Advancing the Business of
Intellectual Property Globally

les Nouvelles

JOURNAL OF THE LICENSING EXECUTIVES SOCIETY INTERNATIONAL ■ VOLUME LX NO. 3 | SEPTEMBER 2025

lesi.org

Strategic Partnerships for IP Development and Market Growth

Join us to experience the unmatched business value that the LES USA-Canada 2025 Annual Meeting provides and see what Boston has to offer! Taking place at the Marriott Copley Place Hotel, this meeting features three days of education, outstanding topical programming, networking events with the over 500+ expected attendees from around the world, and global dealmaking opportunities.

Come and listen to our first keynote speaker, **Professor Giovanni Traverso, Associate Professor, Department of Mechanical Engineering at Massachusetts Institute of Technology.** He will review ongoing efforts towards the development of drug delivery and sensing technologies capable of operating in extreme environment like the gastrointestinal tract and others in his presentation.

In the afternoon, our second keynote speaker, **Jorge A. Goldstein, Founder of Sterne Kessler Goldstein & Fox and Author of "Patenting Life – Tales from the Front Lines of Intellectual Property and the New Biology"** will present during the I Life Science sector luncheon. He will discuss some of the IP cases in his book including fights over the ownership of body parts, patents on living beings, and the appearance of technology cycles involving university-industry collaborations.

Closing out the conference, we will have **Russell Levine, Partner at Kirkland & Ellis LLP, presenting his highly anticipated "Top 10 Court Decisions of the Year Affecting Licensing",** which he has presented at both the LES Annual Meeting and the AUTM Annual Meeting to standing-room-only audiences for many years.

We hope you will come and join the crowd!

NNE

For inquiries please email: lesam@northernnetworking.co.uk or call: +1 888-201-5902

For more information and to register, please visit:

les2025.org

lesusacanada.org

LESI's Annual Conference will focus on how innovation can lead to international impact and growth across all sectors. LESI 2026 will bring together key players and thought leaders to demonstrate how intellectual property acts as an international growth engine.

The meeting will be held in Dublin, Ireland, a fitting destination for the conference due to the country's combination of strategic policies for business, its stable economic environment, and its ability to attract global talent. The country is a significant draw for multinationals and is a hub for tech giants and pharma companies. Ireland's focus on education and innovation has produced a highly skilled workforce, further attracting high-value industries as well as supporting the formation and growth of new rapid scaling enterprises.

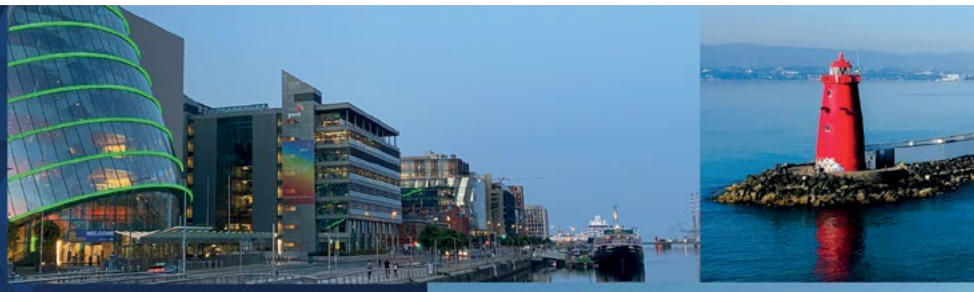
Please do take the opportunity to visit Dublin, Ireland's thriving capital city with its excellent connectivity and experience Ireland's world-renowned hospitality and rich cultural heritage.

For inquiries please email:

lesi2026@northernnetworking.co.uk

or call: **+44 1355 244966**

NNE



lesi2026.org

LES LICENSING EXECUTIVES SOCIETY INTERNATIONAL

thought LEADERS

Lesi's Thought Leadership Program

2025-2026

WEBINARS FOR ALL THREE TRACKS STARTING THIS FALL.

Check
lesi.org/thoughtleadership
for updates.

TRACK 1
SEPs
STANDARD ESSENTIAL PATENTS

TRACK 2
MEDTECH

TRACK 3
MANAGING DATA
IN IP-BASED TECHNOLOGY AND LICENSING

CALL FOR ARTICLES
Special Edition of *les Nouvelles* – March 2026

We invite authors at the forefront of innovation to contribute their insights. MedTech is not only the future of healthcare but also the driving force behind the life-sciences revolution, and les Nouvelles seeks your expertise. **We are curating a special MedTech-focused edition for March 2026, which will be featured at the LESI Annual Meeting in Dublin.**

Please direct any questions or submit your article proposals to **David Drews,** Editor of les Nouvelles, at **ddrews@lesi.org.**

Let us ensure that the next wave of medical advancements is supported by robust intellectual property.

LES INTERNATIONAL

OFFICERS

PRESIDENT	Jean-Christophe Troussel
PRESIDENT-ELECT	Ningling Wang
PAST-PRESIDENT	Sonja London
VICE-PRESIDENTS	Sophie Pasquier, Hemang Shah Tilman Müller-Stoy, Bob Held
CORPORATE SECRETARY	Georgina Busku
TREASURER	Matteo Sabattini
DIRECTORS	Ann Cannoni, Lionel Tan Claudio Ulloa
LEGAL COUNSELS	Gillian Fenton, Peter Ling
OBSERVER	Pam Cox
YMC OBSERVER	Marko Brumnik
EXECUTIVE DIRECTOR	Dana Robert Colarulli

DELEGATES

LES Society delegates appointed in advance of the LESI International Management and Delegates Meeting (IMDM) in Singapore, April 27, 2025."

ANDEAN COMMUNITY
Renzo Leonello Scavia
Juan Pablo Triana

ARAB COUNTRIES
-

ARGENTINA
Gustavo Giay
Verónica Canese

AUSTRALIA & NEW ZEALAND
Cherie van Wensveen
Dallas Wilkinson

AUSTRIA
Andreas Pföstl
Thomas Adocker

BENELUX
Carmen Correa Martin
Achim Krebs
Claudia Zeri

BRAZIL
Thereza G. Curi Abranches
Hannah Vitória M. Fernandes

BRITAIN & IRELAND
Graham Johnson
Karl Barnfather

CHILE
Jorge Fuentes
Andrea Lobos

CHINA
Shaohui Yuan
Christopher Shaowei

CHINA - HONG KONG
Annie Tsoi
Janet Wong

CHINESE TAIPEI
David W. Su
Gary Ma

CZECH REPUBLIC & SLOVAKIA
Denisa Švecová
Lucia Rybanská

FRANCE
Frédéric Portal
Isabelle Romet
Arnaud Michel

GERMANY
Christian W. Appelt
Ingo A. Bruckner
Alexander Haertel
Dr. Martin Heinebrodt
Gabriele Mohsler
Dr. Jochen M. Schäfer

HUNGARY
Georgina Busku
István Molnár

INDIA
Richa Pandey
Rajan Ailavadi

ITALY
Dario Paschetta
Mattia Dalla Costa
Marilena Garis
Antonio Di Bernardo

ISRAEL
Dalit Sagiv
Liad Whatstein

JAPAN
Hiroki Saito
Shoei Imai
Koji Saito
Chikako Hashimoto
Tomomi Fujita

KOREA
Han Sun Lee
Joo Sup Kim

MALAYSIA
Michelle Loi
Joshua Teoh Beni Chris

MEXICO
Claudio Ulloa
Héctor Chagoya

PHILIPPINES
Vida M. Panganiban-Alindogan
Victor N. de Leon

POLAND
Monika Kaczmarska-Paluchowska
Marta Sznajder

RUSSIA
Sergey Dorofeev
Alexey Vakhnin

SCANDINAVIA
Suvi Julin
Ia Modin

SINGAPORE
Olivia Koentjoro
Catherine Lee

SOUTH AFRICA
Joanne van Harmelen
Barbara Berdou

SPAIN & PORTUGAL
José Miguel Lissén
Jordi Ilario

SWITZERLAND
Kilian Schärli
Philipp Groz

THAILAND
Vikran Duangmanee
Kaewkan Wasanasuk

TURKEY
Murat Idal
Mustafa Cakir

U.S.A. AND CANADA
Ann Cannoni
Evelyn Chen
Bob Held
Karthika Perumal
Jeff Whittle
John Paul
Jayde Wood

SOCIETY OFFICERS

CHAPTER	PRESIDENT	SECRETARY
ANDEAN COMMUNITY	Renzo Scavia	Juan Pablo Triana
ARAB COUNTRIES	- vacant -	- vacant -
ARGENTINA	Gustavo P. Giay	Helena Noir
AUSTRALIA & NEW ZEALAND	Cherie van Wensveen	Christopher Wilkinson
AUSTRIA	Karin Hofmann	Thomas Adocker
BENELUX	Carmen Correa Martin	Jurriaan Jansen
BRAZIL	Bruna Rego Lins	Ana Amélia Araripe Montenegro
BRITAIN & IRELAND	Graham Johnson	Tom Gaunt
CHILE	Jorge Fuente	Pablo Acevedo
CHINA-HONG KONG	Annie Tsoi	James Choi
CHINA	Shaohui Yuan	Aimin Huo
CHINESE TAIPEI	David W. Su	Smith S. Huang
CZECH REPUBLIC & SLOVAKIA	Vojtěch Chloupek	Miroslav Černý
FRANCE	Frédéric Portal	Matthieu Lebrun
GERMANY	Gabriele Mohsler	Christian Czychowski
HUNGARY	Levente Pethő	Georgina Wachtler Busku
INDIA	Richa Pandey	Lakshika Joshi
ISRAEL	Hananel Kvatinsky	Dalit Sagiv
ITALY	Mattia Dalla Costa	Simona Cazzaniga
JAPAN	Chikako Hashimoto	Kazumi Koyama
KOREA	Joo Sup Kim	Kwang Yeon Hwang
MALAYSIA	Joshua Teoh Beni Chris	Alyshea Low Khye Lyn
MEXICO	Mariana González-Vargas	Guillermo Roura
PHILIPPINES	Vida Panganiban Alindogan	Reena Mitra-Ventanilla
POLAND	Marta Sznajder	Monika Kaczmarska
RUSSIA	Evgeny Alexandrov	Alexey Vakhnin
SCANDINAVIA	Ia Modin	Suvi Julin
SINGAPORE	Olivia Koentjoro	Anna Toh
SOUTH AFRICA	Joanne van Harmelen	Nolene Singh
SPAIN & PORTUGAL	Erika Jiménez Leube	Guillermo Criado
SWITZERLAND	Philipp Groz	Kilian Schärli
THAILAND	Vikran Duangmanee	Ploynapa Julagasigorn
TURKEY	Hande Hançer	Murat Idal
USA & CANADA	Evelyn Chen	Louise Levien

les Nouvelles

Volume LX Number 3 (ISSN 0270-174X)

les Nouvelles is published quarterly by the Licensing Executives Society International (LESI). LESI is a global association, established in 1973, of 33 national and regional Member Societies, in more than 90 countries, serving more than 6,000 individuals engaged in the profession of licensing intellectual property assets to advance the development and commercialization of new technologies. The Journal is available to all current, dues-paying LES members and subscriptions are available for a fee to non-members. Please contact the Editor for further details or go to www.lesi.org/les-nouvelles.

A peer review and evaluation system is used to maintain the scholarly nature of the material published in this journal. All articles submitted for publication are reviewed and evaluated by members of the Editorial Review Board (ERB). The ERB members are chosen for their expertise in the fields of licensing and intellectual property. All evaluations are reviewed in a double-blind fashion to remove any bias in the results. The final decision on publication rests with the Editor.

A guideline for authors can be found on our Web site at the following address:
www.lesi.org/lesnouvelles/advertise.asp#submission

DEADLINES FOR les Nouvelles:

Copy for publication in les Nouvelles should be received by the Editor-in-Chief as far as possible in advance of the final deadlines, **January 1, April 1, July 1** and **October 1.** Articles are reviewed by the LES Editorial Review Board, and they are published as soon as possible after acceptance. All materials are to be submitted electronically in either MS Word or Text Only format.

Contents

VOLUME LX NO. 3 | SEPTEMBER 2025

Dana Robert Colarulli
LESI Executive Director
Tel: +(202) 841-0276
E-mail: dana@lesi.org

David Drews
Editor
12526 High Bluff Drive, Suite 300, San Diego, CA 92130
Tel: +1-858-603-8825
E-mail: editor@lesi.org

Patents and Trade Secrets as Complementary Protection Mechanisms

By

Peter D. Camesasca, Ph.D.
Partner
Camesasca bvba
Brussels, Belgium
peter@camesasca.eu

DuckSoon Chang
Partner
Kim & Chang
Seoul, Korea
ducksoon.chang@kimchang.com

Prof. Dr. Heinz Goddar
Partner
BOEHMERT & BOEHMERT
Munich, Germany
goddar@boehmert.de

Joo Sup Kim, Ph.D
IP Advisor
LX MDI
Seoul, Korea
joosupkim11@gmail.com

Melanie Müller
Attorney at Law
BOEHMERT & BOEHMERT
Bremen, Germany
mueller-melanie@boehmert.de

Dr. Ralph Nack
Partner, Noerr
Partnerschaftsgesellschaft mbB
Munich, Germany
ralph.nack@noerr.com

Ichiro Nakatomi, Ph.D.
President
Avida Science, Inc.
Tokyo, Japan
inakatomi@avida-science.com

Jonathan Porath
PhD Student
University of Cologne
Germany
jonathan.porath@yahoo.de

Photo: **Workshop held by the authors at LES 2025 in Singapore**

This Article is based on a workshop conducted by the authors at the LESI Conference 2025 in Singapore. The session explored how innovation can be safeguarded not only by patent law but also through trade secret protection – and how both systems can operate complementarily. Using comparative insights from Japan, Korea, and Germany/EU, the discussion addressed the interaction between the two regimes, particularly in the context of cross-border enforcement and digital transformation.

While the main focus was on protecting innovation from an IP perspective, the debate also highlighted an important concern: the interplay between trade secret protection and antitrust law can present unforeseen challenges. Stakeholders may find themselves in situations where they are simultaneously bound by confidentiality obligations and required to license or disclose the protected information under competition law.

The workshop also examined emerging challenges in innovation-driven industries, where patents and trade secrets are increasingly used to safeguard complementary aspects of an innovation – such as core inventions protected by patents and implementation know-how or training data retained as confidential information. Finally, it considered the potential value of establishing an international Trusted Depository for Trade Secrets as a means to facilitate safe, lawful, and commercially viable access to confidential information – especially when used in conjunction with patented technologies.

I. Introduction:

The Complementary Relationship Between Patents and Trade Secrets

The legal protection of technical innovations rests on two central pillars: patents and trade secrets. While fundamentally different in their legal structure, both serve the purpose of incentivizing innovation and safeguarding investments in R&D.

A patent grants the right to exclude others from using a disclosed invention for a limited period, in exchange for making the invention publicly available. By contrast, a trade secret protects commercially valuable information without disclosure, offering potentially indefinite protection – but only as long as secrecy is maintained and reasonable steps are taken to safeguard the information.

Although these mechanisms are often portrayed as alternatives, in practice they are frequently used in parallel to cover complementary aspects of the same innovation. For instance, the core invention may be protected via patent, while the implementation know-how, optimization processes, or AI training data may be retained as trade secrets.

This strategic dual protection is particularly relevant in sectors such as artificial intelligence and process engineering, where not all valuable knowledge qualifies for patent protection, and in biotech, where product life cycles can be long enough for exclusivity to remain commercially valuable even after the expiry of the 20-year patent term.

II.
National Perspectives on Trade Secret Protection and Litigation

1. INTERNATIONAL AND EU-LEVEL

Trade secrets are an essential asset for businesses seeking to protect economically valuable information, particularly when such information does not qualify for registration. At the international level, trade secrets are protected under Article 39 of the TRIPS Agreement, which provides a foundational definition adopted by most jurisdictions worldwide.

According to Article 39(2), protection is afforded to information that:

- **Is secret, in the sense that it is not generally known or readily accessible;**
- **Has commercial value because it is secret; and**
- **Has been subject to reasonable steps under the circumstances to keep it secret.**

This definition emphasizes a balance: robust enough to protect valuable commercial interests, yet flexible enough to avoid placing an excessive burden on secret holders to unnecessarily enclose knowledge that should be publicly accessible. The benchmark is not absolute security, but reasonable measures appropriate to the industry and business context.

Building on TRIPS, the EU adopted the Trade Secrets Directive (TS Directive) in 2016, with the aim of establishing a harmonized legal framework across Member States. The TS Directive was designed to close significant gaps and disparities in trade secret enforcement and to increase legal certainty for businesses operating within the internal market.

Key features of the TS Directive include:

- **A harmonized definition of trade secrets that mirrors TRIPS;**
- **Provisions detailing lawful and unlawful acquisition, use, and disclosure of trade secrets;**
- **Enforcement mechanisms, including civil remedies such as injunctions, damages, and corrective measures;**
- **Procedural safeguards to ensure confidentiality during legal proceedings (e.g., confidentiality clubs, restricted access, non-public hearings);**
- **Proportionality clauses balancing trade secret protection with fundamental rights, such as freedom of expression and access to information.**

Each EU Member State was required to incorporate the TS Directive into national law by June 2018. Germany implemented the TS Directive through the Act on the Protection of Trade Secrets (GeschGehG), which came into force in April 2019.

One of the most critical practical consequences of the TS Directive and its national implementations is the emphasis on **"reasonable steps"** to maintain secrecy. This includes:

- **Physical and IT security;**
- **Contractual safeguards (e.g., NDAs, confidentiality clauses);**
- **Internal compliance protocols;**
- **Employee training and monitoring.**

Failure to implement such measures can result in the loss of protection, underscoring the importance of proactive confidentiality strategies.

Although the TS Directive harmonized substantive law, enforcement culture remains fragmented. The Report of the EUIPO reveals significant variations in litigation volume:

Italy leads with 151 recorded TS disputes, surpassing expectations based on GDP and innovation indices. Germany, despite its strong industrial base, has a relatively low number of cases, indicating cautiousness in litigating trade secrets. France and the Netherlands reflect a more proportional litigation culture, closely aligned with their economic indicators.

These findings suggest that while harmonized legislation exists, procedural traditions, judicial efficiency, and business culture significantly influence whether trade secret holders opt for litigation.

2. JAPAN

The history of trade secret law in Japan dates back to a draft formulated by the Ministry of Agriculture and Commerce in 1911. Subsequently, the Unfair Competition Prevention Law was enacted in 1934, and trade secret protection was clearly established in 1990. The revised Unfair Competition Prevention Law entered into force in 2003 and introduced criminal liability for trade secret infringements, which until then had been addressed solely under civil law. These unfair competition prevention laws are consistent with Article 39 of the TRIPS Agreement mentioned above, which obliges companies to protect their intellectual property.

Recently, in 2023, a law was enacted to partially amend the Unfair Competition Prevention Law and other laws, which came into effect on April 1, 2024. The Amendments include: (1) prevention of acts of imitation in the digital space, (2) enhanced protection of TS and limited provision data, (3) expansion of provisions for calculating damages, (4) expansion of presumptions of use, (5) enhancement of jurisdiction over international TS infringement cases, and (6) strengthening and expansion of penalties for bribery of foreign public officials.

The number of trade secret disputes remains relatively small – there were 26 cases in 2023 – but has been steadily increasing year by year. The overwhelming majority of lawsuits are filed against mid-career professionals who leave their jobs to work for (often overseas) competitors or to establish their own companies in the same field. Even if the former employer wins in court, the damage is usually irreversible: leaked information cannot be "unleaked," and once it has entered the public domain, competitors can hardly be prevented from using it. Most Japanese companies are therefore focusing their efforts on preventing such leaks by taking the following measures:

1. **Manual of Information Management for Business Operation**
2. **Information Management Post-Employment**
3. **Online Training at the Beginning of Work, Annually and Retirement**
4. **Penalty Rules**
5. **Management of Security Control**
6. **Information Control to the Third Party**
7. **Management for Retirees**

3. KOREA

The basic statute governing trade secret protection in Korea is the Unfair Competition Prevention and Trade Secret Protection Act (UCPA). Given the critical role that technology plays in the Korean economy, Korea has expanded the scope of trade secrets eligible for protection and increased the level of civil and criminal sanctions on the misappropriating party.

As in other jurisdictions, a trade secret is defined to require three elements: secrecy, economic value, and efforts to maintain as a secret. Regarding the third element, namely, efforts to maintain as a trade secret, the statute has relaxed the level of efforts necessary to demonstrate this element over the years. Previously, the statute required "substantial efforts" to maintain secrecy, and under the old statute it was not unusual for trade secret civil or criminal actions to be dismissed for failing to meet this requirement. In 2019, the term "substantial" was amended to "reasonable," and in 2024, the statute was further amended to remove the "reasonable efforts" language entirely. This means that as long as the secrecy of the information is maintained, the third requirement is likely to be met, without a need to refer to specific "efforts" taken for the maintenance. Future court decisions will provide more clarity and guidance on what actions at the minimum would meet this lowered standard.

Under the UCPA, there are two types of sanctions for trade secret misappropriation. First, for civil remedies, a legislation was enacted in 2019 that increased punitive damages for willful misappropriation to a maximum of three times the actual damages, and in 2024, this was further increased to a maximum of five times the actual damages. On the criminal side, penalties for trade secret misappropriation are already severe, with potential imprisonment of up to 10 years or fines not exceeding 500 million Korean Won (approximately USD 350,000). Heavier penalties apply for misappropriation intended for use overseas.

Korea's economy heavily relies on the high-tech industries such as semiconductors, display technology, and lithium batteries. Thus, the Korean government considers protection of technologies to be critically important. This is demonstrated by the specialized investigation teams that are formed in various investigation authorities, including the Korean Intellectual Property Office (KIPO), which are all equipped with experienced personnel, including computer engineers, forensic experts, and digital analysts. When reasonable grounds for suspicion are shown, the investigation authorities pursue a court warrant to conduct criminal searches and seizures to secure necessary evidence. This criminal search and seizure process serves as an effective discovery mechanism. Thus, civil actions in Korea, where only limited discovery is allowed, typically follow criminal proceedings once evidence of infringement has been secured through the criminal investigation.

In addition to the police, the prosecutor's office and KIPO, there is also a number of other government agencies that actively enforce measures against industrial espionage and trade secret misappropriation. Two key agencies among them include the Korea National Intelligence Service (NIS) and the Korea Trade Commission (KTC). First, NIS also conducts investigations into trade secret cases, but this agency focuses its investigations on potential misappropriations that occur for use outside of Korea. Second, trade secret holders may seek assistance from KTC to exclude imports and exports of goods that infringe their trade secrets. The remedies provided by KTC are similar to the remedies available in the U.S. International Trade Commission.

III. New Challenges in the AI Era

While generative AI has the potential to help companies enhance their competitiveness and accelerate growth, it also has significant implications for the protection of confidential corporate information:

(1) If an employee enters information related to trade secrets when using a generative AI, the AI may learn that information. Any information entered into an AI system will be stored in the system and can be

very difficult to delete. If secret information is leaked as a result and becomes public knowledge, it will no longer be afforded legal protection.

(2) Even if the data input does not directly contain a given trade secret, the AI system may be able to infer some of the information by analyzing the input. An AI trained on trade secrets will use that knowledge to generate output, potentially allowing competitors to indirectly benefit from the information. Not only would competitors indirectly benefit from the trade secret, but if a patent application is filed using the AI, not only would there be no evidence of its information leakage, but its legal protection could be lost.

IV. Trusted Trade Secret Depository – Vision and Challenges

1. DESCRIPTION OF THE TRUSTED DEPOSITORY

The concept of a Trusted Depository for Trade Secrets is an innovative tool that complements existing protection mechanisms. The idea is not to replace traditional confidentiality strategies, but rather to enhance them by enabling the creation of verifiable, tamper-proof records of secret information — without disclosing the underlying content itself.

This approach is particularly effective in addressing critical issues such as establishing prior ownership, securing investments, or preparing for litigation. Blockchain technology would be at the technological core of the Trusted Depository, providing encryption and hashing mechanisms.

Where confidentiality is the absolute priority, the data is encrypted and stored off-chain, while only a secure reference is recorded on the blockchain. Where the focus lies on proving existence and integrity — for example, in the case of prior use rights — a cryptographic hash of the data is stored. This method ensures that even the smallest alteration is immediately detectable. The decentralized nature of blockchain ensures that no single entity can tamper with the record, while verification processes allow any authorized party to confirm authenticity with ease.

Practical use cases include investment and financing: Companies often need to demonstrate the value of intangible assets without disclosing them. A blockchain-secured Trusted Depository enables neutral appraisers to validate such information while maintaining confidentiality toward investors or banks. The system would also be useful in litigation procedures. Courts often require sensitive information during trade secret disputes. The Trusted Depository allows for tightly controlled access—judges and lawyers can review necessary information without risking leaks. A Trusted Depository would also facilitate the conclusion of licensing agreements, especially when combined with smart contract technology. Instead of direct data exchanges, the depository's public front could include abstract descriptions of deposits, allowing a large group of potential licensees to take note of the secret without disclosing its content.

Finally, from a compliance perspective, the Trusted Depository supports companies in fulfilling their obligation to take 'reasonable steps' to protect confidential information under frameworks such as the EU's TS Directive. In short, by leveraging blockchain and smart contracts, the Trusted Depository not only secures trade secrets, but also enables controlled access, reduces negotiation risks, and strengthens legal enforcement.

2. ROLE MODELS AND EXISTING SYSTEMS

a) Korean 'Trade Secrets Original Certificate Service'

Korea has long implemented two different trade secret depositary systems.

The first is the 'Trade Secrets Original Certificate Service' where a trade secret holder may register the electronic fingerprint of an electronic document containing their trade secrets with one of the government agency or private organizations that are designated by the Commissioner of the Korean Intellectual Property Office. Under this system, which is operated pursuant to the Unfair Competition Prevention and Trade Secret Protection Act, the actual contents of the document – namely, the trade secrets themselves – are not registered. This system is designed to assist trade secret holders in demonstrating that the specified electronic document was in existence on the date it was registered, if and when such need arises.

The second is the "Technology Deposit System" where a company may deposit its technical documents or materials containing trade secrets with a government agency. This deposit system is operated pursuant to the Act on the Promotion of Collaborative Cooperation between Larger Enterprises and Small-Medium Enterprises. There are two primary benefits to this system. First, it helps technology holders, especially smaller companies, in demonstrating that their deposited technology was in existence on the date it was deposited. The government manual states that this deposit system would be particularly useful in cases where a larger business partner unlawfully discloses the depositing company's technology to another subcontractor to allow another subcontractor to produce and supply the same quality parts at a lower

price. In such cases, the deposit serves as evidence that the technology in question rightfully belonged to the depositing company, not to the larger business partner, as of the date of deposit, thereby protecting the depositing company's IP rights. The second utility is similar to a software escrow arrangement. In other words, by having certain technologies deposited, it allows the transaction counterpart to the technology holder access to the deposited technology if the technology holder ceases its operations, such as in the case of bankruptcy. For example, a three-party escrow agreement can be established, including the government depository.

Under both systems, the identity of the depositing party and the types or fields of deposited technologies are not made available to the public.

b) Budapest Treaty

The International Microorganism Deposit System under the Budapest Treaty of 1977 was created to address a practical problem: when patenting inventions involving microorganisms, written disclosure was often insufficient to enable a person skilled in the art to replicate the invention. As a solution, inventors were — and still are — allowed to deposit samples of microorganisms with a certified International Depositary Authority.

Today, 51 recognized institutions worldwide fulfill this function, and they guarantee secure storage for at least 30 years. Depositing biological material serves multiple legal purposes: (1) It satisfies disclosure requirements for patentability. (2) It serves as prior art in disputes, anchoring the state of knowledge at a certain time. And (3), it ensures public access to biological material after patent expiration, thereby supporting scientific and industrial development.

While Budapest deposits are designed to enable public disclosure, a Trusted Depository for Trade Secrets would, in contrast, be designed to guarantee secrecy rather than publicity.

c) WIPO PROOF

WIPO PROOF was a digital fingerprinting and timestamping service launched by WIPO in 2020. The idea behind WIPO PROOF was simple yet powerful: by submitting a file, the user could generate a time-stamped token proving the file's existence and ownership at a specific moment in time.

However, despite its technological merit, WIPO PROOF was discontinued in early 2022 as part of WIPO's internal restructuring. Importantly, the tokens created through the service remain valid indefinitely. Users can still verify these tokens and generate certificates — now free of charge — although WIPO will only retain these tokens in its system for five years from creation, without renewal options. This means that users must download and securely store both the original file and the associated token themselves.

While WIPO PROOF provided excellent evidentiary value, it lacked functionalities that could stimulate licensing activity. There was no public database and no additional tools that would allow for controlled access or facilitate negotiations.

d) i-DEPOT of the Benelux IPO

The i-DEPOT of the Benelux Intellectual Property Office is an official system that allows individuals and businesses to secure a date-stamped proof that a certain idea, design, concept, or creation existed at a specific point in time. It does not create an IP right like a patent or a trademark, but it provides strong evidentiary support in legal disputes — for example, to prove prior authorship or originality. When a file is uploaded, a certificate confirms the time and content of the deposit. Importantly, the content remains confidential unless the user decides to disclose it. Thus, the i-DEPOT is a simple, fast, and relatively inexpensive tool to protect ideas, particularly in the early phases of innovation — before formal IP rights can be applied for.

3. ACCESS AND LICENSING

Trade secrets are rarely licensed out independent of any associated patents. In the view of the authors, this is not necessarily indicative of a general unwillingness on the part of holders of secret technologies and information to monetize their intellectual property through licensing. Rather, it is at least partially a consequence of the practical difficulties involved in initiating and conducting licensing negotiations when the subject matter must remain secret until an agreement is reached.

Beyond providing tamper-proof evidence of existence and ownership of trade secrets and data, a blockchain-based Trusted Depository could serve as a much-needed interface between trade secret holders and potential licensees. Upon deposit, users would have the option to provide a high-level abstract of the content, which would be cataloged and published in a searchable database with the depositor's contact information.

Besides merely connecting the parties of a potential licensing agreement, a blockchain-secured depository would also minimize the risk of unauthorized disclosures during negotiations. While no technology in the world can ever eliminate the risk of human error or intentional breaches of confidentiality, this technology would greatly reduce the risks associated with the transmission of data.

Licensing agreements and their terms remain matters of national law. While further harmonization would be desirable, establishing a Trusted Depository is unlikely to meaningfully contribute to this goal. The inclusion of blockchain and smart contract technology can, however, increase legal certainty in other ways: When parties agree on licensing terms, smart contracts can automatically release access once specified conditions are met, such as verification of payment or conclusion of non-disclosure agreements. Importantly, smart contracts can also accompany negotiations, granting limited access step by step when certain milestones are reached, such as when a security deposit is made. Especially when combined with security deposits, smart contracts can also play an important role in enforcing final licensing agreements by automatically transferring these funds in case of a breach of confidentiality, for example.

4. PATENT LAW IMPLICATIONS AND RISKS

The Trusted Depository System presumes that there is a growing interest in omitting essential information from patent applications. In this regard, there appears to be potential for tension between the Trusted Depository System and the very objective of the patent system: granting exclusive rights for a limited time in exchange for full disclosure of the invention. Specifically, in case the Trusted Depository is used by patent holders to omit certain pieces of information from patent applications and deposit such omitted information in the depository to increase their chances of selling separate licenses to this additional information – would this not conflict with (among others) the U.S. "best mode" requirement for patenting? It appears that, while a failure to disclose the best mode is no longer a basis for invalidating a patent under the U.S. America Invents Act, it is still considered a legal requirement for patent applications.

In addition, one of the typical defenses in trade secret misappropriation actions is that the plaintiff already disclosed the alleged trade secrets through patent filings and therefore is not eligible for trade secret protection. In practice, it is very difficult to determine whether an asserted trade secret has already been disclosed in the patent filings, especially when there is significant but incomplete overlap between the two. Addressing this issue would contribute to a more reliable depository system.

5. COMPETITION LAW CONSIDERATIONS AND RISK

Although trade Secrets and patents provide essential safeguards for innovation, their use must also be assessed in light of antitrust laws. In particular, antitrust concerns may arise when trade secrets are used to restrict market access, limit interoperability or prevent follow-on innovation.

Antitrust authorities have already intervened where the use (or misuse) of trade secrets contributed to market foreclosure. In EU cases such as Microsoft Interoperability & Google AdWorks, regulators compelled partial disclosure of trade secrets in the name of fair use. Furthermore, in the Reuter/BASF and Campari & Pronuptia cases, non-compete or exclusivity clauses tied to confidential know-how were found to extend beyond what was objectively necessary.

The above cases illustrate the careful balance required between protecting confidential information and ensuring competitive market conditions. On one hand, companies must take "reasonable steps" to safeguard trade secrets, as required under the TS Directive; on the other hand, overly restrictive practices – particularly in licensing, distribution, or data-sharing contexts – may attract regulatory scrutiny. Even confidentiality protections in investigations can be challenged, as seen in the Google Automotive Services case before the German Federal Antitrust Authority (Bundeskartellamt).

As concepts such as Trusted Depositories and smart licensing mechanisms become more widespread, innovators need to carefully consider the antitrust implications. Mechanisms like alternative dispute resolution, licensing transparency, and proportional access safeguards can help bridge the gap between IP protection and antitrust law obligations, ensuring that legal strategies remain effective on both fronts.

V. Conclusion and Outlook

Trade secrets play an important role in the protection of innovation, especially where formal IP rights are unavailable, impractical, or insufficient. As technological landscapes are evolving rapidly, legal frameworks are struggling to keep up. Trade secrets have existed for centuries, yet the increasing codification of dedicated trade secret legislation has only been a phenomenon of the most recent decades. To close emerging gaps in protection, companies and innovators are increasingly turning to so-called hybrid protection, combining registered IP rights with additional secrecy.

This new protection model poses new challenges, especially at the intersection of trade secret law and antitrust legislation. The establishment of a Trusted Depository could help facilitate the licensing and controlled sharing of trade secrets. This would be an important contribution to limiting the anti-competitive nature of an innovation landscape that increasingly relies on secrecy. ■

Revisiting Goldilocks:
Reasonable Measures to Protect Trade Secrets in an Era of Enterprise Collaboration and Cybersecurity Risk Management

By

Steven R. Kursh, Ph.D., CSDP, CLP
Software Analysis Group
Cambridge, MA
s.kursh@softwareanalysisgroup.com

Pratik Patel, BS, MBA
Software Analysis Group
Cambridge, MA
p.patel@softwareanalysisgroup.com

ABSTRACT

Our objective in this paper is to provide frameworks and suggested policies that enterprises can use to protect their trade secrets in an era of increased collaborations and greater cybersecurity risks. We discuss how it is necessary for management at enterprises, particularly management involved with licensing activities within industry collaborations, to expand the scope of their reasonable measures to protect trade secrets beyond legal and compliance frameworks. The paper also reviews cybersecurity frameworks from the National Institute of Standards (NIST) and the International Standards Organization (ISO).

We review guidelines from the World Intellectual Property Organization (WIPO) and recommend that enterprises have a layered-security approach to ensure resiliency. Additionally, we discuss how enterprises operating in Europe and Canada face challenges managing personnel given privacy compliance laws and issues related to information security practices to avoid conflicts and ensure lawful practices. Consistent with our earlier research and findings from the Sedona Conference, an underlying theme throughout this paper is that enterprises need to balance protection of trade secrets without stifling innovation, complicating collaborations, or creating operational frictions with suppliers, customers, and other partners in their ecosystems.[1]

I. Introduction

Approximately three years ago in an article titled "The Goldilocks and Three Bears Dilemma: Adopting Reasonable Measures to Protect Trade Secrets in the New Work Environment,"[2] we explored the central challenge enterprises face when protecting trade secrets in an era of remote work: how much security and related measures were needed?

Since publication of the article, we have continued our research and in-the-field work related to reasonable measures and best practices. While the underlying question of "how much security and related measures" remains, the factors driving our assessment of reasonable measures at enterprises have become more complex. Many enterprises now actively participate in collaborations with other enterprises that impact product and service development, including, for example, within the software industry, customization and configuration of software at client and/or subscriber sites, support, and other activities. Additionally, cybersecurity has been more integral to building a secure and protective infrastructure.

Senior managers at enterprises, including management involved with licensing with other enterprises and with clients/customers, should be

1 *Sedona WG12 Commentary on the Governance and Management of Trade Secrets, Sedona Conference,* April 2022.

2 Kursh, Steven and Pratik Patel, "The Goldilocks and Three Bears Dilemma: Adopting Reasonable Measures to Protect Trade Secrets in the New Work Environment," *les Nouvelles, Journal of the Licensing Executives Society International,* Volume VLII, March 2022.

attuned to these changes. We suggest that they consider developing and implementing a consistent strategy for protection of confidential and proprietary information, including trade secrets, that can be used when structuring agreements and, more broadly, collaborative relationships with other enterprises, particularly in industry ecosystems.

Failing to do so may not only increase the risk of trade secret theft but also may significantly weaken an enterprise's position in legal disputes. Many of us are well aware that courts often require evidence that a company took active steps to protect its confidential and proprietary information, including trade secrets. Whatever practices your enterprise now follows, even though consistent with industry customs and practices, it may be time to take a look and consider making changes.

This article builds on our prior work by examining the evolution of reasonable measures and their growing intersection with cybersecurity frameworks and risk management. We remain mindful and ask please that you, too, remain mindful of the words from the Sedona WG12 Commentary on the Governance and Management of Trade Secrets: "Trade secrets should be protected by efforts that are reasonable under the circumstances to maintain their secrecy and value. Absolute secrecy is neither possible nor required. There is no one-size-fits-all approach."[3] Nevertheless, many of us tasked with the development and implementation of policies to protect trade secrets must strive to meet the hurdle of being reasonable relative to industry customs and practices.

The remainder of this article is divided into three-related sections. First, we review trends that are driving the evolution of reasonable measures to protect trade secrets, including collaboration and cybersecurity with risk management. Second, we discuss possible frameworks and policies that enterprises can use to develop and implement reasonable measures to protect their trade secrets. Our discussion draws from recent work by the World Intellectual Property Organization (WIPO) that can be used to help determine "the what" that should be considered by enterprises. We also consider the how and provide a review of cybersecurity frameworks from the National Institute of Standards (NIST) and the International Standards Organization (ISO) as frameworks.

The last section of the article discusses our key recommendation – that enterprises develop and implement multilayered frameworks with policies that incorporate traditional compliance tools with cybersecurity and risk management.

II. Trends Driving Evolution of Reasonable Measures in the Protection of Trade Secrets

In our experience "reasonable measures" to protect trade secrets has been largely rooted in legal and compliance frameworks. "Reasonableness" was primarily assessed by a checklist of formal safeguards: confidentiality agreements, employee NDAs, and document labeling, for example, were central. These actions were viewed through the lens of legal defensibility that a company could prove it took steps consistent with its ongoing-business practices. This approach extended across traditional measures like physical security (e.g., access control), employment practices (e.g., background checks), and administrative controls (e.g., policies and procedures for information handling). These controls were sufficient for environments where data remained on-premises, access was hierarchical, and collaboration was tightly managed.

As we discussed in our first Goldilocks paper, the safeguards had to be updated to account for remote work, which grew rapidly during the COVID-19 pandemic.

Now, however, the landscape has further evolved, and reasonable measures need, accordingly, to evolve further beyond traditional safeguards and the suggested approaches that we discussed in the first paper.

Two key trends are driving the need for change and expansion of our approach regarding reasonable measures.

First, enterprises, reflecting the growth in global ecosystems and supply chains, are joining with other enterprises to collaborate in consortiums where confidential and proprietary information, including trade secrets are shared, creating in effect, multiple ongoing partnerships with multiple enterprises. In other words, instead of "one-to-one" as in traditional partnerships, management involved in licensing now have challenges related to, in the parlance of software engineering and databases, "many-to-many" relationships in collaborative ecosystems.

Second, consistent with customs and practices, many enterprises are expanding the scope of their efforts to consider cybersecurity and risk management. This shift as part of overall cybersecurity efforts includes robust incident response and recovery plans, vetting and managing vendor and third-party access, and maintaining comprehensive data governance frameworks that define how sensitive information is classified, stored, and monitored throughout its lifecycle.

3 *Sedona WG12 Commentary on the Governance and Management of Trade Secrets, Sedona Conference,* April 2022, p. vii.

Additionally, monitoring and auditing capabilities are now critical for detecting misuse and demonstrating ongoing stewardship.

We discuss these trends and provide suggested recommendations below.

III. Increasing Participation in Collaborations

Due to a combination of factors including, but not limited to global supply chains, the internet, focus on core competencies, and market demands for speed and innovation, enterprises are increasingly choosing to work in collaborations with other enterprises in industry ecosystems. These collaborations typically require multifaceted licensing negotiations and resulting agreements that significantly differ from the past. In effect, an enterprise may now have multiple partnerships with many other enterprises simultaneously that are part of an overall value chain. These relationships exceed the traditional partnership models of the past. Indeed, such ecosystems are becoming increasingly common in sectors where innovation, standardization, and joint problem-solving are critical. Hence, enterprise members often have to share confidential and proprietary information, including trade secrets, as part of enabling interoperability.

In our experience most enterprises often seek and maintain collaborations in response to market needs. Consistent with industry customs and practices, these collaborations often involve product development, product testing, sales, implementations, and services. Consider, for example, distribution networks for many enterprise software companies and how the implementation partners often require access to confidential and proprietary information, including trade secrets, to do their implementation work at licensees or in the case of SaaS, subscribers. Similarly, consider joint product development in the life sciences and other activities that often require complex licensing activities. Indeed, in order for ecosystem business models to work, they require per EY (Ernst & Young Global Limited)"...sharing the data, intellectual property and confidential information,"[4] an approach that runs counter to the core principles of protecting trade secrets.

The trend for enterprises to engage in collaborative ecosystems is well recognized. McKinsey notes, for example, how businesses can leverage digital ecosystems to drive growth and innovation.[5] The McKinsey article "...estimate(s) that at least a dozen sectors, including B2B services, mobility, travel and hospitality, health, and housing, are reinventing themselves as vast ecosystems, networks of networks that could add up to a $60 trillion integrated network economy by 2025."

McKinsey's findings are not unique. The Business Performance Innovation network (BPI) found in a survey that 44 percent of all businesses "...seek alliances for new ideas, insights and innovation." [6] We can expect to see more collaborations and new ecosystems being formed going forward.

Collaborations within ecosystems already exist in many industries.[7] In the automotive industry, for example, the Autonomous Vehicle Computing Consortium (AVCC)[8] requires members to share information to accelerate the mass production of safe and affordable vehicles with automated and assisted driving solutions. This collaboration has accelerated the development of autonomous systems, but it has required clear protocols to define what information is shared, how it is used, and how it is protected. Similarly, in pharmaceuticals and life sciences, consortiums like TransCelerate BioPharma bring together major drug companies to address common R&D challenges.[9] Likewise, in technology and semiconductors, organizations like the RISC-V Foundation facilitate collaboration on architecture standards, chip design, and manufacturing techniques.[10]

While collaborations clearly make sense from a corporate strategy perspective among other factors, the very nature of collaborations (aka consortiums) make trade secret protection inherently more complex. While partnerships raise many challenges in regard to trade secret protections, collaborations are even riskier since they involve broader risk surfaces with more ambiguity that requires clear business and operational governance.[11]

This is particularly true with collaborations involving software trade secrets. Many software-related trade secrets have become digitally fragmented and globally distributed by spanning among cloud platforms, remote workforces, and external partners. The notion of perfect protection is not realistic - it's dangerous, as it creates a false sense of security and leads to stagnation of reasonable measure approaches.

Indeed, in our experience the scope and nature of risks related to the loss of trade secrets for enterprises working within collaborations are much greater than with partnerships. More specifically, we

4 https://www.ey.com/en_gl/ecosystems/the-ceo-imperative-are-you-mastering-your-ecosystem-strategy.

5 https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/ecosystem-2-point-0-climbing-to-the-next-level.

6 https://bpinetwork.org/.

7 https://www.forbes.com/sites/katevitasek/2022/11/30/partnerships-three-data-backed-reasons-two-heads-are-better-than-one/.

8 https://avcc.org/.

9 https://www.transceleratebiopharmainc.com/.

10 https://riscv.org/.

11 https://widgets.weforum.org/blockchain-toolkit/pdf/consortium-governance.pdf.

see enterprises that are members of collaborations typically implementing robust legal frameworks and governance structures to safeguard trade secrets. This typically includes multilateral NDAs, clear definitions of ownership and licensing rights and audit controls. Failure by the collaboration members to implement the necessary governance measures may lead to misappropriation, IP disputes, and other challenges. Similarly, there may be reluctance among enterprise members to contribute, thus, undermining the value of the collaboration.

IV. Adding Risk-Management Frameworks to Compliance Approaches

During the past few years we have seen a shift to increased risk-management frameworks for protection of trade secrets that reinforces and complements the ongoing efforts focused on compliance. Reasonable measures are no longer defined by the mere existence of policies, but by whether those policies effectively help to mitigate many of the risks enterprises face. Cybersecurity is at the forefront of this shift, although as we noted in our earlier Goldilocks article reasonable measures are not equivalent to cybersecurity.

Instead, we are seeing increased use of cybersecurity tools as part of protecting confidential and proprietary information, including trade secrets. Hence, for example, we can expect that most enterprises use encryption, multifactor authentication, and endpoint protection. Reasonable measures may now, however, also imply a broader, more proactive approach that can assist in anticipation and prevention of potential losses of trade secrets. Three such approaches are:

1. **Threat modeling (e.g., STRIDE) to anticipate and pre-empt likely attack vectors;**[12]
2. **Data lifecycle management (e.g., Microsoft Purview,**[13] **data governance, data security, and risk and compliance solutions) to ensure sensitive data is classified, monitored, and properly retired; and**
3. **Human behavior risk mitigation (e.g., SANS Security Awareness Maturity Model)**[14] **to address the reality that employees—not just systems—are often the weakest link in security.**

Of course, the appropriate "reasonable measures" remains tied to an enterprise's technical maturity, governance discipline, and ability to demonstrate active stewardship of its trade secrets protection practices. Nevertheless, the impact of remote work, increased collaborations, cybersecurity, and other factors expands the potential for greater risks. Management at enterprises thus need to treat trade secret protection as a living process; they will then be appropriately positioned to defend their practices in the event of a breach or legal challenge.

V. Possible Risk Management Approaches and Resources

Fortunately, there are easily available resources to assist us in expanding the scope of protections with risk management approaches. The World Intellectual Property Organization (WIPO), which we referenced in our first Goldilocks article as a source of recommendations for protecting trade secrets, has since developed a comprehensive guide worth reading and referencing on a continual basis. The guide discusses the four steps in developing a trade secret protection plan:[15]

- **Step 1: Identify and value your "potential" trade secrets;**
- **Step 2: Determine the risks for your trade secrets;**
- **Step 3: Identify and apply reasonable measures to protect trade secrets; and**
- **Step 4: Monitor and react to misappropriation and leakages.**

This structure mirrors risk management frameworks and reinforces the idea that protection must be proactive, contextual, and continuously maintained.

There are also cybersecurity frameworks that can be of value in your efforts to develop and implement reasonable measures to encompass risk management with compliance. Stressing again that reasonable measures are not equivalent to cybersecurity, but that cybersecurity is relevant in regard to reasonable measures, there is an intersection between WIPO's work with modern cybersecurity frameworks such as NIST and ISO/IEC 27001 which reflects the growing recognition that intellectual property (IP) protection requires both legal safeguards and technical rigor.

WIPO provides guidelines for the legal protection of trade secrets, emphasizing confidentiality, access control, and remedies for misuse. In contrast, cybersecurity frameworks necessitate these principles by specifying how data should be protected in digital environments, through practices such as access management, encryption, monitoring, and response protocols.

12 https://www.jit.io/resources/app-security/stride-threat-model-a-complete-guide.

13 https://learn.microsoft.com/en-us/purview/.

14 https://www.darkreading.com/endpoint-security/managing-human-risk-discoveries-from-sans-2023-security-awareness-report.

15 https://www.wipo.int/web-publications/wipo-guide-to-trade-secrets-and-innovation/en/index.html.

NIST and ISO/IEC 27001 are internationally-respected standards that provide structured approaches to managing cybersecurity risk and information security. While they originate from different organizations, they share core similarities in purpose and structure. Both frameworks emphasize a risk-based approach to security, advocating for the identification, assessment, and mitigation of information security risks. Additionally, both promote the implementation of controls across governance, access management, incident response, and continual improvement.

NIST's five core functions of Identify, Protect, Detect, Respond, and Recover[16] broadly aligns to ISO 27001's Plan-Do-Check-Act (PDCA) cycle.[17] This allows enterprises to use NIST as a flexible practical guide since it does not have a formal certification process while relying on ISO 27001 certification for official assurance.[18]

The following table illustrates how ISO 27001 control areas align with the NIST Cybersecurity Framework, offering a framework for integrating trade secret protection into an enterprise's broader security program:

NIST Functions	ISO 27001 Example Requirements [19]
IDENTIFY	**Clause 4.1** - Understanding the Organization & Context: Identifies internal and external factors affecting security.
PROTECT	**Annex A.9** - Access Control: Role-based access and least privilege principles.
DETECT	**Control 8.15** - Logging Respond.
RESPOND	**Clause 8.2** - Information Security Risk Assessment.
RECOVER	**Annex A.5.29** - Business Continuity Planning: Ensures that organizations can recover from disruptions, including trade secret breaches.

In effect WIPO in combination with cybersecurity frameworks such as NIST and ISO 27001 bridges the compliance and risk management approaches. WIPO helps to define the "what" that must be protected while cybersecurity frameworks address part of the "how" to protect it. Together this what and how provides guidelines for enterprises seeking to develop and implement reasonable measures to protect trade secrets.

The reality is that all enterprises face the fundamental challenge of ensuring robust safeguards to protect trade secrets without stifling collaboration. Excessive access restrictions, rigid data controls, and overly cautious information-sharing policies can create operational friction for enterprises and hurt the core issue of creating stakeholder value. This is especially true for those enterprises that have research and development (R&D) environments, cross-functional teams, and external partnerships where agility and exchanging of information is essential and R&D/innovation centers with third-party enterprises and customers. Our approaches to protect trade secrets can go too far and inhibit the enterprise in addition to frustrating personnel. We fundamentally need to accept some risks to enable innovation and collaboration.

Similarly, many of us have seen enterprises that may often expose aspects of their trade secrets in sales presentations, technical support meetings, and other activities. Yet, such exposures are often inherent in the conduct of day-to-day business and are practically essential for many businesses to function.

The challenge for all of us is further complicated by increasing privacy expectations from employees and regulators. Enterprises must also now navigate between privacy compliance laws (i.e., Canada's Personal Information Protection and Electronic Documents Act[20] and Europe's GDPR[21]) and information security practices to avoid conflicts and ensure lawful practices. Managers at enterprises need to be aware of these privacy compliance laws and adopt their reasonable measures policies accordingly.

One of our major concerns is that some enterprises may go too far and create "security silos" that isolate knowledge or discourage collaboration. In our experience this happens when management effectively equates policies for reasonable measures with cybersecurity.

In fact, management must implement controls proportionate to the sensitivity and value of the trade secrets, while still enabling productive workflows. For

16 https://www.nist.gov/cyberframework/getting-started/online-learning/five-functions.

17 https://gccertification.com/iso-27001-and-the-pdca-cycle-a-roadmap-to-information-security/.

18 https: //www.itgovernanceusa.com/iso27001-and-nist.

19 https://www.isms.online/iso-27001.

20 https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/.

21 https://www.eurofound.europa.eu/en/publications/2020/employee-monitoring-and-surveillance-challenges-digitalisation.

example, the practices that can be implemented for activities like marketing and sales presentations are not likely to be applicable with technical algorithms and software source code because the creation, use, and type of information is so different. This underscores the need for dynamic, scalable approaches without compromising a "reasonable measures" defensibility.

Some of the technology tools we use can also create hurdles and problems while providing important functionality and protections. Consider, for example, how data loss prevention (DLP) solutions, a form of technical control, from companies like Google and Microsoft are positioned as tools to "...protect your most sensitive data."[22] Indeed, DLP solutions can significantly reduce the risk of unauthorized sharing of trade secret information by automatically detecting, flagging, and restricting the movement of sensitive data across email, cloud storage, and collaboration platforms. Enterprises can also use DLP to enforce policies that prevent downloading, forwarding, or externally sharing documents marked as confidential. DLP can also provide audit trails for accountability.

Yet, while DLP technologies can be a beneficial component of a trade secret protection strategy, they are not foolproof. If anything, such solutions may provide a false sense of security and focus. Sophisticated users can easily bypass controls[23] through sanctioned or unsanctioned channels (e.g., screenshots, personal devices), and false positives or misclassifications can lead to blind spots. For instance, Google's DLP solution, while effective in many areas, has notable limitations such as its inability to analyze multimedia files or compressed archives, leaving gaps in protection for certain file formats.[24]

Hence, any tool—whether DLP, encryption, or endpoint protection, should be viewed as one layer in a multi-faceted defense strategy, not a silver bullet. Effective protection requires a combination of technology, process, and people working in concert. These tools should not be treated as a simple compliance checklist, but rather as components of a layered defense to protecting trade secrets.

This reality forces enterprises to confront a foundational trade-off: the more accessible information is for productivity and collaboration, the more difficult it becomes to secure fully that information. On one hand, businesses benefit from collaboration, but each access point increases the potential for leakage, theft, or inadvertent disclosure.

Using technical safeguards such as encryption, role-based access, data loss prevention, and zero-trust architecture are vital, but they come at a cost. These measures can introduce friction into workflows, delay decision-making, or inhibit creative collaboration. Striking the right balance requires continuous risk assessments, stakeholder alignment and a willingness to prioritize resilience over rigidity. Enterprises, moreover, should assess their "right balance" on a periodic basis when business situations change. As with the original Goldilocks fable with the porridge being too hot or too cold, managers are thus confronted with the tradeoff of too much security or too little security.

Keep in mind, too, that even enterprises with mature security postures and significant investments in trade secret protection are not immune to breaches. History has shown that technical controls and legal safeguards can be bypassed, especially by insiders or trusted actors. DuPont, for example, had extensive safeguards in place when an insider stole proprietary information about its Kevlar technology.[25] Similarly, Waymo (a subsidiary of Alphabet) faced trade secret theft when a former engineer downloaded thousands of confidential files before joining a competitor.[26] These cases highlight a crucial point, which is that no technical or legal system is foolproof. Insider threats, lapses in compliance, or sophisticated cyberattacks can bypass even the most advanced controls.

Interestingly, in our work we often find that senior managers at enterprises often equate trade secret theft or IP misappropriation with someone hacking. The label of "hacker" often comes to mind and dominates the conversation because hacking and data losses are in the news and hackers often are the "bad guy" in movies and television programs. However, while external cyber threats remain real and relevant, they are not the cause of most trade secret losses. This is another reason not to equate cybersecurity, where protection against hacking is paramount, with reasonable measures to protect trade secrets.

In reality, the most significant and persistent risks originate within the enterprise or through what was expected to be trusted third-party relationships.

In our experience the following threat actors consistently appear in trade secret litigation and breach investigations:

- **Insiders:** Employees, former employees, contractors, and consultants with legitimate access who misuse it intentionally or negligently;
- **Business Partners and Consortium Members:** Collaboration usually requires information sharing and creates risk exposure;

22 https://cloud.google.com/security/products/dlp.

23 https://timesofindia.indiatimes.com/blogs/voices/how-some-tech-savvy-employees-are-bypassing-data-leakage-prevention-measures/.

24 https://cloud.google.com/sensitive-data-protection/docs/supported-file-types.

25 https://www.justice.gov/archives/opa/pr/kolon-industries-inc-pleads-guilty-conspiring-steal-dupont-trade-secrets-involving-kevlar.

26 https://www.theguardian.com/technology/2017/feb/23/alphabet-sues-uber-self-driving-cars-technology-waymo-otto.

- **Competitors:** Competitors often recruit rival talent or obtain information through corporate espionage; and
- **Suppliers:** Outsourced service providers (e.g., manufacturing, development and marketing) often have access to confidential materials for them to fulfil their duties.

Ultimately, the goal is not to eliminate risk entirely, but to manage it grounded in reality. This means designing security practices that assume breaches are possible and structuring governance, response, and legal strategies around that truth.

It also means shifting the narrative from perfection to preparedness by using layered defenses, building a strong culture of confidentiality, and rapid cross-functionality incident response. It is crucial that when incidents occur the enterprise can respond decisively and demonstrate that it took reasonable, proportionate, and good-faith measures to protect its trade secrets.

VI. Practical Recommendations for a Balanced Approach

Achieving effective trade secret protection today requires a return to the "Goldilocks Principle of not too much, not too little, but just right." Overly aggressive controls can paralyze workflows and alienate teams, while overly permissive controls invite misappropriation and legal exposure. The key is balance, which can be achieved by implementing measures that are appropriate for the value and sensitivity of the trade secrets, the structure of the enterprise, and the external threat environment. Enterprises must actively tailor policies and defenses based on their risk tolerance, industry specific threats, competitive pressures, and regulatory exposure. They cannot simply copy others.

In our experience a layered-security approach provides the most resiliency. Such an approach combines risk management with compliance.

It would include, at a minimum, the following:

1. **Technical controls like encryption, access management and endpoint protection;**
2. **Procedural safeguards such as data classification, information handling policies, training and clear process for onboarding/offboarding; and**
3. **Legal instruments such as NDAs, trade secret acknowledgements and agreements with partners.**

Under this approach each layer compensates for gaps in the others, creating an environment where breaches must overcome multiple barriers. Effective enterprises ensure these layers work in concert where legal counsel, information technology, human resources, and business units are aligned on security objectives and operational impact.

Monitoring the measures taken by industry leaders and competitors also provides valuable guidance. Benchmarking against peers may also help validate an enterprise's efforts and possibly avoid outlier behavior that courts might deem unreasonable in litigation. Adopting industry accepted frameworks such as ISO 27001 certifications, SOC2 audits, or NIST CSF mapping can signal intentional, structured and repeatable steps to safeguard confidential information.

For insights into best practices, licensing management at enterprises may want to look to analyst firms like Gartner, Forrester, and IDC, which regularly publish trends and benchmarks on topics like zero-trust architecture and privileged access management for safeguarding trade secrets. The insights these companies provide may help enterprises to stay aligned with evolving standards and ensure their security position reflects current industry customs and practices. In our experience, regular security training, tabletop exercises, and auditing partner compliance are critical. Building a "need-to-know" culture, assigning clear ownership of trade secrets, and tracking granular access can further fortify defenses. Finally, investing in insider threat detection tools and incident response playbooks ensures preparedness when breaches occur.

The reality is that threat landscapes evolve constantly, driven by advances in attack methods and the sheer scale of interconnected ecosystems. Controls deemed sufficient today may be outdated tomorrow. This volatility makes static security plans inadequate and reinforces the need for ongoing iteration, particularly when an enterprise is participating in collaborations.

We would be remiss not to discuss the implications of AI and, accordingly, provide a cautionary note. Looking ahead, enterprise management should consider future proofing their trade secret protection policies in an era increasingly shaped by AI and machine learning. With the rise of generative AI platforms that are used for coding and data analysis, trade secrets can be unknowingly embedded into AI prompts and training datasets. Enterprises, particularly those that develop, license, support or otherwise work with software as a core portion of their business should establish AI usage policies that prohibit the inclusion of sensitive, confidential, or proprietary information in prompts submitted to publicly available AI models (e.g., ChatGPT and Copilot). They must also evaluate partners and vendors for how they handle AI, ensuring agreements that explicitly address data confidentiality, ownership, and training model restrictions. ■

Building A Sustainable Future:
Understanding Permissible Repair VS Impermissible Reconstruction in Support of a Circular Economy

By

Aaron Massuda
Associate Attorney
Womble Bond Dickinson (US) LLP
aaron.massuda@wbd-us.com

Karthika Perumal
Office Managing Partner - Houston
Womble Bond Dickinson (US) LLP
Karthika.Perumal@wbd-us.com

Shiju Thomas, FCIPS
General Manager
Houston Energy Services Co. W.L.L.
shiju.thomas@hescotek.com

The circular economy invites us to fundamentally reconsider our relationship with resources and products. By moving away from the outdated "take-make-dispose" model, companies are embracing a more sustainable approach that prioritizes longevity, repairability, and eventual recycling. This thoughtful design philosophy creates and preserves value throughout a product's entire lifecycle. Effective management of intellectual property (IP) rights serves as a cornerstone of this forward-thinking vision. Companies that skillfully balance robust IP protection with accessible repair rights position themselves to foster continued innovation while advancing sustainability goals. These businesses develop products with extended useful lifespans that significantly reduce unnecessary waste and conserve valuable resources for future generations.

Businesses stand to gain numerous advantages by embracing repair as part of their product lifecycle. Customers increasingly recognize and reward brands that demonstrate genuine environmental responsibility, building stronger loyalty and trust in the products. Products designed with repair in mind naturally create more resilient supply chains that can better withstand parts shortages or other disruptions. This approach also contributes to vibrant local repair economies, reducing transportation-related environmental impacts while creating jobs and economic opportunities in communities where customers live and work.

The legal landscape governing repair rights varies significantly between regions like the United States (U.S.) and European Union (EU). A clear understanding of these different frameworks empowers businesses to make informed decisions about how customers can legally interact with products after purchase. Here, we highlight significant court decisions, relevant statutes, and practical implications for businesses and consumers, specifically for authorized purchasers of an IP-protected product (Product Owners) and the holder of those same IP rights (IP Holder). This knowledge allows a company to develop strategies that protect their valuable intellectual property while simultaneously supporting broader sustainability objectives. By thoughtfully balancing potential revenue from repair services against the needs and expectations of the customers, a company can position its business for long-term success.

U.S. Legal Framework

The doctrine of patent exhaustion plays a central role in understanding the right to repair. Under this doctrine in U.S. law, once a patented product is sold, the IP Holder's rights over that specific item are exhausted. This means the Product Owner is free to use, repair, or resell the item without infringing the patent. The Supreme Court's ruling in *Impression Products v. Lexmark International* (2017) reaffirmed this principle, rejecting attempts by IP Holders to enforce post-sale restrictions through patent infringement lawsuits. Repair is an affirmative defense to a patent infringement claim; however, where the line between a permissible repair ends and impermissible reconstruction begins is not always clear.

Permissible Repair

Permissible repair in the U.S. refers to actions taken to preserve the utility and operability of an IP-protected product, typically a patented product. This includes replacing individual unpatented parts, one at a time, whether of the same part repeatedly or different parts successively. The Supreme Court's decision in *Aro Mfg. Co. v. Convertible Top Replacement Co.* (1961) along with the *Impression Products* decision both established (and most recently reaffirmed in *Karl Storz v. IMS* (2023)) that such repairs are lawful and do not constitute patent infringement under U.S. law.

Impermissible Reconstruction

Impermissible reconstruction involves actions that effectively create a new article from the IP-protected product or embodiment after it has become spent. Typically, the product is protected by patents and thus, reconstruction generally relates to patent infringement. The key distinction lies in whether the activity amounts to making a new article rather than merely preserving the existing one.

Distinguishing Repairs from Reconstruction

While there is no definitive rule, courts assess multiple factors to determine whether a Product Owner has created a new article, thereby reconstructing the patented product. These factors include:

a) **Extent of Replacement** - Courts look at how much of the patented product has been replaced at one time. If the replacement involves a substantial portion of the product at the same time, it is more likely to be considered reconstruction. However, even if the Product Owner sequentially replaces all the worn-out parts of a patented combination, courts have found this sequential replacement does not constitute reconstruction.

b) **Nature of the Parts Replaced** - Replacing minor, unpatented parts is generally considered repair, while replacing essential, patented components can be seen as reconstruction.

c) **Purpose of the Replacement** - The intent behind the activity is considered. If the replacement is intended to extend the life of the product or restore it to its original condition, it is more likely to be considered repair. However, if the replacement effectively creates a new product, it is more likely to be reconstruction.

A pertinent example provided by the court in the *Karl Storz* case illustrates the application of many of the factors listed above. The court held that if a patent is granted for an automobile, the replacement of a spark plug constitutes permissible repair. Conversely, retaining the spark plug while replacing the entirety of the car in one action is more likely deemed reconstruction.

Right to Repair at the Federal Level

Recent national developments have significantly impacted the landscape of the right to repair in the U.S. Major players such as Apple Inc. have endorsed federal legislation, while the Federal Trade Commission (FTC) has intensified its enforcement against restrictive repair practices.

Apple Inc. has publicly supported federal right-to-repair legislation, marking a significant shift in the company's stance on repairability. On October 24, 2023, Apple announced its backing of a federal right-to-repair bill, committing to provide access to tools and parts for customers nationwide.

The FTC has taken significant steps to combat illegal repair restrictions and restore the right to repair for consumers, small businesses, and government entities. In July 2021, the FTC adopted a policy statement prioritizing investigations into unlawful repair practices under relevant statutes, including the Magnuson-Moss Warranty Act and Section 5 of the FTC Act. Targeting practices that raise repair costs, stifle innovation, and limit business opportunities for independent repair shops, the FTC aims to address antitrust and consumer protection violations.

Right to Repair at the State Level

As of 2025, right-to-repair legislation has been introduced in all 50 states. These bills generally aim to guarantee consumers' rights to access replacement parts, repair manuals, diagnostic data, and appropriate tools necessary for maintenance. States such as New York, Minnesota, Colorado, California, and Oregon have already passed right-to-repair laws, setting a precedent for other states to follow. These laws empower consumers by providing tools and information for self-repair, reducing dependency on manufacturers. They support independent repair shops by ensuring access to parts and tools, fostering competition and innovation.

The most notable example is Oregon's 2024 right-to-repair law, which requires manufacturers to provide parts, tools, and information for repairing consumer electronics. It also bans software that prevents technicians from fully installing spare parts, known as "parts pairing."

EU Legal Framework

In the EU, the principle of exhaustion of IP rights also plays a central role in understanding the right to repair. Once a product has been placed on the market by the IP Holder or with their consent, the exclusive rights to that specific product are typically considered exhausted. This means consumers can use the product as intended, including repairing it. However, there are no specific guidelines that apply uniformly across all EU member states or the UK for distinguishing repair from reconstruction. Article 64(3) of the European Patent Convention (EPC), which also applies to the United Kingdom (UK) despite it not being an EU member, requires national courts to handle disputes about European patents using their own laws. The following is an analysis of the general principles and themes that countries under the EPC apply when differentiating between repair and reconstruction.

Permissible Repair

Permissible repair in the EU involves actions that maintain the functionality of a product without infringing on the patent. The Supreme Court in the UK provided guidance in *Schütz v Werit* (2013), outlining factors to consider when determining whether an activity constitutes repair or reconstruction. These factors include:

a) **Subsidiary Nature of the Replaced Component** - Courts assess whether the replaced component is a relatively minor part of the product. If the component is subsidiary and does not embody the inventive concept of the patent, its replacement is likely considered repair.

a) **Life Expectancy** - The life expectancy of the replaced component compared to other parts of

the product is evaluated. If the component has a significantly shorter lifespan and is expected to be replaced periodically, its replacement is generally deemed repair.

b) **Ease of Replacement** - The physical ease of replacing the component and its practical perishability are considered. Components that are designed to be easily replaceable and are relatively perishable in practice are typically associated with repair.

c) **Inventive Concept** - Whether the replaced component includes any aspect of the inventive concept of the patent is a critical factor. If the component does not embody the inventive concept, its replacement is more likely to be seen as repair.

d) **Independent Identity** - Courts examine whether the replaced part has any independent identity from the product. If the part is integral to the product's identity, its replacement may lean towards reconstruction.

Impermissible Reconstruction

Impermissible reconstruction in the EU is defined similarly to the U.S., where actions that effectively create a new product from the patented entity are considered patent infringement. Key factors held by countries applying the EPC that indicate impermissible reconstruction include:

a) **Extent of Replacement** – Replacing all claimed elements of a patented invention without reusing any parts is likely considered reconstruction. Extensive replacement that transforms the product into a new article falls under reconstruction.

b) **Creation of a New Article** – Activities that result in the creation of a new article from the patented entity are deemed reconstruction. This includes refurbishing a totally worn or spent product to make it operable again.

c) **Impact on Patent Rights** – Reconstruction activities that infringe on the patent rights by creating a new product are impermissible. This includes using patented replacement parts or refurbishment methods without authorization.

Distinguishing Repairs from Reconstruction

Differentiating between permissible repair and impermissible reconstruction requires a careful analysis of the factors outlined above. Courts subject to the EPC assess the nature, extent, and purpose of the activity to determine whether it constitutes repair or reconstruction. The EU's Right to Repair Directive further clarifies these distinctions by mandating that manufacturers provide access to spare parts, repair manuals, and diagnostic tools for certain products.

EU Directive on Promoting Repair

The European Union has introduced a new directive aimed at promoting the repair of goods, amending existing regulations to enhance sustainable consumption and reduce waste. The directive, officially titled "Directive (EU) 2024/1799 of the European Parliament and of the Council on Common Rules Promoting the Repair of Goods," was adopted on June 13, 2024, and entered into force on July 30, 2024. Member States are required to transpose it into national law by July 31, 2026.

Key aspects of the directive include:

a) **Obligation to Repair** – Manufacturers of products subject to reparability requirements in EU law must repair those products within a reasonable time and at a reasonable price. This obligation applies to products listed in Annex II of the directive, which includes items such as refrigerators, smartphones, and washing machines.

b) **Prohibition of Repair Impediments** – Manufacturers are prohibited from using contractual clauses, hardware, or software techniques that impede the repair of goods listed in Annex II, unless justified by legitimate and objective factors.

c) **Access to Spare Parts and Repair Information** – Manufacturers must provide access to spare parts at reasonable prices and make repair information available to consumers in an easily accessible manner. This includes publishing indicative prices for typical repairs on their websites.

d) **Consumer Awareness** – The directive mandates that manufacturers inform consumers about the availability of repair services and spare parts, enhancing transparency and encouraging repair over replacement.

Conclusion

For companies in the repair business, distinguishing between permissible repair and impermissible reconstruction is crucial. In the U.S., the doctrine of patent exhaustion and key court rulings support the rights of product owners to repair their IP-protected products. Similarly, the EU emphasizes the principle of exhaustion of IP rights, allowing consumers to repair products as intended. However, companies must ensure their repair activities do not cross into reconstruction, which could lead to legal challenges.

Recent legislation in both regions supports consumer rights and independent repair shops, offering significant opportunities for growth. Federal and state laws in the U.S., along with the EU's directive promoting repair, aim to empower consumers and support independent repair shops by ensuring access to necessary parts, tools, and information.

Finding this equilibrium between IP protection and repair accessibility enables a company to flourish in the emerging circular economy while making a meaningful contribution to environmental sustainability. ■

Legal Horizons in Smart City Innovation

By

David J. Kappos
Partner
Cravath, Swaine & Moore
New York, NY
dkappos@cravath.com

Vincent Joralemon
Associate
Cravath, Swaine & Moore
New York, NY
vjoralemon@cravath.com

Smart cities are no longer a futuristic concept—they are a present-day reality. From Barcelona's energy-efficient lighting to Singapore's adaptive traffic systems, urban centers worldwide are integrating technology to enhance efficiency, sustainability and public services. They are providing early signs that connecting urban systems (e.g., transportation, utilities, public safety, etc.) yields a synergy in which the whole is greater than the sum of its parts.

However, these advancements bring complex legal and governance challenges that require careful navigation. As a cautionary tale, one need only look to Toronto's Quayside project.[1] Started in 2017, the Quayside project aimed to create a technologically advanced neighborhood. Despite its ambitious vision and ample funding, the city abandoned the project in less than three years due to public backlash over privacy concerns and data governance. The lesson: even the most innovative, well-resourced initiatives can fail without transparency, accountability and public trust—foundational pillars of any sustainable smart city governance framework.

Regulators are responding. Laws like the EU's General Data Protection Regulation (GDPR), Singapore's Personal Data Protection Act (PDPA), and California's Consumer Privacy Act (CCPA) require that cities obtain user consent for data collection, limit how data is processed and shared, and conduct Data Protection Impact Assessments (DPIAs). These requirements introduce real friction into smart city models, which often depend on continuous and ambient data collection. The legal challenge is to reconcile innovation with privacy-by-design principles, ethical risk assessments and compliance across multiple jurisdictions.

Finally, there is the issue of IP ownership and control. Smart city initiatives frequently involve a mix of public agencies and private vendors. That raises fundamental legal questions: Who owns the underlying data? Who controls the algorithms and the software driving core infrastructure? Without clear contractual terms, cities risk vendor lock-in—becoming dependent on a single vendor for products or services and losing the freedom to switch to another vendor without incurring substantial cost and disruption. In response, we're seeing new licensing strategies and a growing emphasis on open standards and public-private IP sharing models to help cities maintain meaningful control over their digital infrastructure.

Taken together, these challenges suggest a broader truth: smart cities are not just technology projects—they are legal and governance projects as well. In this article, we will explore each of these themes—from privacy to interoperability, blockchain to AI—and offer a legal framework for guiding smart city innovation. The foundational tensions—between innovation and governance, public interest and private control—carry through every layer of smart city development. When legal frameworks evolve alongside technological innovation, smart cities can realize compounding benefits—where connected systems enhance each other's performance in ways no single solution could achieve alone, while also creating clearer, more cohesive pathways for effective regulation.

I. Data Sharing and Interoperability

Data is the fuel of smart cities—from traffic sensors to utility grids, every system generates and relies on real-time information. And much of the data includes some amount of personal information—names, addresses, identification numbers, etc. While the implementing technology solutions promote integration and optimization, legal frameworks often thwart or even prevent it. Regulations like the EU's GDPR, Singapore's PDPA, and California's CCPA impose tight restrictions on how personal data can be processed and shared—particularly across borders.

For example, the Schrems II decision by the Court of Justice of the European Union invalidated the Privacy Shield framework and raised significant uncertainty

1 See Karrie Jacobs, *Toronto Wants to Kill the Smart City Forever,* MIT TECH. REV. (June 29, 2022), https://www.technologyreview.com/2022/06/29/1054005/toronto-kill-the-smart-city.

about EU-U.S. data transfers.[2] Now, cities working with international vendors or cloud providers must navigate multiple overlapping legal regimes, each with distinct definitions of personal data, consent requirements and transfer mechanisms. To stay compliant, cities routinely conduct privacy impact assessments and adopt technical and legal safeguards—such as pseudonymization, data minimization or Standard Contractual Clauses (SCCs). These SCCs are under regular scrutiny and revision by regulators, meaning cities must continuously monitor updates to ensure ongoing compliance.

Beyond cross-border data restrictions, a second major friction point is interoperability. Cities rely on a matrix of sensors, software and platforms—often from different vendors. Without common standards or open APIs, data becomes siloed. Initiatives like Open & Agile Smart Cities (OASC)[3] promote interoperability by defining Minimal Interoperability Mechanisms (MIMs) that allow systems to communicate regardless of vendor. At the same time, interoperability raises important legal questions—most notably, who owns or has rights to the software interfaces and the underlying data schemas? Licensing models must ensure that open APIs and shared standards do not inadvertently expose proprietary technology or restrict downstream reuse. Efforts to standardize communications across platforms—such as the adoption of ISO/IEC 30141[4] and oneM2M[5] protocols—represent important progress toward technological harmonization. Yet without corresponding legal clarity around access, ownership and licensing, these initiatives risk falling short of their full potential.

As cities strive to integrate diverse technologies, clarity over data ownership and licensing becomes essential to ensure systems can work and grow together. City-collected data may be subject to IP protections—like copyright, confidentiality restrictions or *sui generis* database rights—especially when private contractors are involved. Licensing frameworks are evolving to strike a balance: enabling cities to reuse or share data for the public good while preserving proprietary rights for vendors. Legal agreements must clearly define the scope of permitted use, whether data is subject to open licenses (e.g., Creative Commons),[6] and how derivative works are treated. Absent these terms, cities risk either overstepping IP boundaries or losing access to data they helped generate. This is especially important for emerging models like data trusts and public data commons, where multiple stakeholders contribute and govern shared urban datasets. Clear terms governing access, modification, attribution and redistribution are essential to support these collaborative data ecosystems. As cities generate and integrate data broadly, the legal considerations described above—privacy, interoperability and ownership—form the foundation on which smarter, more trusted infrastructure must be built.

II. Distributed Ledger Technologies: Identity, Payments and Smart Contracts

Smart cities thrive on seamless data flows—but these raise serious legal and technical challenges around privacy, IP and control. Distributed ledger technologies offer one possible solution: decentralized tools for managing identity, payments and trust across systems. Distributed ledger technology—particularly blockchain—is emerging as a foundational infrastructure layer for smart cities.

One high-impact use case is digital identity. Instead of relying on centralized ID databases vulnerable to breaches, blockchain enables decentralized credentials that are owned and managed by individuals and verified through cryptographic proofs. A citizen could, for example, prove residency without disclosing additional personal data. But this architecture introduces legal complexity. Blockchains are by design immutable, while privacy laws (e.g., GDPR) require mechanisms to delete or correct personal data. To address this, smart identity systems typically store sensitive data off-chain and record only hashed or tokenized references on-chain, enabling compliance without compromising data integrity. Zug, Switzerland, for example, has implemented uPort, a blockchain-based identity platform on the Ethereum network, allowing residents to access e-government services and vote securely.[7] More advanced approaches use tools like zero-knowledge proofs (ZKPs), which allow individuals to prove that a specific claim (such as a document's authenticity) is true without revealing any unnecessary personal information. Buenos Aires, for instance, has integrated ZKPs into its miBA platform, enabling citizens to verify credentials such as residency or age without revealing other personal information.[8]

2 Case C-311/18, *Data Prot. Comm'r v. Facebook Ireland Ltd. & Maximillian Schrems*, 2020 EU:C:2020:559 (July 16, 2020).

3 Open & Agile Smart Cities, https://oascities.org/.

4 ISO/IEC 30141:2024, Internet of Things (IoT) — Reference Architecture, Int'l Org. for Standardization & Int'l Electrotechnical Comm'n 2024, https://www.iso.org/standard/88800.html.

5 One Machine-to-Machine Partnership Project (oneM2M), European Telecommunications Standards Institute, https://www.etsi.org/committee/1419-onem2m.

6 Creative Commons, https://creativecommons.org/.

7 Lester Coleman, *Zug Citizens Begin Digital ID Registration on an Ethereum Blockchain*, CCN (Mar. 4, 2021), https://www.ccn.com/uport-self-sovereign-identity-opens-to-residents-of-zug/.

8 Tom Carreras, *Buenos Aires Adds ZK Proofs to City App in Bid to Boost Residents' Privacy*, YAHOO! FINANCE (Oct. 22, 2024), https://finance.yahoo.com/news/buenos-aires-adds-zk-proofs-130000431.html.

Blockchain also supports novel payment and incentive models. Some cities are experimenting with token-based systems for public transit, recycling rewards or local sustainability programs. For example, residents might earn digital tokens for reducing energy consumption, which can then be redeemed for municipal credits or services. These systems promote community engagement and resource efficiency, but raise compliance challenges. Legally, cities must determine whether such tokens constitute regulated financial instruments—and structure agreements with vendors to address licensing, custody, tax treatment and usage restrictions. Depending on how they are structured, tokens may implicate securities regulations or trigger obligations under know-your-customer, anti-money laundering, consumer protection and tax laws. Cities often turn to financial sandbox programs or pursue tailored regulatory exemptions to responsibly deploy token-based tools.

These token systems, and many other smart city applications, are increasingly governed by smart contracts—self-executing code on a blockchain that performs functions automatically when predefined conditions are met. For instance, a contract could trigger payment once a sensor confirms that a public service, like waste collection, has been completed. These tools can streamline workflows and reduce administrative overhead, but also raise legal issues: Are smart contracts enforceable? Who bears liability if the code contains an error?

Some U.S. jurisdictions, including Arizona and Tennessee, have passed laws recognizing smart contracts as legally valid under electronic records statutes. However, broader legal consensus is still developing. To mitigate risk, cities typically require code audits before deployment, human override capabilities and clear documentation outlining the contract's terms and intent.

In addition to automation, blockchain offers an important governance benefit: tamper-proof audit trails. These immutable records can log events such as access to surveillance footage or modifications to infrastructure systems—providing cities with legally reliable records that support public records retention obligations, regulatory audits and accountability mandates.

Yet even as blockchain promises auditability and transparency, many smart city systems are now turning to AI for real-time analysis, prediction and decision-making. These tools offer enormous efficiencies—but also raise critical legal questions about accountability, fairness and intellectual property.

III.
AI in Smart Cities: Legal Guardrails and IP Challenges

Artificial intelligence is increasingly the cognitive engine behind smart city operations—optimizing traffic flows, predicting energy demand and even automating public permitting. But as AI systems take on more civic functions, legal and ethical risks intensify.

Algorithmic bias is a major concern. Tools like facial recognition and predictive policing have been shown to disproportionately impact marginalized populations. The EU's new AI Act addresses this by classifying many public sector AI systems as "high-risk." These systems will require built-in safeguards: transparency, risk assessments, human oversight and accountability mechanisms. Public agencies must be able to explain algorithmic decisions and provide individuals with the ability to contest or override them.

However, transparency requirements create legal tension. Public agencies are increasingly expected to explain decisions made using AI—but many vendors claim the models they use are trade secrets. This conflict between explainability and intellectual property protection is a growing friction point in public procurement and algorithmic accountability. Legal frameworks are still evolving to balance these interests, with some jurisdictions requiring disclosure of key decision logic while protecting proprietary aspects of the model. But the tension plays out in procurement contracts and public disclosure obligations: cities must negotiate terms that allow for meaningful auditability without violating vendor IP protections. Licensing agreements are evolving to include tailored disclosure rights, audit clauses or escrowed algorithms to strike this balance.

An early example of civic AI innovation is Boston's "Street Bump" initiative.[9] The city launched a mobile app that used smartphone accelerometers to detect potholes as residents drove, automatically transmitting this data to public works departments to improve road maintenance. While the project aimed to improve service delivery through citizen input, it also revealed key smart city risks. The data disproportionately reflected activity in neighborhoods where residents had smartphones and downloaded the app—creating blind spots in lower-income or less-connected communities. This illustrates a critical point: even well-intentioned innovation can exacerbate structural inequities if not

9 Justin Reich, *Street Bumps, Big Data, and Education Inequality,* EDUCATION WEEK (Mar. 1, 2013), https://www.edweek.org/education/opinion-street-bumps-big-data-and-educational-inequality/2013/03.

carefully designed and managed. Legal frameworks for smart city AI must incorporate not only privacy and transparency requirements, but also equity-by-design principles to ensure that benefits—and burdens—are distributed fairly.

AI also introduces legal complexity around ownership and intellectual property. Cities may use AI to generate reports, designs or predictive models—but who owns those outputs? In most jurisdictions, AI-generated content is not eligible for copyright or patent protection unless there is meaningful human authorship. For example, U.S. courts and the Copyright Office have held that AI-created works without human input are not protectable, and AI systems cannot be named inventors under patent law.

This makes contracts essential. Cities working with AI vendors need clear terms allocating rights in AI outputs, defining licensing requirements and setting limits on reuse. Moreover, the data used to train municipal AI systems may itself be protected by copyright, trade secret or database rights—making proper sourcing and licensing vital to avoid infringement.

Privacy is another core concern. AI systems often process large volumes of personal data, raising legal obligations under laws like the GDPR. Article 22 of the GDPR, for example, grants individuals the right not to be subject to decisions based solely on automated processing—such as AI systems operating without meaningful human involvement—that result in legal or similarly significant effects.[10] A city using AI to issue parking tickets or determine eligibility for public benefits may need to ensure that meaningful human review is available and documented.

More broadly, privacy-by-design requires cities to limit the collection and use of personal data, adopt anonymization where feasible, and secure AI systems against re-identification (where anonymized individuals are re-identified by linking datasets), inference attacks (where adversaries deduce sensitive attributes from seemingly innocuous data) or data poisoning (where malicious data corrupts AI training sets). Ethical frameworks like Singapore's Model AI Governance Framework offer practical principles—such as transparency, fairness and accountability—that cities can adopt to guide responsible deployment and maintain public trust.[11]

A further risk is the vulnerability of AI models to cyber threats. Smart city AI systems are increasingly targeted by model poisoning (where training data is manipulated to degrade model performance) and adversarial attacks (where inputs are subtly altered to cause misclassification or system failure). These risks demand not only technical defenses—like robust validation, adversarial training and monitoring—but also legal safeguards around liability, response obligations and public disclosure in the event of system compromise.

The AI-related challenges discussed above reveal a broader truth: as cities rely more heavily on algorithmic systems, legal frameworks must evolve not just to manage risk, but to shape outcomes in the public interest. Meeting this moment requires governance models that incorporate accountability, equity and transparency into their design. With clear rules around ownership, oversight, privacy and resilience, cities can ensure that AI builds public trust and drives both efficiency and inclusion.

IV. Conclusion: Ensuring Smart Legal Foundations for Smart Cities

As cities evolve into smart urban ecosystems, legal frameworks must adapt to address the complex and overlapping challenges that accompany technological advancement. Effective data governance is essential to ensure that policies around collection, usage and sharing protect privacy and meet regulatory requirements. Interoperability is equally critical, requiring the adoption of open standards that allow diverse technologies and systems to integrate with one another. Public-private partnerships must be structured to balance innovation with the public interest, enabling cities to retain meaningful control over the infrastructure developed with private collaborators. Finally, the deployment of artificial intelligence must be guided by ethical safeguards that prevent bias, promote transparency and establish clear lines of accountability. By proactively confronting these legal dimensions, cities can unlock the full potential of smart technologies—enhancing urban living while safeguarding the rights and well-being of their residents.

When built on sound legal foundations, smart cities do not just get smarter—they become more responsive, resilient and equitable. The opportunity is not merely to optimize infrastructure, but to reimagine urban life in ways that serve everyone. ■

10 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), art. 22, 2016 O.J. (L 119) 1.

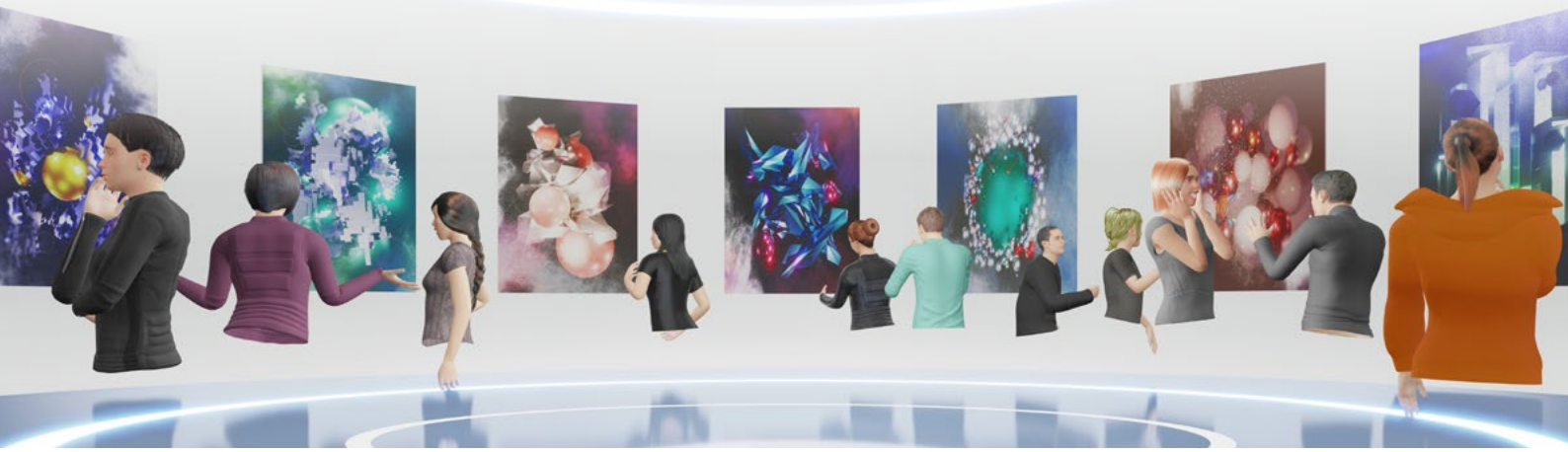
11 Personal Data Protection Commission, *Model Artificial Intelligence Governance Framework* (2d ed. 2020), https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/AI/SGModelAIGovFramework2.pdf.

Metaverse or Marketplace Trap?

How First Sale and Exhaustion Are Being Left Behind

By

Ananya Malhotra
5th year Law Student
Christ Deemed to be University
Bangalore, India
ananyamalhotra274@gmail.com



Introduction

No longer a fantasy of science fiction, the Metaverse is an increasingly fast-growing virtual world in which individuals live, trade, and produce via virtual avatars. The Metaverse has also established a lucrative marketplace for virtual goods, from non-fungible token (NFT)-hooded clothes to virtual real estate. However, a pressing question comes along with more customers paying real currency for these virtual goods: Do they actually own what they purchase?

In the real world, such laws as first sale and exhaustion give consumers power by restricting control that the owners of intellectual property (IP) retain once they sell their products. IP rights are not offended if you give away a video game, resell a book, or distribute a branded product. But those same legal safeguards somehow have a tendency to vanish when we are talking about the Metaverse. The customers may not be able to resell, donate, or even use their purchases in their entirety because most virtual goods are subject to license agreements and not ownership.

This article talks about how conventional IP norms are difficult to enforce in online environments, particularly when ownership and access are obscured by tech platforms and NFTs. The need to rethink and possibly re-envision how we establish ownership in the virtual world grows as digital markets expand and the gap between law and technology widens.

I. What is Metaverse and Why it Matters for IP Law?

Metaverse can be understood as a massive, interactive virtual world where people can chat, play, shop, and create using avatars and virtual personas. Think of it as the next level above the internet, where individuals interact with each other and their environments in real time, often through virtual or augmented reality, as opposed to scrolling on screens. Early examples include platforms like Decentraland, Roblox, Fortnite, and Meta's Horizon Worlds, which provide virtual products like digital artwork, virtual real estate, clothes (for avatars), and even experiences like concerts.[1]

These virtual commodities may first seem exactly like physical commodities: you might buy a virtual shirt, skin, or piece of land. Here's where it becomes complicated, as the Metaverse concept of property is extremely different from the physical world. If you buy an actual commodity, you usually end up with ownership of that specific commodity and can give or sell. Alternatively, you often only gain a permission to utilize a virtual object with particular limitations from the platform upon acquisition. That suggests that you own few rights and that the IP owner or the platform might subject your use and transfer of the digital product to limitations.

1 Kevin Roose, "What Is the Metaverse, and Why Does It Matter?," *N.Y. Times* (Jan. 18, 2022).

Intellectual property (IP) legislation becomes crucial in this situation. Virtual commodities are more than just lines of code; they are frequently covered by trademarks, copyrights, and occasionally even patents.[2] Even after a sale, the creators or owners of the rights maintain control over how these assets are used. For instance, you only have restricted usage rights when you buy a designer skin for a game; you are not granted the freedom to copy, alter, or sell it.

Due to the unclear application of existing intellectual property doctrines such as exhaustion (which restricts rights after a sale) and first sale (which permits resale), the Metaverse poses new legal issues.[3] Knowledge of how IP rights operate in this field is crucial for creators and platforms, and for the millions of consumers and companies betting on the future of virtual worlds, as digital economies expand and individuals spend considerable amounts of real money on virtual goods.

II. Understanding Exhaustion and First Sale: How IP Rights Work in the Real World

We first need to consider how intellectual property (IP) rights work in the actual physical world, that is, under the principles of exhaustion and first sale, to understand why ownership in the Metaverse is so complicated.

The first sale doctrine tells us that once a copyright owner sells or transfers a legally created copy of a work, the owner loses his control over what the buyer will do with the copy. What this means is that you do not need to ask permission from the copyright owners to resell, lend, give away, or even dispose of your copy of a book, CD, or DVD. Just like patents and trademarks, the concept of exhaustion ensures that the rights owner cannot limit further use or distribution after the initial authorized sale.[4]

When you purchase a printed novel from a bookstore, for instance, you are the owner of the physical copy, which you can give to a library, sell on eBay, or lend to a friend. A lawfully purchased video game disc or a branded handbag can also be sold again because the IP owner's ownership over that particular item is deemed “exhausted” following the initial sale.[5]

To counterbalance the rights of creators and consumers, these theories are necessary. Otherwise, producers or right owners would retain full authority over all products, banning libraries, second hand stores, resale markets, and even private lending. Essentially, first sale and exhaustion protect consumer sovereignty, promote market competition, and enable fair use.

But since copies are simple to create and purchases occasionally involve limited licensing agreements instead of outright ownership, these doctrines, which were established for physical items, are tricky to apply tidily in the digital realm. In the Metaverse, this tension is acutely felt.

III. What is the Difference Between Virtual and Real Ownership?

In the Metaverse, purchasing a virtual skin, NFT artwork, or even virtual land entails that what you actually obtain is, at best, a limited license. Depending upon the rules of the platform where the purchase is made, you would actually only be allowed to use the item and not buy it as per the defined guidelines.

One important difference is that, unlike a tangible book or purse, you do not own the digital file. Unless specifically permitted by the platform or rights holder, you are not permitted to freely resell, lend, alter, or distribute these digital works.[6] The nature of intellectual property law explains why businesses usually keep all underlying rights.

The nature of intellectual property law is that, since digital goods are so easily copied, firms generally hold all underlying rights and merely license[7] limited use to consumers. This setup also explains why doctrines like first sale or exhaustion usually do not apply in the Metaverse. Under U.S. law, the first sale doctrine applies only when there is a lawful sale or transfer of ownership, not when there is merely a license. So, even if you’ve paid real money for a virtual asset, you typically cannot invoke these protections because you were never the legal owner—you were just a licensee.

It has a significant impact on consumers. It means that if a platform shuts down, your account gets suspended, or the terms of service get updated, you may no longer be able to use it. Virtual goods are usually neither resalable nor giftable, which leads to a closed system in which companies still have control despite "selling" digital products. Fundamental questions about consumer rights during the digital age are raised by this difference between virtual and actual possession.

2 U.S. Copyright Office, Copyright and the Metaverse (2023).

3 Aaron Perzanowski & Jason Schultz, "The End of Ownership: Personal Property in the Digital Economy" (2016).

4 *Kirtsaeng v. John Wiley & Sons, Inc.,* 568 U.S. 519 (2013).

5 *Impression Prods., Inc. v. Lexmark Int’l, Inc.,* 581 U.S. 152 (2017).

6 Aaron Perzanowski & Jason Schultz, 'The End of Ownership: Personal Property in the Digital Economy" (2016).

7 U.S. Copyright Office, Copyright and the Metaverse (2023).

IV.
The Role of NFTs and Big Platforms: Ownership or Illusion?

In contemporary society, NFTs tend to capture people's attention as assets "owned" by users on the blockchain, where music, art, or even virtual estates are definitively distinct and owned. However, NFTs do not legally grant full ownership of the content they contain.[8] Instead, you receive a unique token that verifies your ownership of a specific digital file but does not grant copyright or reproduction rights to the artwork.

For example, when purchasing NFT art, you become entitled to that specific token, but the artist still legally retains copyright. Therefore, you cannot freely sell or duplicate copies of the artwork without consent. Similarly, Roblox, Fortnite, and Meta's Horizon Worlds enforce copyright laws and heavily regulate virtual items purchased by users within their world.[9] Even though you spend real currency on those purchased assets, your usage of it becomes limited access to those assets governed by terms of service you have no choice but to abide by—basically making it a gated 'walled garden.'

Moreover, such terms and conditions often grant the platform ample discretion to delete assets, suspend accounts, or terminate grants of access at will. This means that your rights are as secure as the rules of the platform allow, which, in the case of an NFT or a valuable object within a game, makes them rather precarious.

In summary, the Metaverse's promise of digital ownership is often more myth than reality. Users remain dependent in the absence of meaningful legal rights or platform compatibility. Although blockchain technology and NFTs are often promoted as instruments of user empowerment, the effective control over digital assets is often in the hands of centralized platforms that can modify, limit, or even withdraw access. Further, the absence of standardized procedure and cross-platform interoperability leaves users with little of what they actually "own" in one virtual space being considered as valuable in another. Without effective legal frameworks and true decentralization, the fiction of digital ownership stands to turn into mere marketing fiction.

V.
What Should Change? Rethinking IP Rights for the Future

Legal frameworks have yet to develop an intellectually reasonable solution to the Metaverse, NFTs, or any other digital assets in contrast with physical property. Users intending to purchase virtual items today find themselves bound by stringent licensing deals that sit at odds with their purchase, essentially meaning they do not actually own whatever virtual item they 'purchased.'

Some scholars claim that a theory of a 'digital fatigue' should be dealt with in order to resolve the gaps in the system. Allowing users to exercise dominion over assets freely, the digital exhaustion principle gives authority for unrestricted resale, lending, and transfer of recourses that had been securely acquired and should be legislatively protected.

Implementing the theory is more challenging than one would think. From a business perspective, assets that are inherently deemed digital disqualify the item from resale due to the unlimited capacity for replication. On the flip side, consumers perceive modern licensing restrictions as stifling and consider themselves trapped in proprietary systems designed by dominant technology firms.

In addition to digital fatigue, potential reforms might include tougher consumer protection regulations to avoid abrupt loss of access to acquired goods or interoperability standards to allow users to transfer assets between platforms. By balancing the interests of creators and users, these adjustments may promote innovation and guarantee equitable treatment. In the end, legal systems around the world need to reconsider outdated frameworks to reflect the reality of digital life, where ownership ought to signify more than just a license.

In addition, the courts and legislators need to address the uncertainty of the legal status of virtual assets, especially regarding creating definitive property rights. As opposed to physical goods, virtual goods tend to reside in enclosed ecosystems where ultimate control is maintained by the platform providers with users having scant recourse if a problem arises. A redefinition of property in the digital space—maybe through statutory recognition of ownership of digital assets as with tangible property rights—would assist in anchoring user entitlements. Such a transformation would require harmonization across jurisdictions to support the inherently borderless nature of digital interactions and commerce so that digital ownership is meaningful and enforceable globally. ■

8 Primavera De Filippi, "Blockchain Technology and Smart Contracts," 21 *Harv. J.L. & Tech.* 1, 18–19, 2018.

9 U.S. Copyright Office, Copyright and NFTs.

'Pay or Okay' Model, Part II: Personalized Advertisements - Competition, Consumer Protection and Unfair Competition Law Concerns

By

Pınar Bakırtaş
Intellectual Property Rights Researcher
4IPcouncil
pinarbakirtas.1998@gmail.com

The views expressed in this article are those of the author and do not necessarily represent the views of 4IP Council.

I. Introduction

In November 2023, Meta introduced a subscription policy for processing data for personalized advertisements in the EU, the European Economic Area and Switzerland. Accordingly, the options offered by Meta, known as the 'pay or okay' model, has (i) a paid version (monthly €9.99 on web or €12.99 on mobile applications) of Meta services with no ads, guaranteeing that users' personal data is not processed for advertising purposes; or (ii) a free of charge version, which requires users to "consent" to the processing of their personal data for advertising purposes.

Part I of this paper addressed concerns raised by Meta's 'pay or okay' model regarding personal data protection laws. This second part will examine concerns surrounding Meta's 'pay or okay' policy focusing on potential abuse of Meta's dominant position and its compliance with the Digital Markets Act (DMA). Additionally, it will explain the arguments raised against Meta's new policy under consumer and unfair competition laws. The considerations in these areas are crucial both independently and in connection with data protection rules.

II. Abuse of Dominant Position

In the EU, Art 102 TFEU (Treaty on the Functioning of the European Union) regulates the unilateral anticompetitive acts of companies, prohibiting the ones in dominant position within a market from abusing their position.[1] Determining an abuse of dominant position requires (i) a dominant position, (ii) an abusive behaviour and (iii) an effect on trade between Member States.[2] The last element is generally not a point of contention, as it is generally applicable. For the purpose of this paper, the third element will not be analysed, as the 'pay or okay' model has already been introduced across the whole European Economic Area.

A. Dominant Position

Initially, an indication of a dominant position can be inferred from regulatory tools. Facebook and Instagram, both belonging to Meta, have been designated by the European Commission (EC) as very large online platforms[3] under the Digital Services Act (DSA)[4] and as gatekeepers[5] under the Digital Markets Act.[6]

Furthermore, whether Meta holds a dominant position has been investigated by different authorities such as the European Commission,[7] the German Federal Cartel Office (German FCO)[8] and the U.S. Federal Trade Commission (FTC),[9] all of them deciding that Meta holds a dominant position in the relevant market. Their analysis will be considered regarding the market share and definitions as well as what constitutes a barrier to entry in the relevant market.

1 Simon Vande Walle, 'Exploitative Abuses in EU, German and French Competition Law' *SSRN Electronic Journal 1.*

2 Gabriel Peric, 'EU Competition Law and Abuse of Dominance A Deep Dive into Article 102 of the TFEU' (Örebro Universitet 2022) https://www.diva-portal.org/smash/get/diva2:1691421/FULLTEXT01.pdf.

3 'Digital Services Act: Commission Designates First Set of Very Large Online Platforms and Search Engines' (*European Comission,* 2023) https://ec.europa.eu/commission/presscorner/detail/en/ip_23_2413.

4 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) OJ L 277.

5 'Digital Markets Act: Commission Designates Six Gatekeepers' (*European Comission,* 2023) https://ec.europa.eu/commission/presscorner/detail/en/ip_23_4328.

6 Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) OJ L 265.

7 Facebook Marketplace (Case AT.40684) Comission provisional decision [2024] https://ec.europa.eu/competition/antitrust/cases1/202513AT_40684_10582539_13405_4.pdf.

8 Bundeskartellamt (Case B6-22/16) Facebook, Exploitative Business Terms Pursuant to Section 19(1) GWB for Inadequate Data Processing, 6 February 2019; Case Summary: https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.pdf.

9 *FTC v Facebook Inc.* (Case No.: 1:20-cv-03590) U.S. District Court of Columbia, 9 December 2020 https://www.ftc.gov/system/files/documents/cases/051_2021.01.21_revised_partially_redacted_complaint.pdf.

1. Market Share and Definition

The German FCO decided that Facebook holds a dominant position in the German market for "private social network market with private users." In the EU, market share of 50 percent or above could be indicative of dominant position in the market.[10] The German competition authority found that Facebook's 95 percent market share for daily active users in this market is a crucial element for assessing lawful competition. In reaching that conclusion, the German FCO clarified that Instagram, WhatsApp, Snapchat, YouTube, Twitter, LinkedIn and Xing were excluded from its analysis of the market of social networks because they were considered to only "offer parts of the services of a social network." Thus, the German FCO did not consider them as genuine competitors. It further specified that even if those services were included in the FCO's analysis, Facebook's market share would be significantly beyond the threshold of a dominant position.

Its U.S. counterpart, the FTC, concluded that Facebook holds a market share above 60% for the U.S. "personal social networking" market. As with the German FCO, the FTC similarly excluded WhatsApp, LinkedIn, YouTube and Netflix from its assessment of the market of personal social networking services. At the same time, the FTC indicated that the company viewed its true competitors to be platforms offering features that differ from those of Facebook, rather than platforms offering copycat features. This perspective can be seen through Facebook's acquisition of Instagram and WhatsApp, two platforms that offer distinctly different features compared to Facebook.

The EC, on the other hand, considered the relevant market as "personal social networking services." When making its analysis it has considered "the broader market for personal social networking services including hybrid social media platforms." The hybrid platforms contain differing features from personal social networking services and are used for different purposes. Still, they contain essential features of a personal social networking service, and therefore are considered all together. The mentioned hybrid platforms in the decision are Instagram, Snapchat and TikTok. According to the provisional decision of the EC, Meta holds a high market share sufficient to establish its dominant position in the market for personal social networking services, including hybrid social media platforms.[11] In concluding so, the Commission rejected Meta's analysis of a market for user's time and attention (including YouTube, LinkedIn, X, Vimeo, Reddit, Pinterest, etc.), stating that such a market does not exist.

It seems that various competition authorities and market players define the market for Meta's services differently. Also, it is important to note that the 'social' connection element that is indicated by all authorities within these online services is diminishing in its importance. This is due to the rise of content being curated by artificial intelligence (AI) analysis rather than just users' 'social' interactions.[12] In the Q1 2023 earnings call of Meta, AI recommended content was indicated as 20 percent,[13] whereas by the Q1 2024 earnings call it had already risen to 30 percent.[14] Strikingly for Instagram, it noted that -as a first- more than 50 percent of the content people see are recommended by AI.[15] As a result, the existing market definition of personal social network services by the competition authorities might be becoming less relevant by the day.

2. Barriers to Market Entry

The German FCO noted that the network effects of Facebook are another critical determinant for determining its market dominance. According to the Office, these effects caused competitors such as Google+ to lose market share, and ultimately leave the market. The EC's provisional decision supports this view. It also mentions the attempt to introduce competing services by other firms have also failed and none were able to establish significant market presence.[16] Another important factor stated by both authorities is indirect network effects. These effects are those created by different groups utilizing the network for the purpose of exchanging value; in this case, users and advertisers. The larger the user database of a platform, the more advertisers it can attract. Such indirect network effects make it harder for ad-funded platforms to enter the market. This is because they must enter both the social network user market and the online advertising market.[17]

The U.S. FTC similarly emphasised the significance of network effects as "high barriers to entry." Additionally, the decision of the FTC revealed some interesting insights discovered from Facebook's internal documents. These documents confirm that it is difficult to attract users away from a leading social networking service due to its established social structure, meaning the way users are interacting within the platform such as liking and sharing photos or comments.[18]

Unlike the German FCO and the Commission, the FTC indicated that challenging the dominant

10 Guidelines on the assessment of horizontal mergers under the Council Regulation on the control of concentrations between undertakings OJ C 031.

11 The Commission, Facebook Marketplace 107-111.

12 'The End of the Social Network' [2024] *The Economist* https://www.economist.com/leaders/2024/02/01/the-end-of-the-social-network.

13 META Q1 2023 Earnings Call Transcript, p.2 https://s21.q4cdn.com/399680738/files/doc_financials/2023/q1/META-Q1-2023-Earnings-Call-Transcript.pdf.

14 META Q1 2024 Earnings Call Transcript, p.3 https://s21.q4cdn.com/399680738/files/doc_financials/2024/q1/META-Q1-2024-Earnings-Call-Transcript.pdf.

15 Ibid.

16 The Commission, Facebook Marketplace 111-118.

17 Bundeskartellamt, Facebook 6-7; The Commission, Facebook Marketplace 111-118.

18 U.S. FTC, *FTC v Facebook Inc.* para 6.

position of social networking services is still possible even if solid network effects exist. It mentioned that this could especially be the case during "periods of technological or social transition." For example, TikTok saw a significant rise in users in 2020 during the Covid pandemic and continues to grow rapidly. It successfully entered the social media market and it has even disrupted giants like Instagram and Facebook. Since TikTok's entry, both platforms have transformed the basis of their feed content curation from chronological to algorithmic methodology.[19] Therefore, even though network effects might hinder market entry, when the market is let free, user demand may lead to new entries. Today, some users have novel demands such as the need for smaller online social communities, platforms with niche purposes,[20] and privacy considerations.[21] These novel needs are not compatible with the current architecture of existing social media platforms. Therefore, despite the barriers created by network effects, new competitors could still be encouraged to enter the market.

Another key barrier to market entry, as highlighted by the European Commission, is the data-driven nature of personal and hybrid social networking platforms. These services rely heavily on large volumes of user data and advanced data processing capabilities. Facebook's unmatched access to vast amounts of data, including from third-party sources, gives it a major competitive advantage that is really hard to match by new entrants.[22]

Overall, the competition authorities' findings of Meta and Facebook's large market share, together with the resulting network effects seem to be essential in determining the existence of a dominant position.

B. Abusive Behaviour

The abusive conducts under Art 102 TFEU could be categorized under exclusionary and exploitative abuses. Exclusionary abuses result in a harm in competition by excluding (potential) competitors. Whereas exploitative abuses refer to anticompetitive acts of the dominant company by directly harming its trading partners, either suppliers or customers.[23] The paid option in 'pay or okay' strategies could be assessed for exploitative abuse due to potential excessive pricing, under Article 102(a) of the TFEU.[24] Abuse depends on whether Meta exploits its consumers with excessive fees. According to the CJEU's *Meta* decision, the competition authorities could assess compliance with the General Data Protection Regulation (GDPR)[25] if it is required for determining the abuse of dominant position.[26] However, traditionally this type of exploitative conduct has not been a high enforcement priority within the abuse of dominance investigations of the EC. Likewise, the only guidelines on Art 102 TFEU from the EC simply focuses on exclusionary abuses.[27]

According to the CJEU's leading decision in *United Brands*, there is no specific way to determine exploitative pricing abuses. Still, the case introduces a two-step cumulative test: The initial stage involves determining whether the price is excessive and it considers an analysis of the dominant firms selling price compared to its cost. If it is considered to be excessive, next is an assessment regarding whether the price is unfairly excessive. This is determined by evaluating whether (i) it is unfair in itself or (ii) when compared to the prices of competitive products.[28]

In later cases, the CJEU updated its jurisprudence that the test to determine whether the price is excessive does not have to be a price-cost analysis and other methods, *e.g.*, price comparison with competitive products, could also be used.[29] The excessiveness test and determining whether Meta's fee is itself unfair requires a very detailed economic analysis, which will be left for the competition authorities to conduct. When it comes to a price comparison with competitive products, it is hard to find a comparative product in the same market offering a similar policy. This is because the market for personal social networking services is defined narrowly by competition authorities.

It is important to note that, in a competitive market economy, prices are expected to vary. Therefore, Facebook and Instagram's fees do not need to be the exact same as those charged by its competitors. According to the CJEU, for such price differences to be considered abusive, there should be an "appreciable" difference, as clarified in the *Latvian Copyright Society* case. There is no specific threshold capable of determining if the difference is "appreciably higher."

19 Kate Lindsay, 'TechScape: TikTok took over social media with its uncanny algorithm – but at what cost?' *The Guardian* (London, 12 September 2023) https://www.theguardian.com/technology/2023/sep/12/techscape-tiktok-algorithm-social-media-war-facebook-instagram-youtube. accessed 27 July 2025.

20 Brian X Chen, 'The Future of Social Media Is a Lot Less Social' *The New York Times* (19 April 2023) https://www.nytimes.com/2023/04/19/technology/personaltech/tiktok-twitter-facebook-social.html accessed 27 July 2025.

21 Exploding Topics, 'The Future of Social Media (2025-2027)' (Exploding Topics, 2 years ago) https://explodingtopics.com/blog/future-of-social-media accessed 27 July 2025.

22 The Commission, Facebook Marketplace 111-118.

23 Walle (n 2) 4.

24 Consolidated Version of the Treaty on the Functioning of the European Union, 26.10.2012, C 326/47.

25 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L 119.

26 CJEU Case C-252/21 *Meta Platforms Inc and Others v Bundeskartellamt* [2023] ECLI:EU:C:2023:537.

27 Communication from the Commission — Guidance on the Commission's enforcement priorities in applying Article 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings [2009].

28 CJEU Case 27/76 *United Brands Company and United Brands Continental BV v Commission of the European Communities. Chiquita Bananas* [1978] ECLI:EU:C:1978:22 para 252.

29 CJEU Case C-177/16 (Latvian copyright Society) *Autortiesību un komunicēšanās konsultāciju aģentūra/Latvijas Autoru apvienība v Konkurences padome* [2017] ECLI:EU:C:2017:689 para 37.

Rather, according to the Court, the difference will be deemed appreciable "if it is both significant and persistent on the facts to the market in question."[30]

Even if excessive pricing is not a very often imposed abuse under EU competition law, the subscription policy of Meta for €12.99 (on mobile applications) could be examined as an exploitative abuse. Although a detailed economic analysis would be carried out by the competition authorities, it is noteworthy that the price applies only to an ad-free service, while user tracking for other purposes would still continue.[31] At the same time, it is not enough that the price is simply higher than those of competitive services but there must be an "appreciably higher" difference.

III. The Digital Markets Act (DMA)

The DMA is introduced to enhance competition and fairness in digital markets by regulating the behaviour of large online platforms designated as gatekeepers. It aims to ensure that these platforms act fairly and allow for market contestability according to clearly defined criteria. Meta has been designated as a gatekeeper by the European Commission, which also issued the first decision (23 April 2025) finding non-compliance with the DMA, imposing a fine of €200 million on Meta. The decision finds Meta's 'pay or okay' model in breach of Art 5(2) of the DMA.[32]

Unlike traditional competition law which is an *ex post* intervention to anti-competitive acts, the DMA provides *ex ante* regulation to large online platforms on how they are allowed to operate in the EU.[33] In that regard, the DMA considers accumulation and aggregation of data across services for advertising forms a competition advantage, posing a barrier to entry.[34] Accordingly, Art 5(2) of the DMA prohibits the gatekeepers from combining and cross-using personal data on their services with data gathered through third parties or other services of the gatekeeper. This is unless the users are given a specific choice and consent to those acts. With the explicit reference of the provision, it is understood that such consent must be GDPR compliant.[35] Most importantly according to the GDPR, consent must be freely given.[36] The DMA provides a mechanism to ensure that consent is freely given: Where the user refuses consent to the combination of its personal data, it should offer "a less personalised but equivalent alternative." Also, using the core platform service or its functionalities should not be dependent on that consent.[37]

Meta's 'pay or okay' subscription policy gave users the choice to either pay for a non-personalized ad-free service (without any processing of personal data) or consent to processing their personal data, including its combination, for personalized advertising. When users refuse to consent and pay for a subscription, they would have to bear the combination of their personal data for personalized advertising. They were not given a choice to opt for a less personalized but equivalent alternative, therefore the EC considered Meta in breach of the DMA. This was not considered a freely given choice.[38] It could be observed that the rationale of the DMA considered by the Commission and the opinion of the European Data Protection Board (EDPB) on consent and pay models (17 April 2024) are in parallel when it comes to requiring the services to offer a less personalized option.[39] Similarly, the EDPB indicated that there should exist an alternative which is free of charge and contains less or no processing of personal data.[40] The alignment of principles and rules across different regulatory devices significantly enhances the effectiveness and consistency of enforcement.

The DMA also indicates that the equivalent alternative should not be different or of inferior quality of service unless that would be directly caused by not being able to process personal data as in Art 5(2) of the DMA.[41] Here, the gatekeeper is expected to prove the direct link between the rejection of consent to processing data as in Art 5(2) of the DMA and the degraded quality in service.[42] What would be considered different or inferior is not certain at this point. In November 2024, Meta announced a change in its subscription policy in Europe where the free version of its services will contain the option to opt for less personalized ads. The EC or the EDPB have not commented on this new approach yet. However, Meta mentioned that the less personalized version will include unskippable ad breaks.[43] It might be argued that this disrupts the quality of the service. At the same time, it has probably emerged as a solution to recoup profits lost from not being able to process

30 CJEU *Latvian Copyright Society* paras 52-55.

31 Alessia D'Amico and others, 'Meta's Pay-or-Okay Model An Analysis under EU Data Protection, Consumer and Competition Law' [2024] *Technology and Regulation* 266-267.

32 European Commission, 'Commission Implementing Decision of 24 April 2024 pursuant Article 5(2) of the DMA (Case DMA.100055 – Meta)' C(2025) 2091 final; 'Commission Finds Apple and Meta in Breach of the Digital Markets Act' (European Comission, 2025) https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1085.

33 'Digital Markets Act Briefing' (European Parliament, 2022) https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)690589.

34 Recital 36 of the DMA.

35 See Part I of the article for a deeper analysis of valid consent under the GDPR.

36 Art 4(11) of the GDPR; Recital 37 of the DMA makes explicit reference to the other features of consent such as being specific, informed and unambiguous as structured in the GDPR. The recital also indicates the fact that rejecting consent should not be harder than giving consent.

37 Recital 36 of the DMA.

38 'Commission Finds Apple and Meta in Breach of the Digital Markets Act' (n 25).

39 'Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms-Adopted on 17 April 2024' (European Data Protection Board, 2024) https://www.edpb.europa.eu/system/files/2024-04/edpb_opinion_202408_consentorpay_en.pdf.

40 *Ibid.*

41 Recital 37 of the DMA.

42 Alessia D'Amico (n 32) 270.

43 'Facebook and Instagram to Offer Subscription for No Ads in Europe' https://about.fb.com/news/2024/11/facebook-and-instagram-to-offer-subscription-for-no-ads-in-europe/ accessed 30 July 2025.

personalized ads. Whether such technical constraint deriving from financial concerns would be acceptable as "a direct consequence of the gatekeeper not being able to process such personal data"[44] is yet to be seen. In fact, the DMA recognises that compliance with some of its obligations, including the ones under Art 5, could affect the economic viability of gatekeepers.[45] In that regard, only under "exceptional circumstances beyond the gatekeeper's control," the Commission could decide to suspend that obligation, in whole or in part, upon request. The EC must state the extent and duration of the suspension.[46] Here, the economic sustainability of the gatekeeper is not considered *ex ante*, but only upon the implementation of the obligation.[47] Other than under exceptional circumstances, the gatekeeper's economic viability is not a concern under the DMA. According to the Commission's decision, gatekeepers cannot demand the preservation of their pre-DMA profits as a prerequisite for regulatory compliance.[48]

As the paid option is not considered an equivalent alternative, the appropriateness of the fee charged is not analysed by the EC. The fact that the fee has not been examined under the DMA by the Commission does not exclude the possibility of its investigation under Article 102 TFEU or other EU legislation. Nevertheless, it is worth noting that the preventive obligations imposed by the DMA may offer a swifter regulatory response. While it might seem like the case-by-case analysis provided by Art 102 of the TFEU is a more flexible approach, for the current case an analysis of the excessiveness of the fee as in Art 102 of the TFEU could have been a more intrusive regulatory instrument. The DMA also provides a framework for addressing fairness in the digital services market, with due consideration to the unique features of these services (in this case the barriers of entry resulting from the accumulation of personal data). In addition, their consistency with GDPR consent principles underscores a strategically coordinated approach to digital regulation within the EU.[49]

IV. Consumer Protection and Unfair Commercial Practices

The 'pay or okay' policy has also been a concern of the European Consumer Organization (BEUC), an association comprising 45 consumer organisations from 31 countries. Its aim is safeguarding the concerns of consumers. In November 2023, the BEUC filed a complaint about Meta's 'pay or okay' scheme before the Consumer Protection Authorities (CPC).[50] The CPC is a network formed by the EU to address consumer protection issues. Through this network, issues or complaints are dealt by relevant national authorities in a coordinated fashion. The BEUC claims that Meta's 'pay or okay' model involves unfair commercial practices which violate European consumer laws in several ways.

They claim:

a) It is an aggressive practice to block access to Facebook and Instagram until users have made a choice between paying or consenting. The sense of urgency and persistence forces consumers to choose an option they may not be willing to make in normal circumstances.

b) It is probable that many consumers think the paid option of Meta's services is privacy-safe. However, Meta might still be collecting and processing personal data for purposes other than advertising.

c) The information provided by Meta is misleading and incomplete as it presents the 'okay' option as free whereas consumers are actually paying with their personal data.

d) Consumers do not have a real choice here. Meta has substantial market power and strong network effects where consumers would not want to lose their connections formed over time. The resulting high fees for the privacy safe paid option discourages users from withdrawing consent to personalized advertisements. Hence, consumers are not offered a genuine choice.[51]

While the first claim relates to aggressive practice as in Art 8 of the Unfair Commercial Practices Directive (UCPD),[52] the next two refer to a misleading action as enshrined under Art 6 of the UCPD, whereas the last claim is relevant to a breach of the GDPR. In both instances under the UCPD, the directive requires that the commercial practice has caused or is likely to cause the consumer to take a transactional decision they would not have taken otherwise.[53] The consumer within the directive is considered as an average consumer who is reasonably well-informed

44 Recital 36 of the DMA.

45 Art 9(1) of the DMA.

46 *Ibid.*

47 Mikolaj Barczentewicz, 'The EU's DMA Enforcement Against Meta Reveals a Dangerous Regulatory Philosophy' (20 June 2025) https://truthonthemarket.com/2025/06/20/the-eus-dma-enforcement-against-meta-reveals-a-dangerous-regulatory-philosophy/ accessed 30 July 2025.

48 The Commission, Meta para 154.

49 Malte Frank and Emma Lewis, 'The European Commission's Challenge to Consent or Pay-Demystifying The Digital Markets Act?' (2024) 47 World Competition 427 www.ycombinator.com/blog/content/files/2024/06/RemedyFest-Final-Report.pdf.

50 'Consumer Groups File Complaint against Meta's Unfair Pay-or-Consent Model' (BEUC Press Releases, 2023) https://www.beuc.eu/press-releases/consumer-groups-file-complaint-against-metas-unfair-pay-or-consent-model#:~:text=Meta is breaching EU consumer,incomplete information in the process.

51 *Ibid.*

52 Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive') OJ L149/22.

53 Art 6 and 8 of the UCPD.

and observant.[54]

Aggressive practices impair or are likely to impair the consumer's freedom of choice. It could be committed by harassment, coercion or undue influence.[55] Undue influence is indicated as exploiting a position of power. It does so by applying pressure that significantly restricts the consumer's capacity to make an informed choice.[56] This should be in a way to make the consumer feel uncomfortable as well as to cause confusion in relation to the transaction decision.[57] Pay or okay may be referred to as an aggressive action because of the fact that the notification of the new policy has disrupted or blocked access to the service itself. This could be regarded as an undue influence considering the user dependency to access the platform (*e.g.*, for social or commercial reasons) and no prior knowledge was provided regarding the new policy.[58] As the consumer's screen was locked until they made a choice, this urgency would lead them to make a "forced subscription."[59] These could make the consumer uncomfortable and confuse them to consent to the processing and combination of their personal data, therefore impairing their free will to make a choice.

Regarding misleading actions as in the UCPD, the directive requires there to be factual information and for this information either to be (i) false or (ii) likely to deceive the consumer even if the information is correct. In this case, the subscription presented as ad-free may deceive the consumer that there would be no tracking and profiling activities in the platform. In reality, Meta still pursues tracking for different purposes such as to improve Meta's products, for analytics and for personalizing user's experience other than with ads.[60] However, an average consumer that is well informed and observant may be expected to know that an ad-free platform does not equate to a completely tracking-free service. In addition, the fact that consumers are told they will continue to use the services for free is contested. First, because the "free" may give the impression users give nothing in exchange whereas they actually provide their personal data. This argument may be a bit far-fetched compared to the rest. Second, because this is not simply continuing to use the platforms for free. Actually, Meta was forced to change its policy because it has been processing personal data with invalid legal grounds under the GDPR.[61]

In addition, European consumer laws require an informed and fair choice. Free and informed consent is also a prerequisite as a legal basis for processing personal data under Art 4(11) of the GDPR. Therefore, the BEUC's assessment asserts that the violation of GDPR should be considered as an unfair and illegal practice under consumer protection law as well.[62]

V. Conclusion

While data protection rights seem to set the primary focus on the 'pay or okay' debate for personalized ads, competition and consumer protection laws also warrant significant discussions. As has been discussed the conflicts in these fields also interact with data protection laws.

The main conditions for abuse of dominant position include both the dominant position of the platform and an abuse of competitively concerning activities regarding personalized ads. It is challenging to establish the dominant position of a firm in the personal social media services market, particularly concerning market definition and share. Network effects are considered as the main barrier to market entry by competition authorities in this particular case. The abuse of a social media platform for processing and combining personal data for advertising under a 'pay or okay' policy may be scrutinized within excessive pricing as in the TFEU. To date excessive pricing has not been imposed much by the European Commission to determine an abuse under the TFEU and it requires deep economic analysis.

The adoption of the DMA has provided specific constraints to large platforms called gatekeepers in order to provide contestability and fairness in the market. Under the regulation, combination and cross-use of personal data is contingent upon user's consent. The DMA lays down the conditions for the validity of consent including it being compliant with the GDPR. The Commission decided that Meta's 'pay or okay' model did not comply with its obligations under the DMA for valid consent. Meta had already updated its 'pay or okay' policy before the decision of the EC. As of today, the conformity of the revised policy with the DMA has not yet been subject to formal scrutiny.

The consumer and unfair competition law claims add substance to the discussion on the user's rights perspective. Consumer organizations claim that 'pay or okay' is an aggressive and misleading practice that does not provide a genuine choice to consumers. ■

54 Recital 18 of the UCPD.

55 Art 8 of the UCPD.

56 Art 2 of the UCPD.

57 Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market OJ C 526/1.

58 Alessia D'Amico (n 31) 264.

59 BEUC, An assessment of Meta's new paid-subscription model from a consumer law perspective (2023) 8.

60 BEUC Assessment 6.

61 BEUC Assessment 6-7.

62 BEUC Assessment 9; Natasha Lomas, 'European Consumer Groups Band Together to Fight Meta's Self-Serving Ad-Free Sub -- Branding It "unfair" and "Illegal"' (*TechCrunch*, 2023) https://techcrunch.com/2023/11/29/beuc-cpc-meta-complaint/ accessed 30 July 2025.

Rethinking Trade Secret Valuation in an AI-Transformed World

By

Josh Beilock
Member of CONSOR® IP Experts
La Jolla, California
jbeilock@consor.com

Weston Anson
Chairman of CONSOR® IP Experts
La Jolla, California
wanson@consor.com

A trade secret, in its most fundamental form, is information that is not publicly known, has economic value due to its secrecy, and is actively protected by its owner. Recent advances in artificial intelligence (AI) are fundamentally altering the way organizations generate, capture, and protect competitive value such as trade secrets. At a base level, companies are rapidly adopting AI-powered systems across critical business functions, from customer engagement to supply chain management.

While automation of select processes reduces operational costs and enhances agility, contemporary research shows the true promise of AI lies in driving deeper transformation—enabling new business models, personalized services, and innovative product channels. For instance, a 2024 report from the Boston Consulting Group titled *Where's The Value In AI?*[1] claims that "(t)he common narrative for AI involves support functions—HR, IT, legal, and the like—where automating relatively low-level and repetitive functions creates significant value. But the companies that are generating the most value are not only deploying productivity plays in support functions but also focusing on reshaping their core business processes and inventing new revenue streams."

However, integrating AI into core business operations carries significant trade-offs. As AI becomes increasingly widespread and easier to replicate, even the strongest competitive advantages—regardless of the measures taken to protect them—are subject to a heightened risk of erosion over time. This article examines how the rise of AI is fundamentally changing the value and protection of trade secrets in the modern economy. It explores how risks to trade secrets such as the tightening of the innovation cycle, erosion of information asymmetry, and reverse engineering, while indeed present before the age of AI, have been dramatically accelerated in recent times. It also compares regulatory trends in the EU and U.S., highlighting how both strict and lax data transparency policies may have negative effects on the values of trade secrets.

Emerging Threats to Trade Secret Advantages

While threats to the protection of trade secrets have always existed, the rapid adoption of AI has led to an exponential increase in three traditional threats to trade secret value: tightening of the innovation cycle, erosion of information asymmetry, and reverse engineering.

Trade secrets have historically derived much of their value from the length of time a company could maintain a competitive edge over rivals. However, with the assistance of AI, innovation cycles are shortening—meaning proprietary methods that once provided years of exclusivity may now become outdated, obsolete, or widely replicated in a fraction of the time. This new dynamic forces organizations to innovate continuously, as even highly guarded information can quickly lose relevance. The end result is a negative feedback loop where companies will be forced to spend more on research and development but will likely realize less value from those innovations.

1 https://www.bcg.com/publications/2024/wheres-value-in-ai.

Another pillar of trade secret value is information asymmetry, which represents the gap between what a company knows and what outsiders do not. AI-driven technologies have the ability to examine vast amounts of data to the point where the differential in knowledge shrinks. The result is a steadily eroding protective moat that consistently puts pressure on trade secret values.

Finally, reverse engineering has long represented one of the main threats to trade secret value primarily because independent discovery of a trade secret has no legal recourse—the cat is simply out of the bag and the value of the trade secret essentially becomes zero. The use of AI supercharges this threat. Automated tools powered by AI can deconstruct software, analyze system behaviors, and examine datasets much faster and more thoroughly than manual methods. In fact, it is likely that many AI models in their current form are already capable of reverse-engineering even the most closely-guarded trade secrets and are simply waiting for a user to ask the right set of questions.

These dynamics are not merely theoretical. In the financial sector, for example, the rise of AI-powered trading platforms has made once highly-guarded trading algorithms much easier to approximate and replicate by competitors, severely compressing the window of exclusive advantage. Similarly, in the pharmaceutical industry, confidential AI-driven drug discovery methods are quickly matched or surpassed by rivals leveraging AI innovations, rendering the original trade secrets obsolete.

This new landscape forces a strategic reassessment: when does it make sense to continue relying on trade secret status, and when should other intellectual property protections, like patents or copyrights, be considered? If the feasibility of independent AI-assisted discovery is too great, the financial justification for secrecy may vanish.

Additionally, as conversations shift toward ethical and societal responsibilities surrounding AI, government action is intensifying, especially around transparency and non-discrimination. This presents new dilemmas: to what extent must transparency into algorithm design, data use, or model performance be allowed before it undermines secrecy? When regulators and consumers demand more openness, how do businesses shield proprietary techniques that underpin their market position?

Transparency, AI, and Trade Secret Regulation

Preserving the value of trade secrets in an AI world certainly faces threats on an economic and technological front. However, the biggest battles over the fate of trade secret values may be political in nature. The meteoric rise of AI use has caused growing scrutiny by lawmakers concerning decision-making processes, data privacy, and potential biases.

The European Union has enacted a robust and sweeping regulatory agenda for artificial intelligence, most notably the 2024 EU AI Act. This legislation imposes broad requirements for transparency. Furthermore, developers must present detailed accounts of their sourcing, training data, and algorithmic logic. Specifically, the law mandates sufficiently detailed summaries of the datasets and methodologies used to train AI models.

While these provisions aim to foster accountability and prevent harm, they present practical challenges for companies managing trade secrets. Even though the EU AI Act attempts to safeguard proprietary information through confidentiality clauses, the realities of regulatory compliance can push companies to expose, intentionally or otherwise, information that ultimately erodes their competitiveness.

Across the pond, the regulatory environment is less uniform and more decentralized. The U.S. continues to rely on a patchwork of state-level measures alongside slow-moving federal developments. Notable state-led approaches, such as Colorado's SB24-205, demand transparency and fairness in automated decision-making, aiming to ensure consumer protection and prevent discrimination. These policies, while less prescriptive than Europe's, still push firms in certain jurisdictions to reveal otherwise confidential data about algorithm operations.

At the federal level, proposed bills like the Generative AI Copyright Disclosure Act of 2024 signal a federal government increasingly interested in AI transparency, at least in the context of copyright protection. Should such bills pass, organizations developing generative models may be required to describe the nature of their training datasets, a duty that could overlap uncomfortably with trade secret preservation.

Importantly, multinational companies face double exposure: they must comply with the strictest elements of both regimes, often requiring them to segment their operations, alter disclosure policies, or localize technology strategies. This increases operational overhead and complicates global intellectual property management, potentially diluting the value of proprietary information simply due to regulatory friction.

Although the EU and U.S. approaches to AI regulation differ, it appears as though the value generated from trade secret preservation will decrease in both environments. For example, the intentional or unintentional divulgence of trade secrets may occur in a heightened regulatory environment fixated

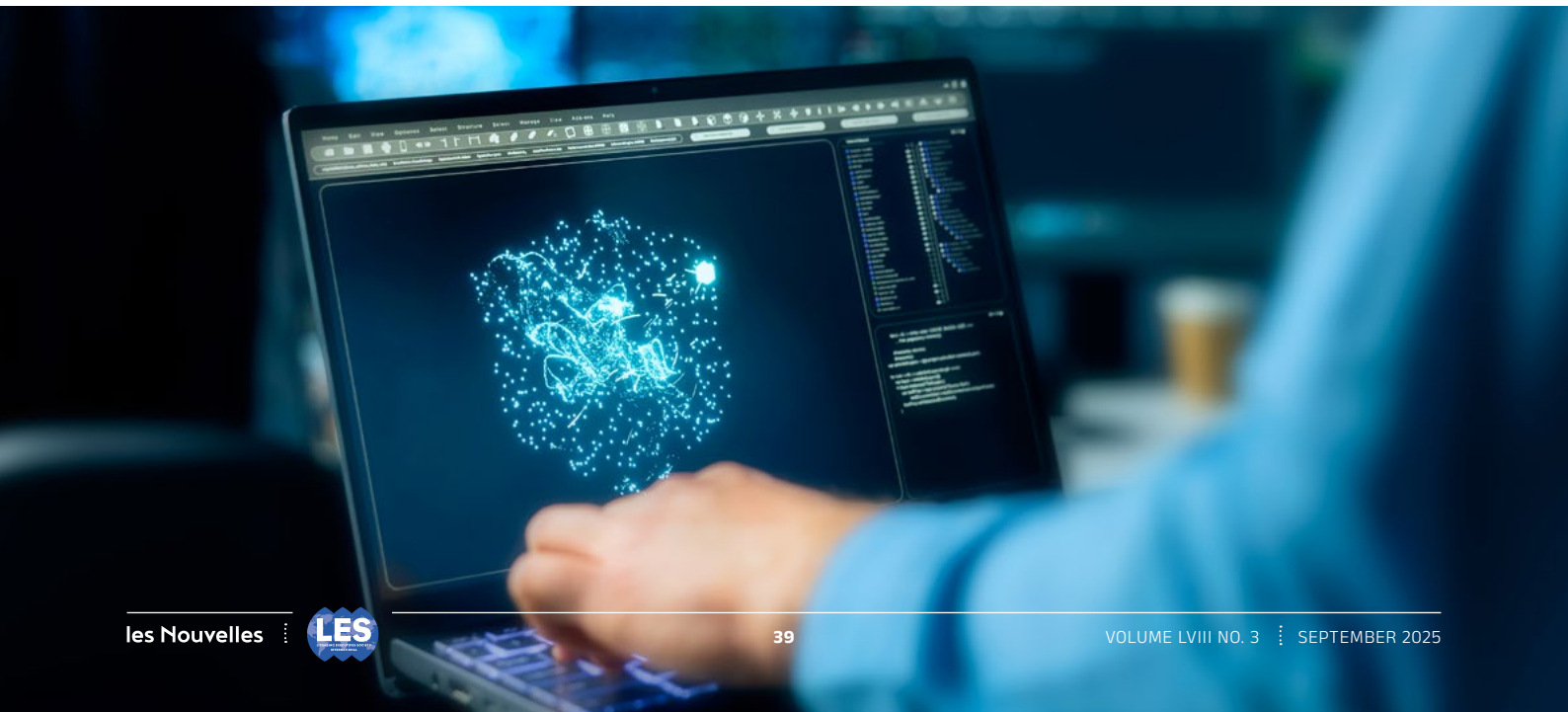
on data transparency and openness. However, in a less regulated environment where AI models have unfettered access to virtually unlimited amounts of data, the value of trade secrets will decrease due to heightened risks of tightening of the innovation cycle, erosion of information asymmetry, and reverse-engineering.

The Road Ahead

To summarize, the EU's emphasis on comprehensive transparency decreases the durability and profitability of keeping methods, datasets, or processes secret. Companies may find that compliance requirements force broad disclosure, potentially leading to rapid competitive leveling. Conversely, U.S. firms may retain secrecy for longer, but the lack of regulatory predictability from state to state complicates long-term strategic planning and risk management. In the end, it may not matter which regulatory environment prevails as both present increased risks for the protection of trade secrets.

As AI reshapes not just markets, but the very rules of economic competition, the strategy of how to manage trade secrets must adapt. In an environment where regulatory transparency is no longer just a theoretical possibility but a requirement, companies that fail to understand or prepare for these realities risk losing their edge entirely, either through forced disclosure or competitive leapfrogging enabled by new AI capabilities.

To remain competitive, organizations should actively audit their trade secret portfolios, conduct regulatory risk assessments, and evaluate when to pursue alternative intellectual property protection such as patents or copyrights, especially for AI-driven innovations. Proactive monitoring of regulatory changes is essential, as laws and enforcement priorities will be in constant flux at the state, national, and international levels. ■



Data Protection and Privacy Conundrum in the Digital World

By

Vikrant Rana
Managing Partner
S.S. Rana & Co.
New Delhi, India
legalresearch@ssra.in

Shilpi Saurav Sharan
Managing Associate
S.S. Rana & Co.
New Delhi, India
legalresearch@ssra.in

ABSTRACT

This paper analyses the complexities surrounding use of unprecedented technology which has led to a major upheaval in the lives of individuals as well as the working of organizations and corporations. In this article we specifically emphasize on the aspect of threat to data protection in view of training of AI on publicly available data as well as the technique of web scraping/data scraping, which has led to data protection issues. In the article, we illustrate cases that substantiate the disrupting impact of AI on data protection on a global scale. We have also delved into the regulatory landscape that governs data protection in India and substantiated case studies that aid in contouring the data protection law prevailing in India.

Introduction

The advent of unprecedented technological advancements and the augmented tendency to hinge on AI tools has exacerbated the legal complexities surrounding data protection and privacy issues on the world panorama. According to the latest reports and statistics, approximately 5.64 billion people around the world are using the internet, which is equivalent to almost 68% of the world's total population.[1] This deep penetration of internet and connectivity in the remotest nook and cranny of the world has, apart from offering profound benefits to mankind, opened the Pandora's box when it comes to disruption of rights, especially data protection and privacy rights on the global stage.

This rapid digitization and upsurge of AI has led to a cynosure of debates on the vulnerability of data protection and privacy rights, which has caused an upheaval not only across industries but also disrupted in countless ways the privacy rights of an individual.

1 https://datareportal.com/global-digital-overview.

The Digital World and the Threat to Data Protection

While technology and technological advancements have been outpouring since the 20th century, it has transformed the way data is being collected, processed, and shared, thereby posing significant challenges to data protection and privacy rights. One major impact recognized by experts on the subject is the sheer volume of data generated by individuals through their online activities, social media interactions, and connected devices.[2] Melanie Mitchell, an American computer scientist, in her book *Artificial Intelligence- A guide for Thinking Humans,* remarks that deep learning[3] by AI requires Big Data and all this data comes from billions of images, text, videos or speech that internet users have uploaded.

AI Training on Publicly Available Data - A Threat to Data Protection

Chatbots have become an integral part of our lives. Whether to book tickets for a trip or ask questions, we bank on Chatbots in our daily lives. However, these Apps collect excessive data, including sensitive data such as biometrics, financial details, government issued IDs and engage in behavioural tracking through chat recordings, etc.[4]

In February 2025, Italy's data protection authority, Garante, blocked Chinese AI model "DeepSeek" on the grounds of lack of information on its use of

2 *The Stanford Encyclopedia of Philosophy, Information Technology and Privacy,* Stanford University, November 20, 2014, https://plato.stanford.edu/entries/it-privacy/, and Frischmann, Brett M., and Evan Selinger. *Re-Engineering Humanity: Automation and the Future of Work.* The MIT Press, 2020.

3 Deep learning uses multilayered neural networks to simulate the complex decision-making power of the human brain.

4 https://ssrana.in/articles/privacy-concerns-in-ai-chatbots-a-comparative-analysis/.

personal data. Italy's Data Protection Authority had questioned DeepSeek on the collection of personal data including its sources, purposes, legal basis and whether the data was stored in China.[5]

This whole matter brought into question potential violations of the OECD Privacy Principles,[6] related to Collection Limitation, Purpose Specification, Openness and Use Limitation. Additionally, other countries including Taiwan, South Korea, the U.S. and Australia have also banned the chatbot.[7]

Similar AI applications, like ChatGPT, Gemini, Copilot and Kimi AI also pose significant data threats, and it is imperative to examine the privacy policies of these chatbots in terms of the kind of data that is being collected, whether they are sensitive personal data, biometric data, financial and transactional data, activity tracking, behavioural data, etc. Reference can be made to the prevailing privacy policies of various chatbots in Table 1.

5 https://www.reuters.com/technology/artificial-intelligence/italys-privacy-watchdog-blocks-chinese-ai-app-deepseek-2025-01-30/.

6 https://www.oecd.org/en/topics/sub-issues/privacy-principles.html.

7 https://www.aljazeera.com/news/2025/2/17/south-korea-removes-deepseek-from-app-stores-pending-privacy-review.

TABLE 1 – Published Chatbot Privacy Policies

CATEGORY	ChatGPT [8] (Parent Company – Open AI)	Gemini [9] (Parent Company – Alphabet Inc.)	DeepSeek [10] (Parent Company - High-Flyer , Quant and Alibaba Group)	Kimi AI [11] (Parent Company – Moonshot AI)
Sensitive Personal Information (PI)	Does not explicitly collect sensitive PI.	Collects highly sensitive PI.	Collects proof of identity or age when the user contacts support.	Collects Phone number information, public information such as avatar, nickname, etc.
Financial and Transactional Data	Collects payment card details and transaction history.	Extensive financial data collection, including bank account details.	No explicit mention of financial data collection.	No explicit mention of financial data collection.
Biometric Data	No biometric data collection.	Collects scan of face geometry for identity verification.	No Biometric data collection.	No Biometric data collection.
Storage of PI	The policy does not explicitly provide where it would store such data.	PI is stored and processed in any country where they have operations.	Policy provides that PI may be stored in servers located outside the country a user lives in.	The policy does not explicitly provide where it would store such data.
Consent	It provides that users can opt out of content provided by them to train modules.	It says that if a user is using the services of Gemini, a user is henceforth giving his consent.	Explicit user consent before data usage for training.	Consent is the lawful basis for processing personal data. (taken from moonshot AI privacy policy.
Data Retention	It retains PI as long as needed in order to provide service or other legitimate business purposes.	Retains PI as long as is reasonably necessary to provide services or legitimate business.	Retains PI as long as necessary to provide services.	Data retained until deleted or upon a deletion request. (taken from Moonshot AI privacy policy).

8 https://openai.com/policies/row-privacy-policy/.

9 https://www.gemini.com/legal/privacy-policy.

10 https://chat.deepseek.com/downloads/DeepSeek%20Privacy%20Policy.html.

11 https://kimi.moonshot.cn/user/agreement/userPrivacy.

Web Scraping and Threat to Data Protection

Web scraping, also referred to as Data scraping, is an automated technique used to extract information, such as text, images, videos and metadata from various websites, which are then analyzed or stored for various uses.[12]

The issue of web scraping and data protection was recently in the news in India, when Shri S. Niranjan Reddy, a Member of Parliament, expressed his concerns over web scraping of publicly available user data by social media companies for training of AI models. He questioned the Ministry of Electronics and Information Technology (MeitY) regarding measures to regulate web scraping, to ensure transparency and establish accountability.

In response, Shri Jitin Prasada, Minister of State in MeitY, emphasized that web scraping is being governed by the Information Technology Act, 2000 (IT Act 2000), its associated rules (IT Rules 2011), and the Digital Personal Data Protection Act, 2023 (DPDP Act 2023).[13]

Hence, web scraping, although not explicitly illegal, is still governed by various data privacy laws as it may involve the personal data of individuals or groups.[14]

12 https://www.miquido.com/ai-glossary/what-is-ai-data-scraping/.

13 https://sansad.in/getFile/annex/267/AU558_hhtT2g.pdf?source=pqars

14 https://ssrana.in/articles/web-scraping-and-personal-data-legal-and-ethical-boundaries-in-ai/.

TABLE 2 - Cases that Accentuate the Adverse Impact of Technological Advancements on Data Protection

ENTITY	Fine Amount	Cause of Action	Regulatory Body	Country or Region
Meta	€1.2 Billion	Transferring personal data of European users to the United States without adequate data protection mechanisms and serves as a significant milestone in data protection regulation.	Irish Data Protection Commission	EU
Uber	€290 Million	Transferring European taxi drivers' personal data including sensitive information like location data and identity documents to the U.S. without adequate safeguards.	Dutch Data Protection Authority	Netherlands
LinkedIn	€310 Million	Processing personal data without a proper legal basis, specifically concerning targeted advertising practices showing the importance of lawful data processing under the GDPR.	Irish Data Protection Commission	EU

TABLE 3 - India's Regulatory Landscape on Data Protection

DPDP Act 2023	In India, data privacy and protection are primarily governed by the recently enacted Digital Personal Data Protection Act, 2023. It establishes a framework for processing personal data. The Act primarily focuses on the processing of digital personal data. It aims to protect an individual's autonomy over their personal data by demarcating rights for individuals and subsequent obligations for data fiduciaries.[15]
IT Act 2000	Primary legislation in India to deal with cybercrime, data protection and E-commerce. Section 43A of the IT Act 2000 provides for compensation for failure to protect sensitive personal data.
IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011	The IT Rules 2011 apply to organizations that collect, store or handle sensitive personal data. The IT Rules 2011 mandate specific security practices and procedures for entities that collect, store, or process sensitive personal data.

15 The DPDP Act defines "data fiduciary" as any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data.

TABLE 4 - Major Data Breach Cases in India

CASE	TYPE OF DATA ALLEGED TO BE BREACHED	IMPACT AND CONSEQUENCES
K.S. Puttaswamy vs Union of India *(AIR 2017 SC 4161)*	Personal information and biometrics of individuals.	The Honorable Supreme Court of India unanimously recognized the right to privacy as a fundamental right under Article 21 of the Constitution of India. This case laid the foundation for data protection and privacy laws and emphasized the necessity of safeguarding personal information.
Jubilant Food Works Limited vs. Union of India *(W.P.(C) 7743/2019)*	Confidential user/customer data, and hosted on URLs without consent.	Delhi High Court in the case ordered removal/ access disablement of the impugned URLs.
AIIMS Data theft case (2022)	Data breach when cybercriminals had hacked into the servers of AIIMS and took charge of more than 1TB of data at the institute asking for hefty ransom.	This led AIIMS to switch to a manual record keeping process thereby slowing down the processes at the Institute.
Data breach of Personally Identifiable Information (PII) by hackers	A report by U.S.-based cybersecurity firm, Resecurity, disclosed a serious data breach wherein the hacker extracted sensitive information from the Covid-19 test details of citizens registered with ICMR.	Personally identifiable information of 815 million Indians had been put up for sale on the dark web.

Conclusion

Generative AI models like ChatGPT and Stable Diffusion use massive data sets and heavily rely on data that is publicly available on the internet for their training, development and upgradation. Hence, they render personal data of individuals, as well as the data of companies, vulnerable to violation and misuse.

The critical aspects that companies should consider are compliance to data protection laws, safeguarding of IP, usage rights and liability. Though AI is part of our daily lives, how it operates to leverage content is not clear and laws to regulate the same are not yet streamlined in many jurisdictions. Hence, the adoption of measures to ensure transparency has become a vital concern for companies. ■

Breaking Free: Unleashing Innovation Beyond Corporate Walls

By

Gayle Anderson
VP of Business Development
ganderson@innventure.com
and

Audrey Dwyer
Strategic Communications Manager
adwyer@innventure.com

Innventure

ABSTRACT

Drawing from the keynote address given by Gayle Anderson, VP of Business Development at Innventure at the Licensing Executives Society Silicon Valley Chapter's Annual Conference, this article presents an alternative commercialization model that preserves corporate value while enabling entrepreneurial execution. The approach combines four key phases: technology evaluation against market needs, company formation, strategic funding, and experienced operational leadership.

The article features a compelling case study of Procter & Gamble's revolutionary polypropylene recycling technology, which transformed from dormant IP to a NASDAQ-listed company valued over $1 billion in seven years. This success demonstrates how creative IP deal structures can unlock trapped value by allowing inventors to guide their innovations while maintaining corporate connections, creating win-win scenarios for all stakeholders.

For IP licensing executives, this model offers a scalable, repeatable framework that transforms R&D from a cost center to a value generator. By engineering new pathways between corporate innovation and entrepreneurial agility, organizations can ensure their breakthrough technologies reach markets that need them most, creating value for corporations, inventors, investors, and society alike.

The Innovation Paradox at the Computer History Museum

Visitors to the Computer History Museum often ask: what was the first computer? The answer is far from simple. What counts as 'first' depends on how you define the problem.

The history of technology is rarely about a single moment or a lone inventor. It's about a series of breakthroughs, each building on the last, often in parallel, and often with multiple uses in mind. This observation frames a critical question about innovation itself: What makes an innovation successful? Is it the brilliance of the idea? The timing of its introduction? Or perhaps something else entirely—like finding the right pathway to market?

The truth is startling: approximately 70% of potentially transformative technologies[1] developed within multinational corporations never reach the market. These groundbreaking technologies sit untapped—not because they lack potential, but because they have never found their pathway to the world.

The Hidden Innovation Crisis

Let's go back to 2015. A brilliant scientist at Procter & Gamble had developed a revolutionary technology for recycling polypropylene—one of the most common yet difficult-to-recycle plastics in our world. This was not just an incremental improvement; it was transformative. It could convert low-value, often landfill-bound plastic into material nearly identical to virgin plastic.

But there was a problem. While P&G recognized the technology's potential, it is not in the recycling business. As Dr. John Layman, the inventor, explained: "If you look at P&G today, we're not a vertically integrated supplier. We don't make our own plastics. We generally buy those and then partner with converters to actually make plastic articles for products or packaging."

P&G knew from day one that if successful, they would need an external partner to bring this technology to life. Despite its enormous potential

1 https://www.sciencedirect.com/science/article/pii/S0268401221001596.

impact, it simply was not aligned with their core business. And this is the dilemma many innovative companies face.

Remember: Just because a technology IMPACTS your business does NOT mean it SHOULD BECOME your business.

The polypropylene recycling breakthrough risked becoming like the Babbage Engine: a brilliant innovation waiting for its moment. A little more history is in order.

The Babbage Engine — as some of you may know — is a mechanical computer designed in the 1800s but was not actually built until 2002. It was a groundbreaking innovation that waited over 153 years until it found its path to reality.

So, how can you ensure your most promising innovations do not have to wait 153 years to reach the market and make a meaningful impact? Invention is not just about being first—it is about creating impact through flexibility and adaptability.... a catalyst for transformation.

The Traditional Innovation Pathways

When companies develop promising technologies outside their core focus, they've traditionally faced limited options:

1. **Try to commercialize it themselves, despite it not being their core business**
2. **Find another large company to license or acquire it**
3. **Work with traditional venture capital that accepts a high failure rate**
4. **Let the inventor leave to create a startup, potentially losing control and future value**
5. **Simply shelve the technology — wasting both the investment and the potential impact**

Many readers have likely considered or navigated these paths firsthand. You know the limitations. You've felt the frustration.

As IP licensing executives know all too well, each pathway has significant limitations that can leave transformative technologies unrealized—not because they lack value, but because they lack a pathway to market.

A Different Approach: Creating New Bridges

The question Innventure's model was inspired by: WHAT IF there was a better way? A path that does not force talented innovators to choose between their corporate home and seeing their technological vision?

That is where this model creates value. The model does not just take technologies to market—it helps to build bridges between corporate innovation and entrepreneurial execution.

Innventure arranged for Dr. Layman, the brilliant P&G scientist who invented the polypropylene recycling technology, to work directly with Innventure during the implementation of the model, creating a knowledge transfer that preserved the deep technical understanding while bringing in industry experts.

This arrangement gave him the opportunity to guide his innovation's journey while maintaining his connection to P&G. P&G had searched globally for recycled polypropylene solutions and found nothing that met their standards. As Dr. Layman explained, "with 8,000 technologists and deep expertise in cleaning, we asked ourselves: Can we put our powers of cleaning to work on cleaning recycled resins?"

What started as a small investment with minimal time commitment grew as they hit milestone after milestone. They discovered they could take even the dirtiest polypropylene and transform it into material nearly identical to virgin plastic.

This is where the Innventure model entered the picture with a novel approach to commercialization that preserves corporate connection while enabling entrepreneurial execution. Together, Dr. Layman and Innventure built a better innovation model by combining Innventure's entrepreneurial agility with the resources and capabilities of a big company like P&G.

Unleashing Innovation Beyond Corporate Walls

This demonstrates what happens when we deliberately engineer better pathways between corporate innovation and market impact—creating a scalable, repeatable model for unlocking untapped value.

Today, PureCycle Technologies, the entity tasked with commercializing the polypropylene recycling technology, is worth over a billion dollars. This was NOT luck.

The Collaborative Innovation Model

The model works in four key phases:

1. **EVALUATE:** Assess the technology against market needs
2. **FOUND:** Create a new company around that technology
3. **FUND:** Provide the necessary capital to develop and scale the company
4. **OPERATE:** Leverage experienced entrepreneurs to drive commercial success

This creates value across the entire ecosystem:

- **For corporations,** it transforms R&D from a cost center into a value generator
- **For inventors,** it creates a path for their innovation to reach the market
- **For investors,** it provides access to early-stage opportunities with reduced risk
- **For society,** it is a solution that addresses today's most pressing challenges

Breakthrough technologies deserve the opportunity to reach customers who need them today. The market is hungry for these solutions. This is one way to get there. And again, it is scalable and repeatable.

The Silicon Valley Contrast

Silicon Valley has long been the epicenter of innovation and disruption. But Silicon Valley is not just a place. It's a mindset—a way of thinking about innovation that transcends geography.

That mindset is about seeing possibilities where others see barriers and connecting dots others have not connected. This remarkable ecosystem has thrived on bold entrepreneurs creating new entities to pursue visionary ideas. But what if we could expand the innovation ecosystem even further?

This is where the approach illustrated by the PureCycle Technologies example differs from the traditional Silicon Valley model. While the startup ecosystem in Silicon Valley has created extraordinary value, it also embraces a high failure rate as just part of the process.

This model incorporates a different mindset that does not accept a "fail-fast" mentality. Large multinationals share this sentiment—it does not make sense for them to license valuable IP to an external partner only to see it fail.

This is exactly why Procter & Gamble, with its 187 years of measured, risk-averse decision-making, chose to employ this framework. Not because they were gamblers taking a chance, but because every other approach had failed to meet the market's need for high-quality recycled resin.

This represents Silicon Valley thinking without Silicon Valley's acceptance of failure—a true market transformation that brings innovation to life beyond geographic boundaries.

The Power of Creative IP Deal-Making

As we look to the future of IP licensing and commercialization, we see tremendous opportunity to expand collaborative innovation models. Across industries, organizations are recognizing that tomorrow's challenges require new forms of partnership.

From climate change to healthcare to artificial intelligence, the most pressing problems demand solutions that combine the resources and expertise of established organizations with the focus and agility of entrepreneurial operators.

Silicon Valley has always led the way in redefining how innovation happens. The spirit of Silicon Valley is not just about creating new companies—it's about finding ways to bring transformative technologies to life, regardless of where they originate.

As IP experts and deal architects, LES members do not just facilitate transactions—they engineer the future. They stand at the intersection where groundbreaking discoveries transform into market-changing realities. LES members understand better than most: markets evolve at their own pace, often faster than corporate strategic planning cycles. Breakthrough technologies deserve the opportunity to reach customers who need them today.

The Computer History Museum reminds us that the history of technology is NOT about a single moment or a lone inventor. It's about a series of breakthroughs, each building on the last, which can be serial in nature OR in parallel, and can potentially result in dual- or even multiple-use cases.

This approach can change everything. It changes how we think about IP licensing, how we approach technology commercialization, and how we define success. The future belongs to those who can connect worlds—combining the resources and expertise of established organizations with the focus and agility of purpose-built entities.

By making these connections through creative IP frameworks, innovation can be unleashed beyond corporate boundaries and transform industries. If you remember just one thing from this article, let it be THIS:

The question isn't whether we need breakthrough innovations—it's whether we will create the pathways necessary for them to reach the world. ■

Photo:
Computer History Museum (Wikipedia)
https://commons.wikimedia.org/wiki/File:Computer_History_Museum_(9364461418).jpg

LES INTERNATIONAL BOARD OF DIRECTORS 2025-2026

FROM LEFT:

Marko Brumnik, YMC Observer | **Ann Cannoni,** Director | **Claudio Ulloa,** Director | **Georgina Busku,** Corporate Secretary
Sonja London, Past-President | **Jean-Christophe Troussel**, President | **Ningling Wang,** President-Elect
Dana Robert Colarulli, Executive Director | **Lionel Tan,** Director | **Hemang Shah,** Vice- President
Matteo Sabattini, Treasurer | **Bob Held,** Vice-President | **Tilman Müller-Stoy,** Vice-President | **Sophie Pasquier,** Vice-President

NOT PICTURED - Legal Counsel: **Gillian Fenton and Peter Ling.**

UPCOMING LESI MEETINGS

2025

September 22-26
LES China Annual Meeting and LESI Industry Visit
Xi'an & Beijing, China

September 29-30
LES Pan-European Conference
The Hague, The Netherlands

October 19-22
LES USA & Canada 2025 Annual Meeting
Boston, MA, USA

November 7
LESI YMC 2025 Pan-European Conference
Lisbon, Portugal

2026

April 26-28
2026 LES International Annual Conference
Dublin, Ireland

October 18-21
LES 2026 USA-Canada Annual Meeting
San Diego, CA

PAST LESI PRESIDENTS

2025	S. London	2007	R. Grudziecki	1989	K. Payne
2024	M. Lasinski	2006	P. Chrocziel	1988	D. Ryan
2023	I. Nakatomi	2005	W. Manfroy	1987	P. Hug
2022	J. Paul	2004	J. Gullikssson	1986	L. Mackey
2021	A. Yap	2003	M. Jager	1985	M. Ariga
2020	F. Nicolson	2002	T. Sueur	1984	F. Pombo
2019	F. Painchaud	2001	E. Shalloway	1983	H. Hodding
2018	P. Hess	2000	H. Goddar	1982	W. Poms
2017	P. Bunye	1999	P. Mandros	1981	S. Heijn
2016	J. Sobieraj	1998	R. DeBoos	1980	J. Stonier
2015	A. Michel	1997	S. Layton Jr.	1979	J. Gaudin
2014	Y. Chua	1996	J. Brown	1978	D. Smith
2013	K. Nachtrab	1995	N. Jacobs	1977	M. Okano
2012	J. Malackowski	1994	O. Axster	1976	B. Hedberg
2011	A. Lewis	1993	L. Evans	1975	M. Finnegan
2010	P. O'Reilley	1992	A. Mifune	1974	J. Gay
2009	A. Liberman	1991	F. Noetinger		
2008	C. Fukuda	1990	J. Portier		

les Nouvelles

VOLUME LX NO. 3 | SEPTEMBER 2025

JOURNAL OF THE LICENSING EXECUTIVES SOCIETY INTERNATIONAL