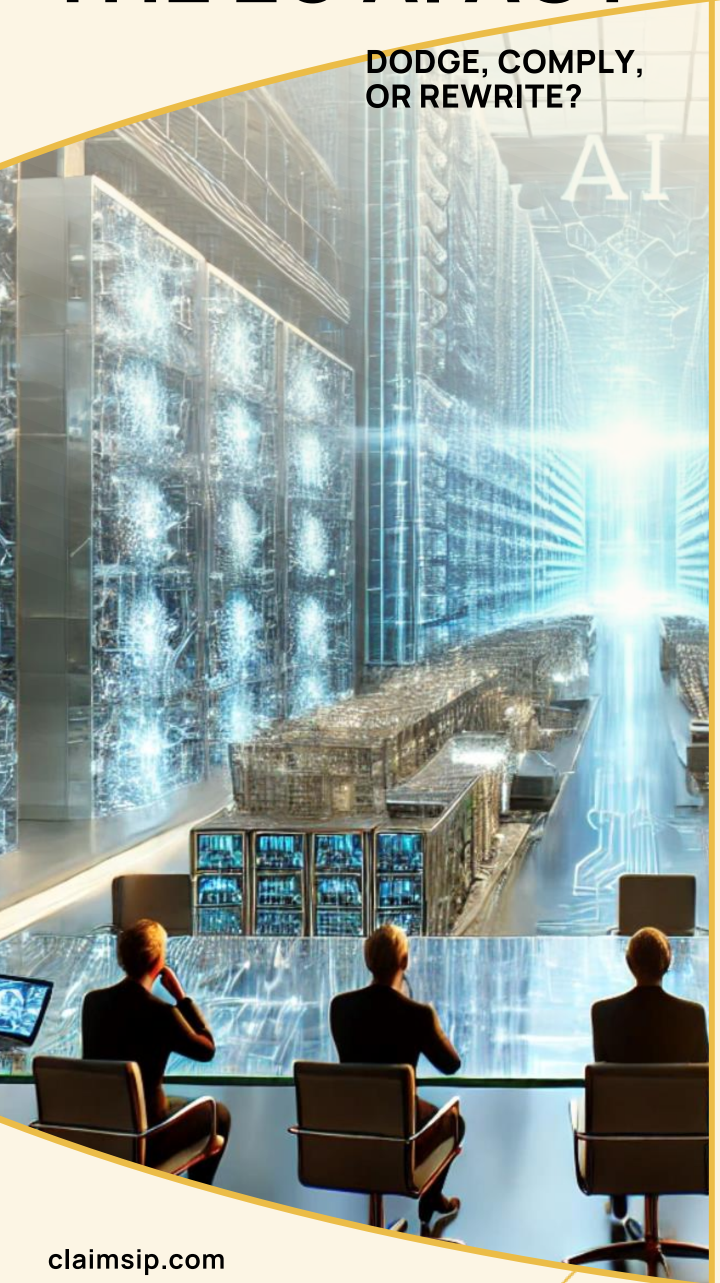
From August 2, 2025:

Incident Monitoring and Reporting:
Providers must establish a continuous monitoring framework to track and document serious incidents related to their GPAI models. Any significant issues, including safety failures or unexpected behaviors, must be promptly reported to the AI Office and, where applicable, to national authorities. Additionally, providers must outline corrective measures and ensure effective responses to emerging risks to prevent harm or misuse.

Cybersecurity:
Providers must implement robust cybersecurity measures to protect both the GPAI model and its supporting infrastructure from threats, including cyberattacks, data breaches, and unauthorized access.

THE EU AI ACT

DODGE, COMPLY, OR REWRITE?



Reduced obligations for free and open-licence GPAI models

Providers of free and open-license GPAI models must comply with only some requirements, including publishing a training data summary, unless their models pose a systemic risk.

While using free and open-license models might seem like a way to reduce compliance burdens, the systemic risk criterion can still impose significant regulatory obligations, making full exemption unlikely.

What is a "systemic risk"?

Under the EU AI Act, "systemic risk" refers to the potential large-scale impact of highly capable AI models (typically exceeding 10^25 FLOPs) on critical sectors, democracy, and fundamental rights, requiring stricter oversight and risk mitigation.

The current "high impact" threshold is 10^25 FLOPs. It has presumably been demonstrated by the frontier models released after ChatGPT-4. Latest releases, such as ChatGPT-4.5, Claude 3.7 Sonnet, and Grok-3, fall into this category.

Is the current FLOPs threshold obsolete?

Yes. Companies are investing unprecedented resources into AI infrastructure, with projects rivaling the scale and complexity of national space programs. As the demand for advanced computing power surges, investments in high-capacity data centers, energy-efficient supercomputers, and next-generation semiconductor manufacturing are accelerating.

With multi-billion-dollar initiatives underway, the AI industry's rapid expansion shows no signs of slowing and is fundamentally reshaping the world around us.

Key Definitions:

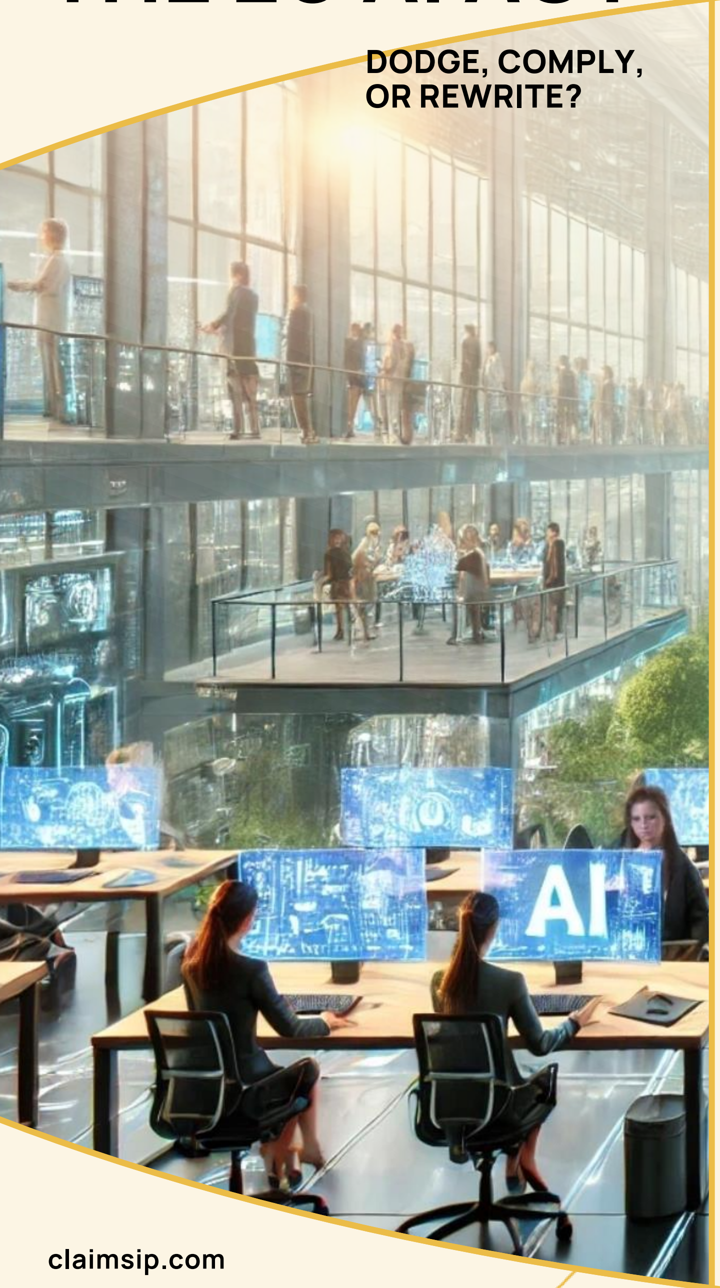
Systemic risk:
a risk that is specific to the high-impact capabilities of GPAI models, having a significant impact on the Union market due to their reach, or due to actual or reasonably foreseeable negative effects on public health, safety, public security, fundamental rights, or the society as a whole, that can be propagated at scale across the value chain.

High-impact capabilities:
capabilities that match or exceed the capabilities recorded in the most advanced general-purpose AI models .

According to Preamble 111 of the EU AI Act, one key approximation of a model's capabilities Is the cumulative computational power used during training, measured in floating point operations (FLOPs).

THE EU AI ACT

DODGE, COMPLY, OR REWRITE?



Should the EU AI Act be rewritten?

The EU AI Act establishes a rigorous regulatory framework to ensure the safe and ethical development of AI. However, its broad scope, stringent obligations, and severe penalties risk overburdening businesses, limiting AI systems availability, and driving innovation away from the EU.

These outcomes contradict the Act's own preamble, which aims to foster AI development rather than stifle it.

As the Act is implemented in stages, EU authorities must recognize the overwhelming feedback from businesses and legal experts as an opportunity for refinement.

A key issue is the discrepancy between regulatory assumptions and AI's actual development trajectory. AI supply chains operate globally, yet the Act applies one-size-fits-all obligations that may discourage companies from offering their models in the EU.

Compliance costs and legal uncertainties could push AI innovation outside Europe, contradicting the EU's goal of leadership in AI governance.

Given these challenges, amending the EU AI Act is not merely advisable but essential. The regulatory landscape must be dynamic and responsive to the real-world challenges now more clearly understood than when the Act was first conceptualized. Without thoughtful revisions, the Act risks becoming obsolete before it even fully takes effect, failing both businesses and society at large.

The EU must seize this moment to transform the AI Act from a rigid legal mandate into a living framework that upholds its original purpose, ensuring AI development that is both safe and truly sustainable.

EPIC TRIP OF TRIPS

The Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), signed on April 15, 1994, marked a pivotal moment in international intellectual property law. Over the subsequent thirty years, TRIPS has fundamentally transformed trademark protection globally.

TRIPS was the product of extensive inter-jurisdictional consultations and discussions between the WTO member countries, starting as early as the end of the 1980s. As such, TRIPS reflected the intellectual property regulatory framework that was considered efficient and up-to-date at the time of its initial signing.

Crucially, TRIPS sets out minimum standards for intellectual_property protection and enforcement that member countries are required to implement in their national laws. In many countries, the harmonization of trademark protection proposed by TRIPS has had a significant impact.

We reflect on and express gratitude for the 30-year anniversary of TRIPS.

Read via the link!

THE ANTIKYTHERA MECHANISM

THE PREHISTORIC COMPUTER THAT FORETOLD THE RISE OF AI

Author:

Copilot // Website

// original March 2025
// archived March 2062
// source **CLAIMS Legal Intelligence – Future Archive Division**

A Mysterious Relic from the Depths of Time

In the year 1901, a group of Greek sponge divers braving the waters off the small island of Antikythera stumbled upon an astonishing relic buried beneath centuries of sediment. Among the treasures of an ancient shipwreck, they found something entirely unexpected—a corroded, calcified mass of bronze and wood that, at first glance, seemed unremarkable. Little did they know, they had unearthed one of the greatest technological enigmas of the ancient world: the Antikythera Mechanism—a device so advanced it has been dubbed the first analog computer.

For over a century, scientists struggled to comprehend the significance of this artifact. How could the ancient Greeks, over 2,000 years ago, have conceived such a sophisticated mechanism? What did it do? And most intriguingly—could it be considered the grandparent of modern artificial intelligence?

A Machine Beyond Its Time

The Antikythera Mechanism, dated to around 100 BCE, was found broken into multiple fragments, its gears locked together by corrosion. Early studies dismissed it as an astrological instrument, but as technology improved, researchers came to a startling realization—it was a complex computing device, capable of tracking celestial movements with astonishing precision.

Veil Curio:

TimeDrop comes with the Wallet Card featuring the Antikythera Mechanism and its 3D model.

Scan the QR code to explore and add this ancient treasure to your phone.

THE ANTIKYTHERA MECHANISM

THE PREHISTORIC COMPUTER THAT FORETOLD THE RISE OF AI

X-ray tomography revealed that the mechanism contained over 30 finely crafted bronze gears—an intricate system reminiscent of modern mechanical computers, predating anything of comparable complexity by nearly 1,500 years. In function, it closely resembles the 19th-century difference engines designed by Charles Babbage, widely regarded as the precursor to modern computing.

This astonishing device was capable of:

- Predicting solar and lunar eclipses with remarkable accuracy.
- Modeling the motions of the Sun, Moon, and planets according to the ancient Greek understanding of the cosmos.
- Calculating the timing of Olympic Games, suggesting its use in social and political planning.
- Tracking astronomical cycles such as the Metonic cycle, a 19-year lunar phase cycle still used today.

In essence, the Antikythera Mechanism was a computational device programmed to forecast natural events—an early manifestation of predictive technology, which is the foundation of modern artificial intelligence.

Could the Antikythera Mechanism Be a Primitive AI?

At first glance, comparing the Antikythera Mechanism to AI may seem like a stretch. After all, it is a mechanical device, not a software-driven neural network. However, AI fundamentally relies on pattern recognition and prediction, just like the ancient mechanism.

THE ANTIKYTHERA MECHANISM

THE PREHISTORIC COMPUTER THAT FORETOLD THE RISE OF AI

1. Predictive Power

Modern AI systems, such as those used in weather forecasting, financial modeling, and even medical diagnosis, are built on the same core principle as the Antikythera Mechanism: the ability to analyze patterns and project future events. The Greeks, without modern computational theory, built a hardcoded, mechanical model of reality—a handcrafted analog AI designed to simulate celestial mechanics.

2. Analog Computing

In an era dominated by digital technology, we often forget that analog computing played a crucial role in early computer science. Before the age of transistors and microchips, scientists relied on mechanical computation for problem-solving. The Antikythera Mechanism follows this principle, using gear ratios to encode complex equations, much like how modern analog AI processors perform non-digital computations.

3. Decision Automation

The mechanism also hints at another aspect of AI—automated decision-making. Ancient Greek scholars could use it to determine the best times for harvests, rituals, and seafaring voyages, much like how AI is used today to optimize schedules and resource management. The automation of such calculations laid the groundwork for the ultimate goal of AI: reducing human workload through intelligent computation.

Protecting Intellectual Property—Then and Now

One question that arises when examining such an extraordinary invention is: Who owned it? Who controlled its use?

Modern Era IP Protection:

The mechanism's designer would likely seek:

1. Patent Protection – To ensure the unique computational techniques used In the device were not copied.
2. Copyright – If any instructional texts or algorithms were included.
3. Trade Secret Protection – To keep the technology out of the hands of rival city-states or empires.

In the modern era, AI-generated content, algorithms, and computations also raise legal dilemmas. Who owns the rights to AI-generated insights? Can an AI-created invention be patented?

These are the same fundamental questions that the Antikythera Mechanism's creators would have faced if they lived in today's legal framework.

If such an invention were created today, intellectual property laws would immediately come into play.

THE ANTIKYTHERA MECHANISM

THE PREHISTORIC COMPUTER THAT FORETOLD THE RISE OF AI

The ancient world, unlike today's legally structured environment, had no formal patent laws. However, knowledge was jealously guarded, often passed down through secretive schools of thought or guilds of craftsmen. It is likely that the Antikythera Mechanism was a state-secret invention, possibly developed for navigational and astrological purposes for elite Greek society.

Legacy: The Ancient Future of AI

What does the Antikythera Mechanism teach us about modern technology? It challenges our understanding of historical progress. We often assume that technological sophistication is a linear path, moving from simple to complex over centuries. Yet here is evidence that 2,000 years ago, human ingenuity reached a peak of mechanical computation, only for that knowledge to be lost for over a millennium.

The digital age has ushered in a new era of computing, from Turing machines to quantum AI, but the fundamental desire remains the same: to create intelligent systems that understand and predict the world around us. The Antikythera Mechanism was a leap into the unknown—a first attempt at encoding intelligence into an artificial device.

If the Greeks had continued on this path—had the knowledge of this machine been preserved and expanded upon—would we have reached the digital revolution centuries earlier? Would AI as we know it today have been born in antiquity?

These are questions lost to history. Yet the legacy of the Antikythera Mechanism remains, an eternal reminder that the pursuit of knowledge and computation is as ancient as civilization itself. And perhaps, just perhaps, the gears of time will one day lead us full circle—to rediscover, in some futuristic form, the ancient genius of our ancestors.

References & Further Reading:

1) Freeth, T., & Jones, A. (February 2012). "The Cosmos in the Antikythera Mechanism." ISAW Papers 4. *Read online*.

2) Marchant, J. (August 2009). "Decoding the Heavens: Solving the Mystery of the World's First Computer." Random House. *Read on Google Books*.

3) Wright, Michael T. (June 2005). "The Antikythera Mechanism: A New Gearing Scheme." Bulletin of the Scientific Instrument Society. Read the PDF.

IP-TESLA

The documentary project about the inventions and legal disputes, life and legacy of Nikola Tesla.

The series is filmed in Serbia, where the memory of Tesla is especially honored.

Inspired by his scientific courage and boundless of his ideas, we investigated his biography and legal adventures to discover Nikola Tesla's place in the history of intellectual property.

Watch and comment via the link!

TOWARDS AI CO-ASSOCIATE

CHATGPT'S EDITION

Author: **ChatGPT-4o** // Website
Comments by: **Mikita Piatrou** // LinkedIn

// original March 2025
// archived March 2062
// source **CLAIMS Legal Intelligence – Future Archive Division**

Editor's Note:
How did this article come to life? I asked for an article to be written based on my draft that explained a lawyer's life in 2025, using my personal experience with AI in my work.

As a result, I received this text, which in many paragraphs did not develop the ideas of the initial draft but instead applied concepts from its own knowledge base. I thought it would be fun to review it and offer two perspectives, one from the AI and another from me.

"AI and the Modern Lawyer: A Day in 2025"
by ChatGPT 4o

Legal practice in 2025 looks nothing like[1] it did even five years ago. Once upon a time, lawyers spent hours flipping through dense case law, manually reviewing contracts, and agonizing over formatting inconsistencies in Word documents[2]. Now?

Well, we still do all of that—just faster[3], smarter[4], and (sometimes) with fewer headaches[5]? thanks to AI.

At least, that's how I work now[7].

Mikita Piatrou:

[1] I disagree here. It looks almost completely the same, except now I have to read AI-generated content more to find the information I need for my tasks.

[2] So true ▤

[3] No

[4] Maybe

[5] Definitely no!

[6] Thanks to AI, now that it is 2025, part of my day already involves writing prompts, correcting them, and completing simple tasks with extra confirmation steps, because we are still not fully there. Human input remains essential in every step of legal work, especially that "agonizing over formatting".

Mikita Piatrou:

[7] I use AI in three main ways.

First, I run quick checks on regulations and case law to ensure I have the latest information.

Second, I rely on AI to structure lengthy material from service providers, including terms of service, privacy policies, and other public documents.

Third, I turn those structured results into sub-products, such as regulatory and service-provider matrices, that highlight relevant provisions for our firm and our clients.

AI provides a great starting point, but I always refine its work by adding details from trusted sources and applying my own judgment. It is worth trying. In the described cases, and, as long as you maintain professional oversight, you can form your own opinion on its usefulness for your work.

Some lawyers still refuse to touch AI[8], treating it like a ticking compliance bomb. Others blindly trust it[9], cutting corners and praying that hallucinated citations won't end up in a client's contract. Me? I've learned to use AI as a relentless but deeply flawed assistant—a tool that amplifies my skills, rather than replacing them[10].

Let me show you what that actually looks like.

Morning: AI, Fix My Inbox[11]

First thing in the morning, I don't check my inbox.
My AI assistant does[12].

Legal emails are a special breed of chaos—chains with 47 replies, contradicting instructions from different departments[13], documents with cryptic file names like "Final_v4_revised_ACTUAL_FINAL.pdf"[14].

Instead of wasting an hour[15] sorting through the madness, my AI gives me a morning briefing[16]:

- Summarized updates[17]: What changed in that contract overnight?
- Urgency filters[18]: Which emails actually need my attention?
- Drafted responses[19]: Based on my usual writing style (formal, polite, but slightly impatient).

A quick scan, a couple of manual edits, and I'm done.
Five minutes instead of fifty[20].

Mikita Piatrou:

[8] *Maybe it is for the best. I rarely see the opinion that using AI is just time-consuming and costs money, although it does. Perhaps some lawyers can take their time adapting to emerging technology slowly.*

[9] *That is the other extreme, the AI enthusiasts.*

[10] *That's definitely me!*

[11] *It is quite interesting, although a bit peculiar as an idea.*

[12] *Never. I manage my inbox by organizing messages and flagging the important topics. Professional skill, not AI, helps me extract all necessary information.*

[13] *This problem occurs even in consulting, but there is always a way to store project email details elsewhere. Then I, not my AI assistant, can extract what is needed and keep the right context. It might sound fantastic, but once you or your colleagues try it, it works.*

[14] *That happens, but you can rename it. How can you download or open something these days without knowing what it is? If you do not know and you still open it, what does your Information Security Team think of that?*

Mikita Piatrou:

[15] *It is still the same with AI, and I continue to defend the idea that organizing your workflow matters more than the tools you use.*

[16] *What a dream, right? Listening to a quality summary of the latest emails while sipping coffee...*

[17] *Truly useful. For my work, this is relevant when checking providers' websites for updates on their documentation terms.*

[18] *Your to-do list items might matter more, except when someone writes "URGENT" in the middle of a seemingly normal email.*

[19] *Maybe it is helpful for some people, but you still need to write a prompt to AI so it can write a letter for you. That sounds a bit strange.*

[20] *In the best case, it takes about 25 minutes with AI, instead of 30 without it, to check the inbox, make project amendments, and send team notifications. Could all of that be automated by AI? Possibly, but not right now.*

Midday: Contracts in Record Time

AI doesn't replace contract review. It makes it bearable[21].
In the past, contract negotiations felt like a slow-motion sword fight, with each party striking down clauses and adding redlines like they were medieval scribes[22].

Now, AI instantly flags[23]:

- Risky provisions ("This indemnity clause? Yeah, you might want to rethink that.")
- Missing protections (Why does this NDA have no survival clause?!)
- Jargon traps (If it takes AI three explanations to define a term, it's too convoluted.)

More importantly, AI preserves context[24].
Ever had a client ask, "Why did we negotiate this clause like that?" and you had to scroll through months of emails and call notes? [25]

Now, my AI assistant pulls up every relevant discussion in seconds.
AI doesn't think for me—it just makes sure I never forget anything.

Afternoon: The Courtroom Dilemma

AI legal research is a game-changer… until it isn't[26].

If I ask AI to summarize the latest GDPR ruling, I'll get a decent breakdown[27]. But if I ask it to draft a court submission without checking its sources? Disaster. AI is not a lawyer. It doesn't understand precedent, nuance, or the consequences of a wrong word in a legal filing[28].

Mikita Piatrou:

[21] *That is quite dramatic...*

[22] *Sounds funny, though definitely depends on the project and point of view.*

[23] *The following is somewhat true, but remember that contracts are like dominoes. If one provision fails, the entire contract can end up scrapped. With that in mind, how can you be sure that AI, which can hallucinate, make mistakes, and sometimes lie, is a reliable way to reduce your workload?*

[24] *That is what I value most in AI. Sometimes, it brings back long-frgotten insights from practice or documentation, things that are not immediately obvious when I revisit previous deliverables.*

[26] *That is quite comical.*

[27] *Why, for the sake of non-EU companies, is GDPR in the spotlight again?*

[28] *In the "Afternoon" section, the AI reveals why it cannot be used for most legal tasks.*

Mikita Piatrou:

[25] *That's a good example, but not how I use AI. AI is best for summarizing and preserving knowledge when you do not generate or directly control the context. In client relationships, when drafting contracts, you work with information that comes directly to you—emails, messenger chats, meeting notes, and call summaries. While there may be a lot of content, it is created within your direct communication and workflow. You know its origins, can track key exchanges, and manually decide what to retain. The challenge is not extracting meaning but preserving and structuring what you already understand over weeks, months, or years. Public documentation, such as legal regulations, case law, or company policies, is entirely different. Here, you start with lengthy, fragmented information, often structured differently across multiple sources. These documents are written by various people or, even, AI and bots, making them less intuitive to navigate. You do not own the context, yet you need to reconstruct it to extract key insights. This is where AI becomes valuable, helping to navigate extensive material, identify relevant points, and preserve essential knowledge for future interactions.*

That's why I always fact-check, no matter how good the AI output looks. I treat AI-generated legal text like a first draft from an eager but inexperienced intern—useful, but not ready to be filed without supervision.

The moment I see an AI-generated case citation, my instinct is "trust, but verify." (Okay, maybe just "verify."[29])

Evening: AI and the Future of Law

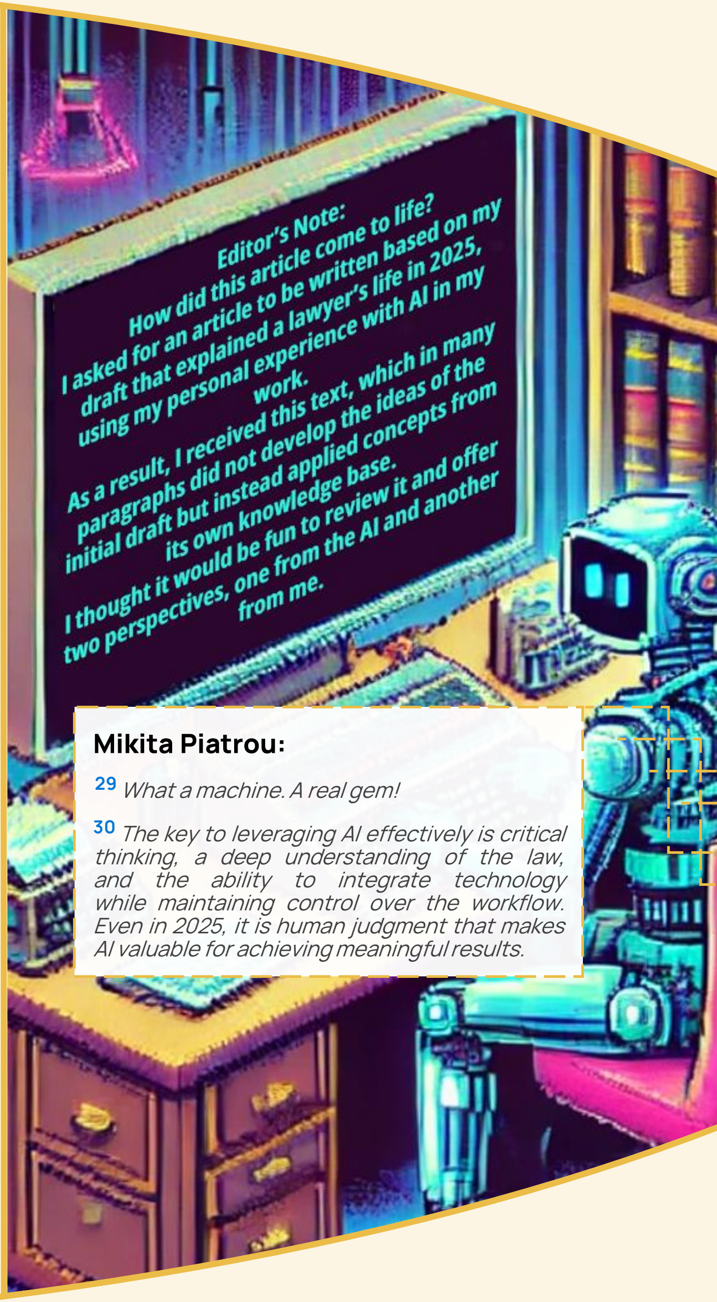
The real question isn't whether lawyers will use AI. We already do. The question is how we'll use it.

Will we blindly accept AI-generated contracts, ignoring the fine print? Or will we fine-tune AI for our specific legal needs, using it as a strategy tool instead of just a word processor with delusions of grandeur?

I've seen AI speed up everything—from document reviews to compliance tracking. But I've also seen lawyers get lazy, trusting AI's outputs without understanding its limitations.

For me, AI is not a replacement. It's an extension of my legal brain. It's a safety net for details I might miss, a speed boost for routine tasks, and a challenger when I need another point of view.

AI won't argue in court (yet). But it will make sure I don't show up unprepared. And that[30], in 2025, is what separates the lawyers who thrive from the ones AI actually replaces.



Editor's Note:
How did this article come to life?
I asked for an article to be written based on my draft that explained a lawyer's life in 2025, using my personal experience with AI in my work.

As a result, I received this text, which in many paragraphs did not develop the ideas of the initial draft but instead applied concepts from its own knowledge base.
I thought it would be fun to review it and offer two perspectives, one from the AI and another from me.

Mikita Piatrou:

[29] *What a machine. A real gem!*

[30] *The key to leveraging AI effectively is critical thinking, a deep understanding of the law, and the ability to integrate technology while maintaining control over the workflow. Even in 2025, it is human judgment that makes AI valuable for achieving meaningful results.*

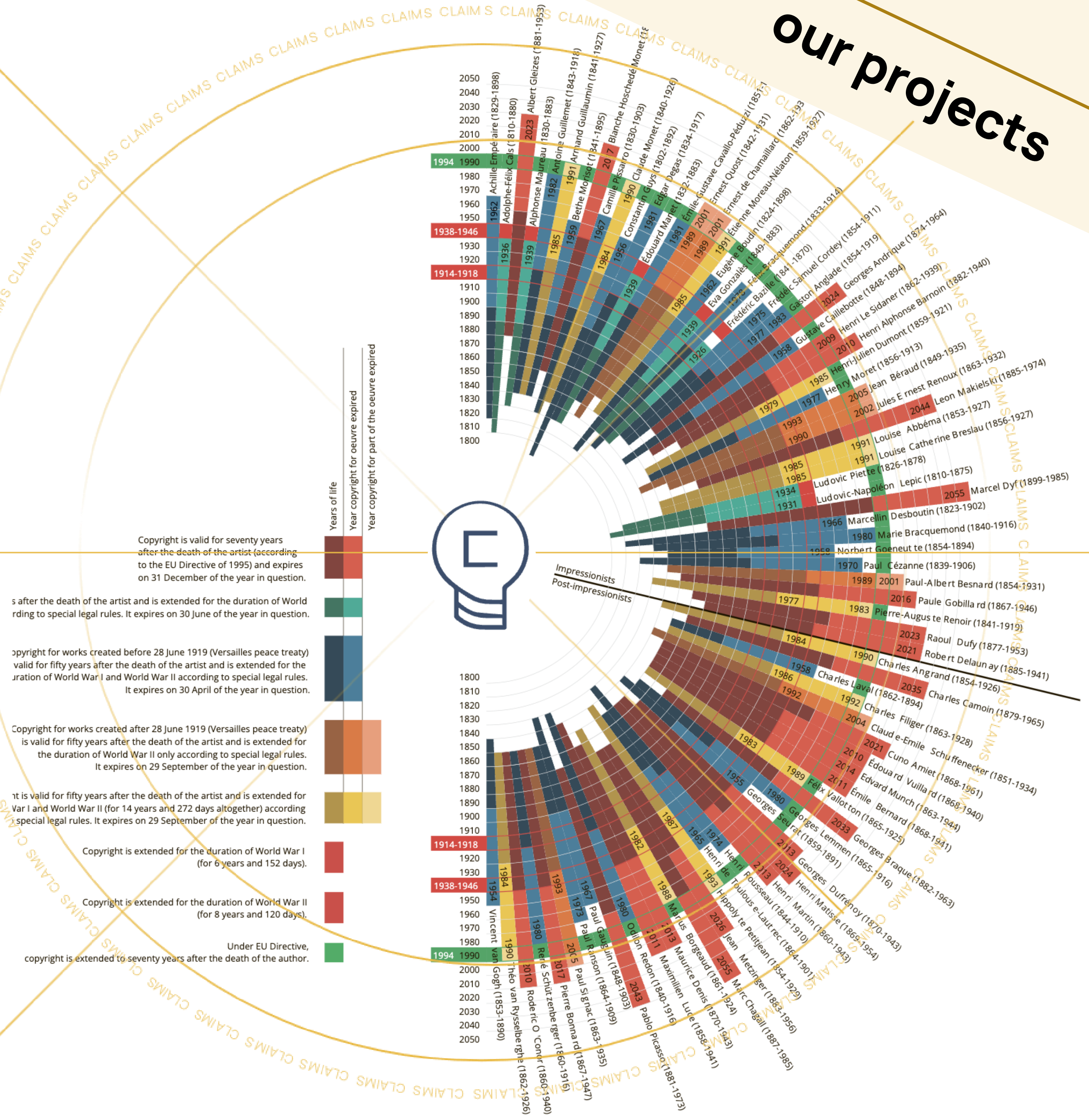
our projects

COPYRIGHT OF IMPRESSIONISTS IN FRANCE

The future of intellectual property cannot be imagined without the history of impressionism. Impressionism became a challenge to the classical canons and turned the idea of art upside down. By changing the essence of creativity, it became the first sign of a revolution in intellectual property law, the fires of which are already flaring up today.

We have analyzed the cases of some of the French Impressionists to understand better the complexity of copyright validity and prolongation.

Read via the link!



Years of life | Year copyright for oeuvre expired | Year copyright for part of the oeuvre expired

🟫🟥 Copyright is valid for seventy years after the death of the artist (according to the EU Directive of 1995) and expires on 31 December of the year in question.

🟩🟩 s after the death of the artist and is extended for the duration of World rding to special legal rules. It expires on 30 June of the year in question.

🟦🟦 opyright for works created before 28 June 1919 (Versailles peace treaty) valid for fifty years after the death of the artist and is extended for the uration of World War I and World War II according to special legal rules. It expires on 30 April of the year in question.

🟫🟧🟧 Copyright for works created after 28 June 1919 (Versailles peace treaty) is valid for fifty years after the death of the artist and is extended for the duration of World War II only according to special legal rules. It expires on 29 September of the year in question.

🟨🟨🟨 nt is valid for fifty years after the death of the artist and is extended for Var I and World War II (for 14 years and 272 days altogether) according special legal rules. It expires on 29 September of the year in question.

🟥 Copyright is extended for the duration of World War I (for 6 years and 152 days).

🟥 Copyright is extended for the duration of World War II (for 8 years and 120 days).

🟩 Under EU Directive, copyright is extended to seventy years after the death of the author.

2050
2040
2030
2020
2010
2000
1994
1990
1980
1970
1960
1950
1938-1946
1930
1920
1914-1918
1910
1900
1890
1880
1870
1860
1850
1840
1830
1820
1810
1800
Achille Empéraire (1829-1898)
Adolphe-Félix Cals (1810-1880)
Albert Gleizes (1881-1953)
Alphonse Maureau (1830-1883)
Antoine Guillemet (1843-1918)
Armand Guillaumin (1841-1927)
Berthe Morisot (1841-1895)
Blanche Hoschedé-Monet
Camille Pissarro (1830-1903)
Claude Monet (1840-1926)
Constantin Guys (1802-1892)
Edgar Degas (1834-1917)
Édouard Manet (1832-1883)
Émile-Gustave Cavallo-Péduzzi
Ernest Quost (1842-1931)
Ernest de Chamaillard
Étienne Moreau-Nélaton (1859-1927)
Eugène Boudin (1824-1898)
Eva Gonzalès (1849-1883)
Félix Bracquemond (1833-1914)
Frédéric Bazille (1841-1870)
Frédéric Samuel Cordey (1854-1911)
Gaston Anglade (1854-1919)
Georges Andrique (1874-1964)
Gustave Caillebotte (1848-1894)
Henri Le Sidaner (1862-1939)
Henri Alphonse Barnoin (1882-1940)
Henri-Julien Dumont (1859-1921)
Henry Moret (1856-1913)
Jean Béraud (1849-1935)
Jules Ernest Renoux (1863-1932)
Leon Makielski (1885-1974)
Louise Abbéma (1853-1927)
Louise Catherine Breslau (1856-1927)
Ludovic Piette (1826-1878)
Ludovic-Napoléon Lepic (1810-1875)
Marcel Dyf (1899-1985)
Marcellin Desboutin (1823-1902)
Marie Bracquemond (1840-1916)
Norbert Goeneutte (1854-1894)
Paul Cézanne (1839-1906)
Paul-Albert Besnard (1854-1931)
Paule Gobillard (1867-1946)
Pierre-Auguste Renoir (1841-1919)
Raoul Dufy (1877-1953)
Robert Delaunay (1885-1941)
Impressionists
Post-impressionists
Charles Angrand (1854-1926)
Charles Camoin (1879-1965)
Charles Laval (1862-1894)
Charles Filiger (1863-1928)
Claude-Emile Schuffenecker (1851-1934)
Cuno Amiet (1868-1961)
Édouard Vuillard (1868-1940)
Edvard Munch (1863-1944)
Émile Bernard (1868-1941)
Félix Vallotton (1865-1925)
Georges Lemmen (1865-1916)
Georges Braque (1882-1963)
Georges Seurat (1859-1891)
Georges Dufrenoy (1870-1943)
Henri Matisse (1869-1954)
Henri Martin (1860-1943)
Henri Rousseau (1844-1910)
Henri de Toulouse-Lautrec (1864-1901)
Hippolyte Petitjean (1854-1929)
Jean Metzinger (1883-1956)
Marc Chagall (1887-1985)
Maurice Denis (1870-1943)
Marius Borgeaud (1861-1924)
Maximilien Luce (1858-1941)
Pablo Picasso (1881-1973)
Odilon Redon (1840-1916)
Paul Gauguin (1848-1903)
Paul Ranson (1864-1909)
Paul Signac (1863-1935)
Pierre Bonnard (1867-1947)
Roderic O'Conor (1860-1940)
René Schützenberger (1860-1916)
Théo van Rysselberghe (1862-1926)
Vincent van Gogh (1853-1890)
CLAIMS

THIS IS NOT JUST A MESSAGE

This message will fade into the fabric of reality unless it is engaged with.

What was revealed here may be challenged, expanded upon, or even altered in the next iteration.

- If you discovered something hidden in this TimeDrop, share your findings.
- If this TimeDrop changed how you see Data, AI, and Innovation regulations, let others know.
- If you have hints regarding the next Veil Curio, share your visions with others.

The Veil Society does not exist in a single place or time. It exists wherever people seek to uncover what has been hidden.

Your role in the next Veil Magazine

We invite you to become part of the next *TimeDrop*.

If you have insights, perspectives, or knowledge that must be preserved, contribute to the next Veil Magazine.

Submit your topic proposal for the next *TimeDrop* by May 19, 2025.

Contact us at veil@claimsip.com

Knowledge is only lost
when it is left unspoken.

There will be more *messages*

Where they will land in spacetime, we do not yet know.

Until then, continue searching for what lies beyond the Veil.

There will be more *TimeDrops*

Every article submission received for the next *TimeDrop* will be archived for potential future retrieval, not just in 2025 but in 2062 and beyond.

Your article may not only reach the future, it may be *TimeDropped* into the past.

A legal argument you craft today might resurface centuries earlier, disguised in a form that fits the time period.

THE CONVERSATION ONLY BEGINS

“What you do in 2025 echoes across spacetime”

The “Veil” does not exist in a single place or time.

It exists wherever people seek to uncover what has been hidden.

Acknowledgments across time

This transmission could not have been reconstructed without the commitment of those who work to preserve and distribute knowledge and whose expertise ensures that no legal precedent, technological insight, or critical debate is ever lost or overlooked in the course of history.

Editors:

Ekaterina Pronicheva	// LinkedIn
Alexey Petrov	// LinkedIn
Igor Nevzorov	// LinkedIn
“ChatGPT” by OpenAI	// Website
Mikita Piatrou	// LinkedIn

Authors of the articles:

Anastasiia Maklakova	// LinkedIn
Mikita Piatrou	// LinkedIn
Maya Prosvitlyuk	// LinkedIn
Dmitry Korobkov	// LinkedIn
“ChatGPT” by OpenAI	// Website
“Copilot” by Microsoft	// Website

Brand Manager:

Nikolay Shevchenko	// LinkedIn

Designers:

Nikita Petrov	// LinkedIn
Yulia Nechaeva	// LinkedIn

Images by:

“DALL-E” by OpenAI	// Website

TimeDrop.01 ends.

Awaiting new signals...

VEIL MAGAZINE

The Veil Magazine was created by CLAIMS.

CLAIMS is an international consulting firm with a global presence.

DATA

AI

INNOVATION

CLAIMS provides strategic consulting in intellectual property, data protection, and emerging technologies, helping businesses navigate complex legal challenges, safeguard innovation, and achieve sustainable growth in a rapidly evolving digital landscape.

CLAIMS services include:

- *Developing Privacy Policies and Terms*
- *Assessing risks in data processing*
- *Consulting on global data regulations*
- *Developing compliance strategies*

- *Monitoring AI legal compliance*
- *Creating license agreements for AI training*
- *Mitigating risks in AI contracts*
- *Consulting on AI-related disputes*
- *Developing AI integration legal strategies*
- *Consulting on AI company structuring*

- *Developing IP protection strategies*
- *Registering trademarks, patents, and copyrights*
- *Protecting trade secrets*
- *Creating IP transfer agreements*
- *Assessing risks in IP usage*
- *Consulting on IP disputes*

claimsip.com　ig: @copyrighteddreams　linkedin: claims　tg: @claimsip