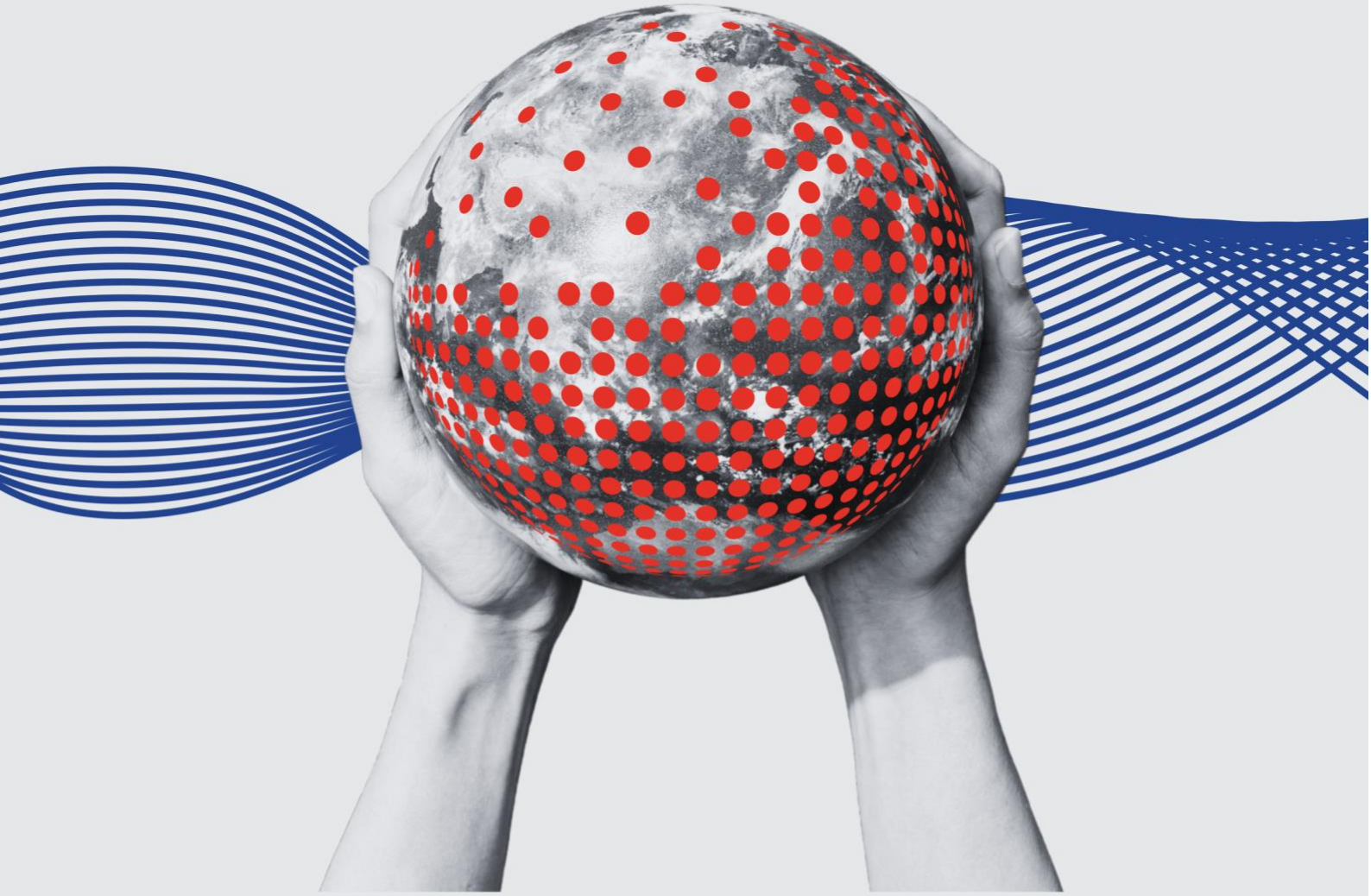
SCOPE IPR

EU-ASEAN Sustainable Connectivity
Package - Intellectual Property Rights

ASEAN Handbook

on IP Rights in the Digital World



EUIPO
EUROPEAN UNION
INTELLECTUAL PROPERTY OFFICE

Funded by
the European Union

asean

Table of Contents

Table of Contents 1
1. Introduction to IP Rights in the Digital Era 2
2. Copyright and Digital Content 5
3. Trade Marks and Digital Branding 12
4. Trade Secrets 19
5. Patents and Designs in the Digital World 24
   5.1 Designs 24
   5.2 Patents 25
6. IP and Other Intangibles in the Digital World 30
7. Emerging Technologies and IP 34
8. IP and Business Strategy 38
9. Harmonisation of IP Rights in the Digital Era: Future Directions and Policy Recommendations 44
10. Intellectual Property Symbols and Their Meanings 50
Glossary 51

1. Introduction to IP Rights in the Digital Era

The digital era is fundamentally challenging and reshaping intellectual property (IP) rights. Copying digital content (from music to movies to software) and redistribution, sometimes without the copyright holder's permission, is now easy. The global reach of the internet, social media, and applications (apps) makes IP infringement a cross-border issue, making enforcement difficult and raising legal and jurisdictional issues.

New technologies from artificial intelligence (AI) to blockchain and cloud computing create complex questions about ownership and authorship of IP. There is always a tension between protecting IP and ensuring access to information, but the sheer scale of online copying makes this a bigger challenge than in the past. Data collection is now a norm of business, conflicting with the importance of protecting personal data and the IP that can be derived from that data.

IP laws are being tested by AI-generated content and the ease of digital sampling. At the same time, automation and AI tools are helping with IP creation and generation, as well as IP protection and management. New types of IP enforcement mechanisms, such as website blocking and content takedown notices, are becoming commonplace. These often operate in private domains like social media platforms and e-commerce marketplaces, far away from traditional government authorities, creating new roles for government in regulating enforcement outside their normal reach (e.g., Notice & takedown systems).

The digital era requires a re-evaluation and adaptation of IP laws and practices to address the unique challenges and opportunities presented by new technologies.

In the digital age, IP protects a variety of elements, including:

Copyright
Creative content such as music, audiovisual, animation, published software and other art forms. Much of it today is digital.

Trade Marks
Cover goods and services and are also used as URLs and online handles.

Trade Secrets
Protect business secrets and can include algorithms and customer data.

Patent
Protect inventions across all fields of technology, including products, processes, and increasingly in some jurisdictions, software and even business methods - provided they are new, non-obvious, and inventive, usually of a scientific nature.

Designs
Protect aesthetic creations, usually physical objects, but increasingly digital designs like user interfaces and digital icons.

Today, intangible assets are crucial to the digital economy; whether this means positioning on an app store, a license deal, brand equity or a unique piece of business know-how. IP rights are the legally protectable form of, and a subset of, intangible assets which a business can own and apply in the real or digital context. Innovation and intangible assets are central to companies' competitiveness, and the digital world is creating a grey area between ever more subtle intangibles and IP.

Commercialisation and contracts are critical to IP. Contracts are how IP is applied and usually remunerated. The digital world is speeding up commerce, making traditional contracts less effective. Click licenses, smart contracts, and even the blockchain are being adopted to enable smart and fast use and payment for IP.

IP enforcement traditionally operated only in the real world through government departments like Customs, Police, administrative bodies and courts. Today, vast amounts of enforcement are done online, using IP notices and takedown procedures, often without any involvement from government authorities. For example, Notices are typically issued by IP owners (or software suppliers) to social media platforms requesting the removal of IP infringement.

ASEAN is addressing the coming digital age with its ASEAN Digital Masterplan 2025. This will help the region enhance digital connectivity, digital systems integration, and cybersecurity. ASEAN plans to transform itself into a leading digital community by focusing on five key strategic pillars: more digital infrastructure, digital transformation, resilience, trust and security, digital policy, regulation, and standards, and cooperation and collaboration. One example is the ASEAN Digital Data Governance Framework, promoting 5G technology for the 4th Industrial Revolution, and implementing policies to harmonise digital regulations and standards across member states. Businesses can expect these transformations to reach them soon and must adapt their practices to take the best advantage of the digital age and compete globally.

The purpose of this handbook is to help IP owners, and particularly SMEs to understand how IP operates in the digital era and how to protect, deploy, commercialise and enforce their IP in ASEAN Member States, in the coming decade as technology revolutionises the IP world.

2. Copyright and Digital Content

Copyright protects all kinds of music, video, commercial software, databases, apps, entertainment gaming software, graphic artwork and written content. Copyright is protected automatically and arises upon creation, or more accurately, 'fixation', the term when a work is crystallised from an idea.

Some countries have a voluntary registration system, but in reality, the millions of copyrights that come into being every year cannot all be registered. Some blockchain businesses will log all their copyrights, along with relevant data. To be eligible for protection, a copyrighted work must be original or independently created and must be fixed in a tangible form. Copyright grants creators with exclusive rights to their original works, preventing unauthorised copying, distribution, performance, communication and adaptation. It lasts for a specific period, varying depending on the form and country, but usually at least 50 years.

Copyright rules are largely well established, arising from conventions and treaties on IP. Treaties like the World Trade Organisation's Trade Related Aspects of Intellectual Property Agreement, agreed in 1995, sought to harmonise many areas of IP law by setting IP law and practice standards which all WTO member states had to adapt their IP laws and practices to. There have been several more recent IP treaties, but few in recent years have addressed IP in the digital age. As a result, emerging digital issues remain largely unharmonised globally, leading to variations in how different countries approach matters such as online infringement liability and the treatment of AI-generated works.

Most copyrights are commercialised through contracts, such as licences to use them. Downloadable software is typically licensed to users through click-to-accept agreements, often used to deliver end-user licence agreements (EULAs) that set out the terms of use before software installation or access. Musicians license their music rights to record companies for performances and collect royalties through collecting societies or streaming. Books are translated or adapted into films, and gaming houses license rights to characters, among other examples. Intermediaries can be appointed to license copyrights on behalf of the creators, for example, performing rights organisations.

Another model is Creative Commons, which provides standardised, free licenses that allow creators to specify how their works can be used. These have varying levels of permission, from allowing any use with attribution to restricting commercial use and adaptations. These are very common for online content sharing.

Online commercialisation is increasingly done through technology. Many web-driven businesses provide licenses for photos, videos, and other digital content. New technology like Blockchain can provide immutable data to verify content ownership. Smart contracts are self-executing agreements coded on the blockchain, which can automate the licensing process, track usage, and distribute royalties automatically.

It can also help micro-licensing, when granular licensing of content for specific uses opens up small revenue streams for creators and makes it easier for users to access and license content, including across borders.

Protection of copyright against infringement (often called copyright piracy) refers to unauthorised reproduction and other misuses. What constitutes copying or reproduction is a complex area which technology is changing. In the real world, this might mean reproduction of a copyrighted work or a public performance, which is easily seen. Online, music piracy was once dominated by file sharing, but today, streaming has become the more prevalent method. However, with streaming (unlike file sharing), there is no copying of a file. Instead, this new form of copying is called communication to the public, which constitutes infringement where there is no actual copy made.

Online piracy platforms created a new issue, namely the liability of the platform distributors. This is called secondary liability. It is well established in common law countries like Singapore, Malaysia, Australia and the UK, which share their judicial sources of law. Civil law countries like Thailand, Viet Nam, the Philippines and Indonesia require specific laws to enact secondary liability. In essence, secondary liability means the platforms are liable if they know or ought to have known that the content was illegal. If they do not have the knowledge, they have a safe harbour, provided they put in place a process to remove content quickly.

In reality, the large-scale piracy problem today is one of location. Most piracy sites come in the form of torrents, streaming, file sharing, cyberlocker, online forums and social media sharing. But many are located in countries without laws to prevent them. Different copyright industries often have large industry associations that handle large-scale problems.

Digital Rights Management (DRM) technologies are used by copyright holders to control the use of their digital content. DRM includes encryption, access control, copy protection, and use restrictions. DRM also uses other technology called Technological Protection Measures (TPMs), which are, in essence, digital locks. So, streaming companies use DRM and TPMs to stop people from misusing the streamed content, e-books use DRM to stop users from re-sharing or copying, and software companies use DRM to prevent unauthorised installation and use of their software. Software companies also use phone home DRM tools to ensure they know when installed software accesses their services for updates or additional information. These reports are generated when unlicensed users access these features.

Many but not all copyright laws protect DRM and TPMs to prevent circumvention to varying degrees.

SMEs face problems protecting content online, considering the advances in technology. They may own thousands of copyrights, so the first step to protect their works is to document and capture the data. SMEs may need to use web monitoring

and file detection tools, and seek the assistance of industry associations or national copyright collecting societies, or IP lawyers. Most online platforms, or social media sites, have procedures for submitting takedown notices for infringing content. There are also digital tools like "Content ID" systems that help copyright holders identify and manage their content. National Government resources from the IP and Copyright offices may be helpful, too. Often, the hardest step for SMEs is organisational, how to manage their IP effectively and how to create internal resources to do so.

One complex area of copyright is fair use. Fair use permits a party to use a copyrighted work without the copyright owner's permission for purposes such as criticism, comment, news reporting, teaching, scholarship, or research. But "fair use" in copyright law is not the same in all countries. The specific exemptions or limitations for fair use vary in scope, application, and the specific factors considered. In general, it covers when educational, news reporting, transformative and other special uses are permitted. In certain circumstances, limited use of copyrighted material is allowed without permission from the copyright holder. The aim is to balance the rights of copyright owners with the public's interest in using copyrighted works for those narrowly defined purposes. Some countries have other fair use exceptions for storing copyrighted works, like archives and libraries.

A specific example of the challenge of how fair use applies in the digital age is content creators who comment on others' works. There is a whole industry around this online now. For example, a content creator using samples of video games for review purposes or making reaction videos using samples of music videos cannot claim that this is fair use, as the creator is, in effect, running a business. In practice, platforms may remove this content or demonetise it, leading to a loss of revenue. Or if repeated, the platforms' policies will block the content or remove the account ultimately. Many content creators object to this as harming their business model, without adversely affecting copyright owners.

Different content creators in the differing sectors will have different strategies for protecting rights on digital platforms and social media.

In terms of general practices, there are various approaches:

1. Create original content; ensure content does not copy others, or in cases where it refers to others, it avoids using direct copies but only refers to other content (if that is critical) tangentially.

2. Capture content in some way to have a clear record. In most cases, the original files are automatically saved, but streamed content keeps a different record. Key data to keep (usually metadata) is the date of creation and author(s) of each copyright work.

3. Utilise technological solutions, including, watermarking technologies for visual files, adding technical changes into the software behind content, or using digital rights management systems.

4. Legal tools like contracts should cover how content is used.

5. Actively monitor for infringement. An internet browser search or alert tool can notify of infringement copies, or businesses may engage a software company to search for online copies/performance. Some industries, like music, have well-established systems, run by associations and collecting societies.

Copyright in databases is a complex area. Data itself is not usually regarded as original and creative. However, the level of creativity required in each country's copyright law varies. The global trend has shifted from artistic merit to accepting even a minimal level of creativity, recognising works that demonstrate even a modest degree of creativity, such as the arrangements of data. But as data has become critical to industry, this issue is vital for data aggregators. Europe solved the problem by creating a special database right, as a new type of IP. But in the ASEAN region, no country does this, so whether databases are protected depends on how much data selection has taken place by a human, and whether that process is somewhat creative.

Technology's encroachment into copyright has been profound in recent years. There are technology solutions for many of copyright's problems, creating new opportunities, revenues and tools for creators. At the same time, copyright has become much more complicated, and gaps have been exposed in copyright protection. Copyright laws need to be updated[1] to reflect the impacts of AI, fair use, and the digital age. At the same time, harmonisation is needed across the region to avoid differential treatment in what is now a borderless digital world for creators.

[1] As at 2025 most ASEAN IPOs are now reviewing their copyright laws.

Summary of Chapter 2: Copyright and Digital Content in the Digital Economy

Global Harmonisation Gaps
While traditional copyright is well-established through treaties, issues specific to the digital age - such as AI-generated works and online infringement liability - remain largely unharmonised globally, creating different legal approaches between countries.

New Forms of Infringement
Online piracy has shifted from file-sharing to streaming, introducing the legal concept of "communication to the public" as a form of copyright infringement, even without a physical copy being made.

Platform Accountability (Secondary Liability)
Online platforms face "secondary liability" for illegal content if they know or should have known about it. To avoid this, they must implement "safe harbour" procedures, such as takedown notices.

Technological Solutions for Licensing and Enforcement
Blockchain and smart contracts are emerging technologies that can automate licensing, track content usage, and distribute royalties automatically, enabling new models like micro-licensing.

Summary of Chapter 2: Copyright and Digital Content in the Digital Economy

Digital Locks (DRM/TPMs)

Digital Rights Management (DRM) and Technological Protection Measures (TPMs) are technologies used to control and restrict the use of digital content, such as preventing copying or unauthorised installations, although not all countries protect these measures equally.

Fair Use Challenges

The concept of "fair use" is complex and varies by country, creating particular challenges in the digital age for content creators who use parts of copyrighted works for commentary or reaction videos, as their commercial activity can complicate a fair use claim.

SME Protection Strategies

Small and medium-sized enterprises (SMEs) must proactively protect their digital copyrights by documenting ownership, using technology like web monitoring and digital watermarking, and utilising platform-specific takedown notice procedures.

Database Copyright Issues

As data becomes a critical asset, copyright protection for databases is a complex issue. It often depends on the level of human creativity involved in the data's selection or arrangement, with some regions creating specific database rights to address this.

3. Trade Marks and Digital Branding

Trademarks protect brands. They must usually be registered under a process where an application is filed and then examined by an IP office to ensure formalities requirements are met, that the mark complies with registrability rules[2]including substantive requirements on absolute and relative grounds. The application must cover specific goods and services using the 45 classes of the Nice classification[3]. Trademark rights are territorial - each trademark right is national and must be registered in each country separately. Trademarks are examined based on the national laws of that country.

There are two ways to file a trademark:

A. One is to file a national application with the Trademarks Office. They review it, examine it, and if there are no objections, the trademark may be granted after an opposition process. Applications can be filed in other countries and claim priority based on the first application[4].

B. Alternatively, the Madrid System[5] is an international trademark registration system based on the Madrid Agreement and the Madrid Protocol. Trademark applicants are able to file one application to register their trademark in multiple countries. It simplifies and reduces the cost of registering trademarks across multiple jurisdictions of interest to the applicant. In summary, an international application is filed, and then subsequent designations are sent to each national IP office.

Trademark applications can be opposed by third parties during the trademark examination stage. It takes from 6 months in very fast countries to a year or so, typically in other countries, to registration.

Because trademark registration can take time, and given the high volume of marks already registered today, entrepreneurs and businesses should conduct a trademark search early to identify any potential conflicts before filing and launching their brand. This helps avoid costly rebranding later. The search should include countries where the entrepreneur intends to launch or offer their product or service under the trademark within the next 3 to 5 years. While SMEs may not be able to cover every market at once, planning ahead is key to building up a strong and strategic trademark portfolio.

---

[2] Trademark registrability refers to the ability of a mark (word, phrase, symbol, etc.) to be officially registered with a trademark office, granting the owner exclusive rights to its use and protection against infringement. In essence, it's about meeting the legal requirements for trademark protection and successfully navigating the registration process.

[3] The Nice Classification is a system used worldwide for grouping similar goods and services into 45 distinct classes, used for trademark registration purposes.

[4] Using a system under the Paris convention, later overseas applications filed within 6 months take the same priority date, that is the date of filing of the first application.

[5] The Madrid system is administered by the World Intellectual Property Organization (WIPO),

Trademarks today encompass more than words. Logos and stylised scripts are commonly registered (but don't forget that with logos, there may be overlaps with graphic copyright works). Slogans may be registered too, and some countries allow more non-traditional marks like sound marks.

In the digital era, entrepreneurs and businesses must go beyond trademark registration to also secure domain names and social media handles for their brands. However, as the online environment is global, the exact brand name may not always be available - it may already be in use by a business in another country. In such cases, adding a descriptive word can help differentiate the handle. For example, a jewellery business called SILVERADO may choose to add the word JEWELLERY in its social media handles because the main.com domain name or Instagram handle is taken by a different business in another country. The precise domains and handles needed will vary. Many small businesses use Instagram and TikTok. Particular business sectors may have specific ones; travel businesses have several specific online platforms for the travel and vacation sector.

Trademark commercialisation is done in many ways. Once trademarks are registered, they protect the sale of the goods or services by the owner. However, a trademark owner can choose not to sell the goods or services directly and instead license the rights to others. It is possible to license trademarks to others; indeed, sometimes it is preferable. Hotel groups are largely brand licensing companies today, as they own few properties but license them from the owners. Merchandise (e.g., toys or clothing from films, musicians, games, etc) is a form of licensing, whereby the owner gives the rights to produce and sometimes sell to a specialist producer of the goods. Online, many brands are licensed into games, virtual worlds, and NFTs in the collectables world.

Marketing a brand is vital. This was traditionally done through advertising and marketing agencies. Today, online marketing is a huge industry and is increasingly automated. For example, pop-up adverts are usually automated by online brand advertising companies to appear only when relevant. Social media marketing requires promoting the business and brand online to target customers. Influencers and endorsements can help drive customer engagement. There are even automated ad platforms that place online advertising automatically as pop-ups and banners online. Wherever appropriate, businesses should consider using written contracts or formal agreements when engaging marketers, influencers, or advertising platforms. This can help clarify expectations, reduce the risk of brand misuse, and mitigate reputational harm arising from misrepresentation or error.

Infringement of trademarks happens in several ways. Copying a trademark in whole or a substantial part, then using it on similar goods or services, is the most common form of infringement. Where the infringing sign is not identical but merely similar, most countries require some element of consumer confusion to be present. Very often, this is a technical legal question. In some cases, this can be a criminal issue, especially if it is deliberate or the copying is identical. In other cases, it can be a civil liability, or in some countries, there are administrative bodies where trademark complaints are filed.

Counterfeiting is when a deliberate replication of identical products occurs. In the ASEAN region, the most common complex counterfeit products come from major manufacturing source countries where production is very sophisticated and low cost; with lower tech counterfeits like apparel, footwear, toys, etc, more often locally made in the region.

Genuine commercial conflicts do happen where two businesses have similar names. Where two businesses have different markets, it may be possible for the parties to reach an agreement for both parties to still operate in their respective markets and avoid conflict. Businesses can also take preventative steps, such as undertaking trademark monitoring for similar marks, then conducting searches and seeking advice to avoid conflicts.

Brand protection in digital environments has become a major challenge; e-commerce and social media have driven the sale of goods and marketing of businesses online. In the case of online counterfeiting, the same rules as copyright arguably should apply to trademarks. That is, a person who infringes is the primary infringer and should be the first person liable. But in reality, they may be in another country (or in the case of drop shippers, never even see the goods). Since most e-commerce marketplaces are private organisations, the argument around the world is that they should take responsibility to police their platforms to stop crimes. Therefore, some countries impose secondary liability for those who sell counterfeit goods with knowledge (e.g., after they have received a legal notice that the goods are counterfeit), and yet do not remove them. What constitutes legal notice is technically complicated; it can include a simple written/emailed notification, or there are other forms of notice, such as implied or constructive, which are technical legal concepts. Those platforms that offer good content removal systems should qualify for safe harbour.

However, reality is different. Trademark secondary liability rules are not harmonised around the world, partly because mass goods e-commerce arrived 20 years after online copyright file distribution. As a result, rules differ or are still not yet in place in many countries. Indeed, online counterfeit goods sale is commonly a cross-border industry, because the producer may be in one market, the online vendor or drop shipper in another, the consumer in another, and the genuine brand owner somewhere else.

Harmonisation between the different ministries and across ASEAN member states is needed. At present, AMSs take different approaches to the issue, so it is challenging to understand the different systems and processes in each country; this is more so when many platforms operate across different countries, but most run different enforcement processes.

Meanwhile, a substantial industry has emerged to support online brand protection. Many companies now offer software that enables brand owners to monitor e-commerce platforms, identify suspected counterfeit listings, and request their removal. Many brand owners now outsource the surveying and issuing of notices requesting the takedown of online adverts for counterfeit goods to these software companies. Or

they recruit teams to handle the huge volume of notices and takedowns that occur. That puts pressure on the marketplaces to put in place procedures which often differ from one to the next and hire their teams to handle the receipt of notices and takedowns. Some of these online brand protection companies offer products for SMEs; this trend is likely to increase as the overall cost gets cheaper.

However, online brand protection software typically targets only the adverts, addressing just one part of the problem. Dealing with the underlying problem of the physical counterfeit goods is still important. When an e-commerce platform removes the adverts, the suppliers and traders offering the counterfeit goods may move platforms, relist them under a new name or simply continue offering them.

Brand owners must undertake inquiries into the offline location of the infringer and counterfeit goods and take legal action. Taking legal action against merchants offering counterfeit goods is difficult since IP owners have no information on the merchants. By their nature, e-commerce marketplace data is under the control of the e-commerce company, and they do not publish it. Legal actions can require the cooperation of the e-commerce marketplaces. There are complexities around disclosure of identities of hidden merchants, past sales of counterfeits, repeat offenders, when exactly do platforms have knowledge and whether their systems are strong enough to qualify for safe harbour.

The online counterfeiting problem is one on a huge scale now, as e-commerce has become the largest channel to buy goods (including counterfeit goods). One proposal gathering momentum is the use of Codes of Conduct for IP owners and e-commerce marketplaces to agree on standards and processes for various practical issues, such as notice and takedown timings, Platform KPI measurement, treatment of repeat offenders, merchant identity disclosure, and joint legal actions (between IP owners and e-commerce platforms).

There are suggestions that AI-based tools will be able to spot and deal with counterfeit goods more efficiently in time; this is, after all, a technology industry. The question is whether e-commerce marketplaces are incentivised to do this.

Infringement and other brand misuse on the internet, social media and other digital formats is a frequent issue. These are sometimes related to other kinds of fraud, such as phishing. Companies may hire software companies to trawl for misuses and then seek to remove them through a variety of legal tools. These include the social media platform’s trademark policy, which usually allows trademark owners to show evidence of brand ownership and submit a notice to remove a brand’s use. Cross-border problems exist here, too, as the person misusing the mark may be elsewhere. If the secondary liability rules are not clear, trademark owners have to hope the platform is responsible and will remove the illegal use.

There are a variety of other trademark infringement issues and solutions. Domain names misusing others’ brands can usually be removed through online arbitration. The

most famous is the UDRP system[6], which covers most global domains, but some national domains have local arbitration systems. These are usually cheaper than court proceedings. Metatags, keywords/and AdWords disputes can often be resolved by going to the search engine.

Brand impersonation is not uncommon, usually as part of a wider fraud, when a company finds its brand misused by a criminal network, often for financial gain. For example, a bank might find fake websites, emails or SMS messages pretending to be from the bank, or criminals may set up fake online stores pretending to be the original brand owner[7]. A combination of criminal fraud enforcement by criminal authorities and trademark complaints to the relevant national body is usually necessary to prevent such misuse and protect consumers.

A key challenge in the online trademark world is the role of government. Large volumes of online infringement problems arise today, and most ought to be dealt with bilaterally between IP owners and online platforms/internet service providers using platform IP dispute mechanisms. Then, there is limited direct involvement from government authorities. However, in some countries, including parts of ASEAN, public authorities are increasingly engaging with platforms to support enforcement efforts. However, the huge volume of IP complaints between rights holders and online platforms means it may not be feasible for governments to directly intervene in most cases. This raises important questions about whether governments should play a more active role in regulating these private platform enforcement mechanisms - for instance, by setting standards for platform compliance or imposing penalties for inaction - and how such regulation should be designed.

While trademarks are vital to the sale of goods and services online and offline, IP owners should not overlook the need for other registrations to operate a business. Company, business, product, import and other regulatory regimes might apply to a business or sector. Businesses should seek legal advice on setting up a business to get a full overview of all the regulatory requirements.

[6] The Uniform Domain Name Dispute Resolution Policy (UDRP) is a framework for resolving disputes concerning the registration of internet domain names that allegedly infringe upon trademarks. It offers a streamlined and cost-effective alternative to traditional court litigation. Trademark holders can file a complaint with an approved dispute resolution service provider asserting that a domain name registration is abusive.

[7] See article by The Rakyat Post of Maybank cautioning customers about counterfeit websites designed to mimic their official site aiming to steal user credentials : *There's A New Fake Maybank Website Tricking Malaysians & Stealing Banking Information*)

Summary of Chapter 3: Trade Marks and Digital Branding

Beyond Traditional Registration
Digital branding requires securing domain names and social media handles in addition to formal trademark registration, often facing global availability challenges.

New Commercialisation Avenues
Trademarks are increasingly licensed for digital products, including virtual goods in games, virtual worlds, and NFTs, creating new revenue streams.

Automated Online Marketing
Digital marketing relies heavily on automated ad platforms and social media, necessitating formal agreements with marketers and influencers to prevent brand misuse.

Online Counterfeiting & Secondary Liability
·E-commerce platforms face complex "secondary liability" for counterfeit goods, with varying and unharmonised rules globally, unlike copyright's more established framework.

Cross-Border Enforcement Challenges
The global nature of online counterfeiting complicates enforcement, as producers, vendors, and consumers can be in different jurisdictions, requiring international cooperation.

Summary of Chapter 3: Trade Marks and Digital Branding

Emergence of Brand Protection Software
A significant industry of software companies now offers tools for brand owners to monitor e-commerce platforms and automate takedown requests for counterfeit listings.

AI for Counterfeit Detection
AI-based tools are emerging to more efficiently detect and address counterfeit goods online, though marketplace incentives for adoption remain a question.

Online Dispute Resolution
Domain name disputes (cybersquatting) can often be resolved through online arbitration systems like the UDRP, offering a more cost-effective alternative to court litigation.

Brand Impersonation & Fraud
Digital platforms are susceptible to brand impersonation as part of wider criminal fraud, requiring a combination of criminal enforcement and trademark complaints.

Government Role in Platform Regulation
There's a growing discussion about governments playing a more active role in regulating private platform enforcement mechanisms to standardise IP dispute resolution.

4. Trade Secrets

A trade secret is defined as information that offers a competitive edge and is kept confidential. It has three key elements:

- Not Publicly Known: The information must not be generally known or easily accessible by the public or competitors.
- Economic Value: It must provide an economic benefit, such as a cost advantage, higher product quality, or other competitive benefits.
- Reasonable Efforts to Maintain Secrecy: The business must take active steps to keep the information confidential, including using non-disclosure agreements (NDAs) and securing the information.

Trade secrets are a form of IP. However, they have different characteristics from other forms of IP. They are not registered, and in some countries, their status as IP is not very clear. Trade secrets are often used in technology, but they are very different from patents. While patents are government-granted rights to inventions for a limited period, trade secrets are protected automatically as long as reasonable efforts are made to keep them secret. It is possible to attract investors and build a business entirely based on trade secrets. Companies have even undertaken stock market listings with trade secrets as their core IP.

Some examples of trade secrets include various types of confidential business information that provide a competitive edge, such as sales methods, consumer profiles, advertising plans, supplier lists, manufacturing processes, financial information, and more. Trade secrets are valuable to a wide range of businesses, from tech companies and manufacturers to sales and distribution firms, franchises, designers, and startups. Startups and SMEs often overlook their importance– entrepreneurs and venture capital investors should think about them as an additional IP asset.

Today, huge numbers of businesses depend on data. Many of the world's great tech companies use algorithms which are trade secrets, along with collecting user data. In the digital era, the automation of data collection online has created vast trade secrets for businesses, from user analytics, customer behaviour, buying patterns, social media preferences, product preferences, and subscriber engagement. Many traditional hardware companies now use sensors to collect data. This includes agri-tech, med tech, fisheries, factories, logistics businesses and internet of things producers. Most industrial processes can be optimised through data collection and analysis.

Personal Data can be protected as a trade secret when companies collect it for business purposes. Also, under personal data privacy rules, it is subject to a separate legal protection. Personal data regimes typically require businesses to manage personal data transparently, fairly, and accurately, for limited, minimised purposes; and to manage storage, integrity, confidentiality, and limit cross-border transfer. What

amounts to personal data may not always be clear. Businesses need to manage their data with both legal trade secrets and personal data privacy regimes in mind. A data breach can cause companies personal losses, as well as create liabilities for breaches of data privacy rules.

Protection of trade secrets involves three key techniques:

- Physical: Using locks, security guards, NDAs, access rules, and a "Need to Know" approach within the business.
- Technical: Implementing device restrictions, password rules, encryption, and cybersecurity measures.
- Legal: Drafting contracts with NDAs and confidentiality clauses for all business partners.

This process to protect trade secrets in larger companies requires internal collaboration amongst lawyers, HR, IT, management, and security, as well as external advisors. SMEs do not always have these resources inside and may need to bring in consultants to help.

A common trade secrets challenge is their definition, audit, and capture. Trade secret databases exist, but there are risks in third-party reliance and even capture, documenting and adding them to a database. The cross-border nature of trade secret management and IT risks, including inadvertent disclosure, employee theft, competitor theft, cyber-attacks, and industrial espionage, must be carefully managed. Employee education on cybersecurity issues is critical in the work-from-home era.

SMEs need to come up with a clear strategy on how to define, capture, protect and manage trade secrets. In the case of digital businesses, the sheer volume of trade secrets may make this challenging.

The most common enforcement scenarios involve departing employees and directors who go on to establish competing businesses or join rival companies. Cybertheft and industrial espionage are also a concern. Trade secret theft enforcement is not harmonised in ASEAN. In civil law countries, it can be a criminal offence, with a complaint to the police needed to initiate it. In common law countries, it is usually a civil wrong only, so it requires the trade secret owner to file a civil lawsuit. Cases are often complex, so even in civil law countries, they may be more suitable for the civil courts since the police are often only able to handle (or can only justify public resources for) clear cases of trade secret theft. Many are in practice part of more complex business disputes.

Lastly, cybertheft, fraud and other related crimes can lead to trade secret theft, which is why IT protections and business management commitment are as important as legal tools.

Some cases show how trade secrets are practically protected. In Viet Nam, a US company's dismissal of an employee for breaching confidentiality rules was upheld by

the People's Court of Ho Chi Minh City[8]. In Singapore, a payroll and HR services company's lawsuit against former employees for alleged misuse of confidential information was unsuccessful due to a lack of evidence of actual misuse of the information in the employee's possession[9]. In Malaysia, a manager was found to have breached his employment terms by misusing company confidential information, with the High Court ruling that the duty of fidelity extends beyond the employment term. It is also not uncommon for employment contracts to provide that the obligation survives the termination of employment, so the employee remains bound by it[10].

Trade secret protection is not only a legal issue but also a business one. Trade secret protection processes require a commitment from management and integration into business processes. Departments like HR and IT play a crucial role, and legal assistance is vital in setting up processes. Contracts, particularly NDAs and confidentiality clauses, are essential, and prevention is always better than legal action since there is no cure for the loss of a trade secret.

Ultimately, more harmonisation of data and trade secret rules across ASEAN member states would be desirable to ensure the same practice and procedure is followed everywhere, and then businesses can plan in the same way.

[8] Viet Nam People's Court of Ho Chi Minh City - Case No. 20/LD-ST dated March 17, 2005

[9] Singapore Court of Appeal April 2020, I-Admin (Singapore) Pte Ltd v Hong Ying Ting and others - https://www.judiciary.gov.sg/docs/default-source/judgments-docs/i-admin-(singapore)-pte-ltd-v-hong-ying-ting_smu-case-brief.pdf?sfvrsn=dfd16ba5_2

[10] Ecooils Sdn Bhd v Raghunath Ramaiah Kandikeri HIGH COURT (JOHOR BAHRU) — CIVIL SUIT NO 22–516 OF 2007 SUPANG LIAN J 17 OCTOBER 2012

Summary of Chapter 4: Trade Secrets

Digital Era's Vast Trade Secrets
The automation of online data collection generates immense trade secrets for businesses, including user analytics, customer behaviour, and social media preferences, crucial for optimising industrial processes and digital services.

Algorithms as Trade Secrets
Many leading tech companies rely on proprietary algorithms, which are protected as trade secrets, alongside the user data they collect.

Personal Data Overlap
Personal data collected for business purposes can be protected as a trade secret, but it is also subject to separate, stringent privacy regulations, requiring businesses to manage data with both legal frameworks in mind.

Enhanced Digital Protection Measures
Protecting digital trade secrets requires robust technical measures like device restrictions, password rules, encryption, and comprehensive cybersecurity to guard against cyber-attacks and inadvertent disclosure.

Cross-Border Management Challenges
The global nature of digital businesses and IT risks complicates trade secret management, necessitating careful handling of data across borders and vigilance against cyber-theft and industrial espionage.

Summary of Chapter 4: Trade Secrets

Employee Education for Cybersecurity
In the work-from-home era, educating employees on cybersecurity is critical to prevent trade secret theft, particularly from departing employees who might join competitors.

Enforcement Discrepancies
Trade secret theft enforcement is not harmonised across ASEAN, with civil law countries often treating it as a criminal offence, while common law countries typically handle it as a civil wrong, leading to varied legal approaches.

Prevention over Cure
Due to the irreversible nature of trade secret loss, proactive IT protections, strong management commitment, and comprehensive legal contracts (like NDAs) are paramount for digital businesses.

Need for Harmonisation
Greater harmonisation of data and trade secret rules across ASEAN member states is desirable to standardise practices and simplify planning for businesses operating in the borderless digital world.

5. Patents and Designs in the Digital World

5.1 Designs

Design laws protect the appearance of a product, specifically its shape, configuration and surface ornamentation. The features must have aesthetic value, be novel and original. A large industrially produced product like a blender can attract design protection, but so can a new dress, necklace or chair. Conventional industrially designed products might well last 15 years in the marketplace; however, in the age of fast fashion and online trends, many designs go out of date and are no longer in use after a couple of years. These trends have exposed that traditional registration systems around the world are not as suitable as they once were, as they don't provide a simple solution for fast-moving designs. As a result, many designers do not get protection for their designs today.

There are three types of IP systems in the world which can protect products and related items like packaging:

- Registered designs
- Unregistered designs
- Unfair competition (slavish imitation), or passing off, in some circumstances

Registered design systems require an application which is checked by the design office and then granted. These work for industrial products, which justify the time and cost of the process. But fast-moving products, or products driven by online trends or digital designs, are not always well suited to a lengthy application and grant process that protects designs one by one.

Most ASEAN Member states have registered design systems using an application system, leading to registration. Some jurisdictions also offer unregistered design protection, which can provide limited rights in certain circumstances. Common law countries have passing off systems to protect reputation, which can include product cues. Some civil law countries protect slavish imitation under unfair competition, including the trade dress of products; these kinds of unregistered rights require legal action to enforce them.

Businesses can apply to register designs at the national IP offices. There is also an international registration system called the Hague system[11]. So far, Cambodia, Brunei, Singapore and Viet Nam have joined it. Or businesses can rely on the unregistered rights, if available.

Outside ASEAN, some countries have adopted unregistered design protection for sectors that have accelerated or transformed in the digital age. New types of designs

[11] The Hague Agreement Concerning the International Registration of Industrial Designs created an international system administered by the World Intellectual Property Organization (WIPO) that allows you to register industrial designs in multiple countries through a single application.

in the online environment are arising: Graphic User Interfaces (GUIs), app and desktop icons, User Interfaces (UI & UXs), Virtual Reality (VR) and Augmented Reality (AR) designs, which are entirely virtual. AI-created designs will become commonplace soon. At present, many countries (including many ASEAN member states) would not accept these as design registrations. Therefore, law changes are needed in many ASEAN Member States for the digital age – to offer faster protection, to allow fluid

digital designs to be registered, to allow virtual product designs like GUIs, to allow designs that require frequent updates and iterations, and to allow nonhuman design creators. A number of ASEAN Member States are now looking at how to amend their design laws.

Designs can be commercialised through contracts like any other form of IP. Licensing and merchandising are common. Outsourcing manufacturing is more common than not for designers, even when they wish to sell products themselves. In practice, many ASEAN designs do, in fact, license their unregistered designs too, although the exact legal basis is not strong.

The digital age raises many new areas that affect design copying and enforcement. Firstly, the ease of copying and distributing products today. New products can be easily seen online, then copied, modified, and distributed rapidly. Secondly, design files are usually digital and can be copied and shared, leading to increased infringement. 3D printing enables the easy production of individual items which may copy designs. The decentralised nature of digital manufacturing makes it difficult to monitor and control design infringement, too

Online marketplaces and e-commerce platforms are major channels for the sale of products, making it easier for copycats to distribute infringing designs. Monitoring and notice, and takedown systems (like those used for trademarks) are not as widely used in ASEAN for designs, partly because fewer are registered. The volume of online sales makes it challenging to detect and enforce design rights, requiring technology companies to support businesses. The improvement of designs for the digital age is a pressing IP need in ASEAN. Business owners in the digital age need to check the latest status of law changes. They need to decide whether, and how, to secure design protection or whether to rely on alternative unregistered protections and, where possible, other IPRs like copyrights and trademarks.

5.2 Patents

Patents protect inventions that are new, inventive and not obvious[12]. Everything from IT devices to industrial machines to chemicals and pharmaceuticals can be patented. A product or a process can be patented. A patent must be drafted as a specification document that describes the invention and its claimed unique features. Patents are filed, examined against prior art (pre-existing technology), and then granted. Although

[12] Although patentable inventions must be new at the date of first application, there are exceptions, called non prejudicial disclosures, whereby inventors may disclose the invention without harming the right to a patent. An example is disclosure at officially recognized international exhibitions.

each patent must be granted by the respective IP office, various international systems exist to simplify the process. The Patent Cooperation Treaty (PCT) is one example whereby applicants can file internationally and then designate each country later. Businesses use the PCT to simultaneously seek patent protection in numerous countries by filing a single international patent application, simplifying the initial process and deferring the costs of individual national filings.

The digital world has had several impacts on the patent system. The biggest, started in the US, when patent eligibility was widened to include software and business methods (especially online). Most countries did not follow this, but Indonesia did in 2024, widening patent criteria to allow digital and software patents.

The ability of AI to generate inventions independently - or to assist human inventors - has raised important questions about inventorship, ownership, and the patentability of AI-generated works.[13]. ASEAN countries' patent laws do not presently accept non-human inventors; however, many inventions now use AI at least partially[14]. Another AI question relates to the patentability criteria of "inventive step" and "obviousness" when AI is involved – for example, when AI can specify every permutation, e.g., of a molecule, is there an inventive step in the invention?

Technology integration has led to the creation of patent pools[15], Standards[16], Standard Essential Patents (SEPs)[17] and the concept of FRAND licensing[18]. SEPs are patents essential to industry standards, and FRAND licensing ensures that patent owners license these essential technologies on equitable terms, preventing them from abusing their monopoly by charging unfair or excessive fees. In summary, these are patent processes/systems that allow producers to create devices and implement new technologies when multiple individual patents from several companies are needed. Examples include 5G, video coding and Wi-Fi systems. By following these processes and paying the relevant royalties, companies can legally use the technology. However, this already complex system is being challenged further in the digital era. The proliferation of connected devices in the IoT era now widens the number of technologies subject to these regimes. For example, IoT connectivity, communication and connected car and driver assistance systems now require device producers to adopt the standard systems. Ensuring access to essential technologies while

[13] See USPTO guidance on the topic - https://www.federalregister.gov/documents/2024/02/13/2024-02623/inventorship-guidance-for-ai-assisted-inventions

[14] https://www.hypeinnovation.com/blog/how-ai-is-accelerating-innovation#:~:text=How%20is%20AI%20used%20in,3D%20models%2C%20and%20generate%20simulations

[15] A patent pool is an agreement between two or more patent owners to cross-license their patents related to a particular technology, often to facilitate the development and implementation of complex technologies by providing a package license to third parties

[16] Instructions, guidelines, rules or definitions that are then used to design, manufacture, install, test & certify, maintain and repair electrical and electronic devices and systems.

[17] A Standard Essential Patent (SEP) is a patent that protects technology that is essential to comply with a specific industry standard set by a Standard Setting Organization (SSO); implementers of the standard must necessarily use the patented technology.

[18] FRAND (Fair, Reasonable, and Non-Discriminatory) licensing refers to the commitment made by owners of Standard Essential Patents (SEPs) to license their patents on terms that are fair,

protecting patent holders' rights is a key concern. New licensing models may emerge, perhaps backed by blockchain tech, with smart contracts.

Patent harmonisation remains a challenge. While international treaties exist, patent laws still vary significantly across countries. ASEAN countries may need to consider this issue in their laws, given that one of its Member States, Indonesia, has widened its patent eligibility criteria, essentially offering to protect technology there but not elsewhere in the region. In addition, the speed of innovation in the digital era, with AI and large datasets driving increased patenting, already resource-challenged IPOs will need to find ways to speed up search and examination. Traditional manual review will become obsolete as AI examination becomes the norm. Until then, patent quality will be a rising concern. Claims conforming and PPHs [19]can reduce the resource cost of examining the same patent in many countries. Patent mapping is now widely used by IP owners to study technology fields and support invention strategies. Such software needs to be more widely used by ASEAN inventors.

[19] **Patent Prosecution Highways (PPHs)** are agreements between patent offices that allow an applicant whose claims have been found allowable in one office to request accelerated processing of a corresponding application in another participating office.

Summary of Chapter 5: Patents & Designs in the Digital World

Design Protection Lag
Traditional design registration systems are ill-suited for the rapid pace of digital designs (e.g., fast fashion, online trends), leading many designers to forgo protection.

Emergence of Digital Designs
New types of designs like Graphic User Interfaces (GUIs), app icons, VR/AR designs, and AI-created designs are not adequately covered by current laws in many countries, including ASEAN.

Legislative Reform Needed for Designs
Law changes are required to enable faster protection, allow registration of fluid digital and virtual product designs, accommodate frequent updates, and address non-human creators.

Digital Copying & Enforcement
The ease of digital copying, 3D printing, and decentralized manufacturing poses significant challenges for detecting and enforcing design rights online, with inadequate monitoring and takedown systems in ASEAN.

Summary of Chapter 5: Patents & Designs in the Digital World

Software and AI Patentability
The digital world has expanded patent eligibility to include software and business methods in some jurisdictions (e.g., Indonesia), while raising complex questions about AI inventorship, ownership, and the "inventive step" criteria for AI-generated inventions.

Standard Essential Patents (SEPs) in IoT
The proliferation of connected devices in the IoT era intensifies the importance and complexity of SEPs and FRAND licensing, requiring new models to ensure access to essential technologies.

Patent Harmonisation & Efficiency
Patent laws still vary significantly globally, and the rapid pace of innovation driven by AI necessitates faster examination processes, potentially through AI-powered tools, to maintain patent quality.

Strategic Patent Tools
Patent Cooperation Treaty (PCT) and Patent Prosecution Highways (PPHs) simplify international patent filing and examination, while patent mapping software aids in studying technology fields and developing invention strategies.

6. IP and Other Intangibles in the Digital World

Business intangible assets are non-physical resources that hold value for a business, contributing to its competitive advantage and future earnings potential. IP, such as patents, trademarks, copyrights, and trade secrets, is a crucial category of these intangible assets, providing legally protected exclusive rights that can be commercialised and so can contribute to a business's value by preventing imitation, enabling licensing, and enhancing brand recognition.

Many other intangible assets also exist in a business, generating value. Goodwill, customer relationships, brand equity and know-how are examples of intangible assets. These are not legally protectable in the same way as IP, but may be partially defined or protected by law, or only recognised in some countries.

A good example of a partially protected intangible asset is internet-based names, such as domain names, social media handles, and other URLs[20]. These names are connected to trademarks as they usually comprise all or part of the brand name, but are technically numerical addresses represented as words. The internet is global, while trademarks are registered in each country, and for different classes of goods and services. As a result, multiple businesses in different countries and sectors may legally own identical trademarks in different regions or industries. But internet URLs, for example, for DOVE soap and DOVE chocolate, which come from different producers, do not conflict in the trademark sense, but as URLs, they have to be

differentiated. So, www.dovechocolate.com or @dovechocolate becomes the solution. New brands face this commonly, requiring multiple words to secure vital digital marketing assets.

Unfair competition, passing off, trade dress and image or publicity rights are sometimes considered as a quasi-IP right. They have a degree of protection from international treaties. Some countries provide strong protection against copying of business cues (such as distinctive features, indications or other unique identifiers), whereas others provide little to no protection. Singapore and Malaysia, as common law countries, have clear rules under the concept of passing off. They protect against comparative advertising (where a competitor's brand is used in marketing) under trademark law. Many civil law countries apply 'German-style' anti-slavish imitation rules, preventing businesses from excessively copying competitors' product designs or branding (as is the case in Thailand and the Philippines). Other jurisdictions have not expanded their unfair competition rules in the same way.

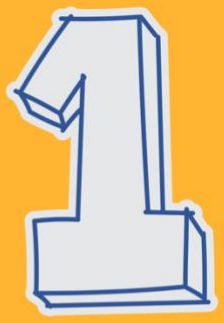
Given that the rules vary across ASEAN member states, some level of harmonisation at a regional level would be beneficial.

[20] URL stands for Uniform Resource Locator. In simpler terms, it's the web address of a specific page or file on the internet

Rights of publicity or image, or personality rights, are protected in some countries. These are an individual's right to control the commercial use of their identity, including their name, image, likeness, voice, signature, or other distinctive characteristics. These rights prevent the unauthorised exploitation of a person's persona for commercial benefit without their permission or contractual compensation. In the digital age, with the rise of influencers and online celebrity culture, personality rights have become crucial for well-known individuals to endorse products and monetise their reputation. It is important in the world of AI and deepfakes to prevent misuse of names, images, personalities and voices. AI is now able to create commercial opportunities for legitimate licensing which did not exist in the past. For example, a popular personality from one side of the world can endorse products and services on the other side of the world without being physically present. Similarly, AI deepfake technology can be used to impersonate public figures. AI tools can generate music and other content using specific voices. While copyright law protects specific expressions such as photographs and video footage, it does not typically extend to a person’s likeness or identity. Protection of image, personality, or publicity rights varies by jurisdiction and is usually governed by separate legal frameworks.

Geographical indications are a well-established IP right. They are indications which identify a good as originating in a territory, region or locality, where a given quality, reputation or other characteristic of the good is essentially attributable to its geographical origin. They are critical in a region with cultural heritage. In the digital space, many of the same issues arise as with branded goods. Producers must contend with online misuse of their GIs, fake products and digital marketing by competitors that might misuse elements of their product or reputation. They must register domain names, URLs, social media handles and may have to prevent others from trying to register them. This is often a challenge as GI producers are usually associated with limited funding and are sometimes based in remote locations. To compete effectively, they need to develop expertise in digital IP protection.

Summary of Chapter 6: IP & Other Intangibles in the Digital World



Digital Brand Identifiers

Internet-based names (domain names, social media handles, URLs) are crucial intangible assets in the digital economy, requiring differentiation from trademarks due to the global nature of the internet versus territorial IP rights.

Unfair Competition in Digital Marketing

Laws against unfair competition, passing off, and slavish imitation (trade dress) vary significantly across jurisdictions, highlighting a need for harmonisation in ASEAN to address digital marketing practices.

Publicity Rights and AI/Deepfakes

The rise of influencers and AI-generated content (including deepfakes) makes personality/image rights critical. AI creates new licensing opportunities for public figures but also poses risks of unauthorised impersonation.

Geographical Indications (GIs) Online

GI producers face challenges with online misuse, fake products, and digital marketing by competitors, necessitating expertise in digital IP protection and securing relevant online identifiers.

Summary of Chapter 6: IP & Other Intangibles in the Digital World

AI's Impact on Personality Rights

AI's ability to create realistic voices and images raises new questions about the scope of publicity rights, as copyright law typically doesn't cover a person's likeness or identity.

Digital Marketing Assets

New brands commonly need to use multiple words or variations to secure available digital marketing assets (domain names, social media handles) due to the high volume of existing online identifiers.

Cross-Border Enforcement

The varying legal frameworks for unfair competition and publicity rights across countries, particularly within ASEAN, complicate cross-border enforcement against digital misuse.

7. Emerging Technologies and IP

Social media and the rise of User Generated Content (UGC) have created an entire industry of video platforms, content creators, and influencers. Today, they represent a major force in IP creation. As this industry is still new, many content creators lack the experience to fully leverage their IP. Many have huge copyright portfolios, their names can become brands, and they have the potential to build licensing programs (if their IP portfolio is in order). On the flip side, many content creators unknowingly or mistakenly incorporate others' IP into their content, leading to legal risks. Although many content creators operate commercially, fair use (or its equivalents, like fair dealing) may still apply depending on the specific context and jurisdiction. However, commercial use typically weighs against a finding of fair use, especially when the original work is central to the new content. Video platforms have systems to remove content that infringes, including strike systems, demonetisation, or other sanctions. A legitimate debate exists about whether platforms overcautiously remove content due to concerns about being sued for secondary liability. This rapidly growing digital sector now intersects with copyright and trademark laws in many ways that are still evolving. As it operates globally, the lack of harmonised rules on online misuse and secondary liability makes the rules different across jurisdictions.

IP and AI are another huge area creating controversies in patents and copyright. AI creation, fair use and LLM training[21] using copyrighted materials are the subject of many lawsuits all over the world and debates about whether and how copyright laws should address it. Patent ownership and AI-generated inventions are two of the major patent controversies. Add to that the ability to create infringements using AI, such as deepfakes and a whole new set of rules will likely be needed in the coming years.

In another sense, AI can benefit IP because many IP creation processes, from creation and design to design-around[22], to the search and registration systems, are all large dataset analysis exercises. These are currently performed by humans according to processes, and most will almost certainly be replaced by AI, perhaps with human oversight.

Blockchain and cryptocurrencies also have applications in AI. There are companies now offering copyright deposit and management services using blockchain processes to record them. This automates the large volume and expensive problem of protecting millions of copyrights every year in every country. Licensing IP through blockchain-based smart contracts[23] enables low-cost automated royalty solutions and is creating a new micro-licensing industry. Content creators and other digital asset owners can

[21] Teaching an AI Large Language Model (LLM) to understand and generate human-like text involves feeding the model massive amounts of text data and adjusting its internal parameters (weights and biases) through a process called machine learning, specifically deep learning.

[22] Design-around refers to the process of creating something similar to but without copying existing IP.

[23] A smart contract is a self-executing agreement where the terms of the contract are directly written into code and stored on a blockchain.

tokenise[24] their works and issue micro-licenses for their use, enabling granular control over rights and automated royalty distribution.

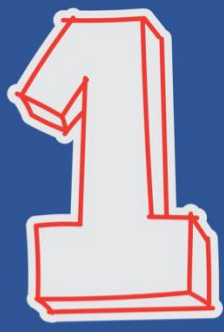
NFTs (Non-Fungible Tokens) are unique digital assets that represent ownership of a specific item or piece of content, such as art, music, videos, or collectables, with their ownership and authenticity recorded and secured on a blockchain. This is a new industry, which is growing as Virtual Reality and Augmented Reality, and the metaverse expands. Digital worlds, from gaming to virtual worlds, will have a host of IP issues. Copyright and trademark conflicts already exist. Hermes objected to NFTs of its Birken bags[25], and fashion retailer Mango faced legal objections after VEGAP, a Spanish collective society for artists, objected to digital adaptations of artists' works for metaverse display[26]. As the digital world grows, the commercial use and copying of others' IP will increase rapidly.

[24] Tokenize means to represent something real or abstract as a digital token on a blockchain ledger.

[25] https://www.reuters.com/business/hermes-wins-permanent-ban-metabirkin-nft-sales-us-lawsuit-2023-06-23/

[26] https://intellectual-property-helpdesk.ec.europa.eu/news-events/news/mango-prevails-court-supports-nft-art-exhibition-metaverse-general-court-upholds-yannick-noahs-tm-2024-02-15_en

Summary of Chapter 7: Emerging Technologies & IP



UGC IP Management
Social media content creators face challenges in managing their IP, including accidental infringement and navigating fair use, while platforms grapple with secondary liability and content removal systems.

AI and IP Controversies
AI generates significant legal debates regarding copyright (AI creation, fair use, LLM training on copyrighted material) and patent law (ownership of AI-generated inventions).

AI's IP Efficiency Benefits
AI can streamline IP processes like creation, design-around, and search/registration, potentially improving efficiency with human oversight.

Summary of Chapter 7: Emerging Technologies & IP

Blockchain for IP Automation
Blockchain and smart contracts enable automated copyright deposit, low-cost royalty solutions, and a new micro-licensing industry for digital assets.

NFTs and Metaverse IP Conflicts
Non-Fungible Tokens (NFTs) and the expanding metaverse (VR/AR) introduce new IP conflicts, particularly concerning copyright and trademark infringement in virtual environments.

Global Harmonisation Gap
The borderless nature of these emerging digital sectors highlights the critical need for harmonised international rules on online misuse and secondary liability.

8. IP and Business Strategy

Most digital businesses and even traditional businesses operating in the digital era depend on intangible assets and IP today. Creators, content owners, branded goods and services businesses, inventors and designers all need to learn about how IP works in the digital economy. Part of the reason this is so critical is that it is changing rapidly. Few in business foresaw the rise in AI, and even fewer can predict how it will impact the world. IP, more than any other business asset, precisely because it is intangible in nature, will be a key driver of the digital economy. Not only is it much easier to create new IP, but it is also becoming easier to exploit and commercialise it. And it is becoming easier to copy others. Additionally, more and more industries are operating across borders, making the old national concepts of IP increasingly outdated and becoming barriers.

Music is a great example. In the last century, recorded music was hard to produce, rare, and sold as physical goods on records and CDs; that was how artists made money, with live music as a promotional afterthought and cost. Today, music is produced in huge volumes and has become nearly free; artists fight with streaming platforms for royalties, with only successful ones making large incomes. Artists must now perform, manage social media channels (generating advertising and endorsement fees) and sell merchandise. The digital era has fundamentally disrupted the traditional music business model, shifting revenue away from physical sales toward live performances, online engagement, and alternative monetisation streams.

Design, media, entertainment, professional services and education are similarly being transformed. Copyright and trade secrets, including proprietary data, now account for the vast majority of value in these sectors.

Many traditional industries and business sectors will be revolutionised by AI, Web 3.0

and the Internet of Things. Medical diagnosis, drug discovery, personalised treatment, medical imaging analysis, robotic surgery, and patient monitoring are all now changing due to the use of data, AI, software and digital systems. Industrial and household devices use sensors to collect data and will soon think for themselves (such as automatically ordering spare parts when needed, or reminding the owner to buy food, in the case of a fridge).

Multi-national companies, mid-sized companies, and small businesses have, until now taken different approaches to IP protection. Most IP management software was built for MNCs. But now small businesses, start-ups, and digital companies own and commercialise large IP portfolios. New digital IP tools will be needed to log, capture and protect IP. Traditional registration systems will need to adapt, speed up and automate. The concept of manual comparison and examination will become obsolete, so IP offices must adapt fast. Tools for licensing, IP contracts and automated payment with fintech tools will become the norm for smaller businesses. Those that are fast will have advantages over larger, slower competitors.

Online copying and infringement are a problem today because of the volume and cross-border nature, whether copyright files or counterfeit goods are sold on e-commerce. Cybercrime is increasingly connected to IP theft, from phishing emails to deepfake social media posts.

New rules are urgently needed in regions like ASEAN to protect its consumers and creators. Technology solutions to detect infringements will emerge, and AI tools will predict patterns of infringement. The first AI dispute predictors in IP are being created to indicate likely outcomes

Competition from other countries is now the norm in the digital world. ASEAN creators need open markets in the region and beyond to become global successes.

A key issue for SMEs is the costs of IP activities, from registration to contracts to enforcement. New solutions addressing this are starting to appear, but not enough yet exist since most IP services vendors target larger corporations. SMEs can often apply directly to IP offices or get help from their local IP office for IP protection. There are also some SME helpdesks to use. Over time, online IP filing, IP record management, and brand protection services will increasingly be tailored to SMEs.

Below is a checklist of many strategies for SMEs to follow:

A. Protecting IP:

- Identify and categorise digital IP: recognise all digital assets that qualify for IP protection, including software code, website design, databases, digital content (text, images, videos, audio), algorithms, business methods implemented digitally, and brand names/logos used online.
- Register trademarks and domain names: apply for trademarks for brand names, logos, and slogans used in the digital space. Register relevant domain names and consider variations to prevent cybersquatting.
- Use copyright for digital content: understand that original digital creative works (code, text, graphics, videos, music) are automatically protected by copyright.
- Explore patent protection for digital inventions: if a digital product, process, or software involves a novel and non-obvious technical invention, explore patent options (utility or design patents, depending on the nature of the innovation).
- Implement trade secret protection for valuable digital information not suitable for patenting (e.g., algorithms, customer data handling processes), implement strong confidentiality tools, access controls, employee agreements, and data encryption.
- Use watermarking and digital rights management (DRM) tools: for digital content like images, videos, and software, employ watermarking to indicate ownership and DRM technologies to control access, copying, and distribution.

- Secure databases and digital assets: Implement strong cybersecurity measures to protect valuable digital IP from unauthorised access, copying, and theft. This includes firewalls, intrusion detection systems, and access controls.
- Clearly define IP ownership in contracts: ensure that contracts with employees, consultants, and partners clearly define ownership of any digital IP created during the collaboration.

B. Commercialising IP:

- Incorporate IP into digital products and services: leverage unique IP to differentiate product and service offerings and create a competitive advantage in the online marketplace.
- License IP: grant licenses to others to use digital IP (e.g., software components, digital content) for a fee or royalty, expanding revenue streams.
- Offer software as a service (SaaS) or use a content subscription model: monetize software or digital content through subscription models, leveraging the underlying IP.
- Integrate IP into online marketing and branding: Use trademarks and copyrighted content to build a strong online brand presence and attract customers.
- Develop APIs and integration tools: If you have valuable digital functionalities, create APIs and tools that allow other businesses to integrate with a technology, potentially through licensing agreements.
- Tokenise digital assets (e.g., NFTs): for unique digital creations, explore tokenisation via NFTs to establish ownership, scarcity, and facilitate new forms of commercialisation (e.g., selling digital art, collectables).
- Utilise affiliate marketing: enable others to promote digital products or services that incorporate IP, paying them a commission on sales.
- Data monetisation: If you possess unique and valuable digital data (while respecting personal data privacy rules), explore opportunities for anonymised data sharing or analysis services.

C. Enforcing IP:

- Monitor online infringement: regularly monitor online platforms, marketplaces, social media, and websites for unauthorised use of IP (e.g., counterfeit products, copyright infringement, trademark violations).
- Implement website terms of use and copyright notices: Clearly state IP rights and usage restrictions on websites and digital platforms.

- Send warning letters: When infringement is detected, promptly send formal cease and desist letters demanding that the infringing activity stop, if necessary, through law firms.
- Utilise online dispute resolution mechanisms: Many online platforms have their own dispute resolution processes for IP infringement (e.g., takedown requests on marketplaces, social media content removal).
- Engage IP attorneys specialising in digital IP: For significant or persistent infringement, consult with lawyers experienced in digital IP law to explore legal options like lawsuits or takedowns.
- Document and preserve evidence of infringement: Carefully document all instances of suspected infringement, including screenshots, URLs, and dates.
- Adopt digital watermarking with tracking capabilities: Some advanced watermarking technologies can track the unauthorised distribution of digital content.
- Collaborate with industry associations: Join relevant industry associations that may offer resources or collective action against online IP infringement.
- Educate customers about IP infringement: inform customers about how to identify genuine products and the risks of purchasing counterfeit digital or physical goods.
- Consider blockchain-based IP systems: explore emerging blockchain solutions that aim to provide secure and transparent records of IP ownership, potentially aiding in enforcement.

Summary of Chapter 8: IP and Business Strategy

IP as Core Digital Asset
Intangible assets and IP are now fundamental drivers of value for all businesses in the digital economy, especially with the rapid evolution of AI, Web 3.0, and the Internet of Things.

Disruption of Traditional Models
Digitalisation fundamentally alters industry business models (e.g., music, media, professional services), shifting revenue streams towards digital content, data, and online engagement.

New IP Management & Automation
The increasing volume of IP, particularly for SMEs and digital companies, necessitates new digital tools for IP logging, capture, protection, and automated licensing solutions (e.g., via fintech and blockchain).

Escalating Digital Infringement
Online copying, counterfeiting, and IP theft are massive, cross-border challenges, increasingly linked to cybercrime like phishing and deepfakes.

AI for IP Enforcement & Prediction
Emerging technology solutions, including AI, are being developed to detect infringements, predict patterns, and even forecast dispute outcomes, indicating a shift towards automated enforcement.

Summary of Chapter 8: IP and Business Strategy

SME-Specific IP Challenges
SMEs face unique cost and resource challenges in IP activities, requiring tailored online filing, record management, and brand protection services, often supported by local IP offices.

Strategic IP Protection
Businesses must proactively identify and categorise digital IP (software, data, algorithms, online brands), implement robust protection measures (registration, trade secrets, cybersecurity, DRM), and clearly define IP ownership in contracts.

Digital IP Commercialisation
Strategies for monetising digital IP include product differentiation, licensing (including micro-licensing), SaaS models, API development, tokenisation (NFTs), and data monetisation.

Proactive Digital Enforcement
Effective online IP enforcement requires continuous monitoring of platforms, clear website terms, utilising platform dispute mechanisms, and meticulous documentation of infringement.

Need for Harmonised Rules
The global and rapidly changing nature of digital IP issues highlights an urgent need for new and harmonised international rules to protect creators and consumers.

9. Harmonisation of IP Rights in the Digital Era: Future Directions and Policy Recommendations

ASEAN is de facto operating a borderless digital market for IP-backed trade. Digital content, brands, and all kinds of goods and services operate in the digital environment without heed for national borders. UGC, AI and the blockchain are driving entirely new non-national/virtual markets. Many ASEAN businesses operate in these business environments. This fundamental nature of the digital era raises the question of harmonising IP. IP was last substantially harmonised by the TRIPS agreement in the 1990s, with a number of WIPO treaties that also followed. But these were well before the digital era.

A number of multilateral and bilateral agreements in the 21st century have covered a few elements, mainly at a very general level. For example, the Regional Comprehensive Economic Partnership Agreement (RCEP), which ASEAN member states have subscribed to, requires countries to apply criminal enforcement for trademarks and copyright to the digital environment. However, these agreements generally lack detailed provisions on implementation. There is no single defined set of harmonisation steps for the digital world. The European Union has introduced several instruments that serve as useful references for digital IP regulation. However, even within the EU, not all digital IP-related areas—such as criminal enforcement of IP rights - are fully harmonised.

There is potentially a unique opportunity for ASEAN to create a single market for the operation of IP in the digital era. At present, digital businesses and operators trade across markets but operate in differing and non-harmonised legal and IP systems (insofar as they apply to the digital world). Many of the TRIPS-era harmonisation efforts, which focused on traditional or physical-world IP contexts, offer limited relevance or utility for digital businesses today. The intent of ASEAN to create a huge digital market will not easily be achieved with different rules for the use, protection and enforcement of digital IP.

Some of the areas that could be addressed are set out below. A more detailed analysis may be needed. In many cases, simply general statements of harmonisation are not helpful in complex new technology markets. Detailed implementation plans or interpretations are often needed.

A. Copyright

The use of registration systems in individual AMSs could be replaced by a single ASEAN online and automatic deposit system for copyright, covering all countries. This would encourage far wider use, especially by SMEs, especially if it could be integrated with a commercial database app allowing a business to manage their copyrights.

Copyright secondary ISP liability varies between civil and common law countries, and with different obligations and penalties between AMSs. A single clear definition along with what constitutes safe harbour, knowledge and notice, and when civil or criminal

penalties apply would enable ASEAN content owners to have more consistent practice in the region.

Consistent protection in copyright laws of DRM and TPMs to prevent circumvention is required by RCEP Art 11.14, but in practice, this is not applied across ASEAN.

Fair Use is another area where variations in application can exist, so a clear and detailed statement of application would help the implementation of RECP Art. 11.18 on fair use. This should cover all the new digital uses to help balance digital creators' and content owners' rights in creating new content.

ASEAN could explore whether to establish a right in copyright in databases or a sui generis right.

Copyright laws in ASEAN need to be consistently updated to address the evolving impact of AI, particularly in 4 key areas: (1) creation by or with AI tools; (2) fair use and AI-generated works; (3) the permissibility of using third-party content for training large language models (LLMs) and (4) the legal treatment of LLM outputs that may infringe existing rights. If ASEAN Member States amend their laws independently and inconsistently, it may create new barriers to digital trade. In areas like LLM training, fragmented national laws may pose a greater challenge than a lack of regulation, since cloud-based model training is inherently cross-border.

B. Trademarks

Better digital searching and more open registration systems would help businesses in ASEAN, as would lowering the cost and speeding up registration.

Urgent harmonisation of trademark secondary ISP liability is needed. Multiple different ministries in different countries have led to different, often conflicting ISP liability laws around the region. The urgent harmonisation requirement is to have consistent trademark secondary ISP liability definitions (across both civil and common law countries) and with consistent obligations and penalties across all AMSs. A single clear definition along with what constitutes safe harbour, knowledge and notice, and when civil or criminal penalties apply would enable ASEAN trademark owners and e-commerce platforms to have certainty and consistent practice across the region. One option which is gathering momentum is the use of Codes of Conduct for IP owners and e-commerce marketplaces to agree on standards and processes for notice and takedown timings, KPIs, repeat offenders, identity disclosure, and joint legal actions.

C. Trade Secrets

Trade secrets rules vary by country because the core WTO TRIPS rules are provisions are high-level and limited in scope. The RECP framework for trade secret protection similarly outlines only general obligations. Common law countries like Malaysia and Singapore use 'confidential information' rules, and civil law countries like Thailand, Indonesia, Philippines and Viet Nam treat trade secrets as a more solid form of IP with more active protections. Harmonisation of rules would help cross-border trade. As an example, the UK, when it was an EU member, was required to enact a trade secrets

law to supplement its common law confidential information rules, to enable European harmonisation.

Some AMSs treat trade secret theft as a civil law issue, and others as a criminal breach.

The protection of know-how could be considered, whether and how it should be treated in ASEAN. In practice, it appears in commercial contracts, so businesses are using it as an intangible asset without legal protection in many countries.

Personal data definitions need to be clarified as regards business data. For example, is an online trader's data personal or business data? In some countries, merchant e-commerce data related to online business transactions is generally considered business data. In many AMSs, the law is unclear and needs harmonisation and/or clarification; at present, this enables infringers to hide their identity under data privacy laws to avoid detection.

The intersection of data and trade secrets needs more study to understand how this might need harmonisation in future.

D. Designs

Many designers across ASEAN face challenges accessing existing design protection systems, which are often perceived as too slow, costly, or complex for fast-moving industries. ASEAN could explore an unregistered design system for short, fast product designs, e.g. 3-5 years. It could explore an instant low-cost regional deposit system, alternatively, for say 5 years. Or preferably both, because in reality, designers are not one industry but many. The fact is that millions of IPRs are being lost in ASEAN every year because no rights are created by the AMS design laws. Meanwhile, in other regions, their competitors build up huge IP portfolios for little or no cost. ASEAN designers are therefore at a huge disadvantage globally.

There is no consistent practice for whether designs in the online environment are protected: GUIs, icons, UI & UXs, VR & AR designs, which are entirely virtual. AI-created designs are now commonplace but are currently not protected in ASEAN. The same harmonisations for secondary ISP liability for online companies allowing design infringement are needed as for trademarks and copyright.

E. Patents

Should patent eligibility be widened in AMSs to include software and business methods (especially online), and perhaps new tech such as algorithms and data analysis techniques? Consistency in how software and business methods are treated under patent law could benefit the region, especially as Indonesia has moved toward a broader interpretation aligned with U.S. practice. Expanding patent eligibility may open avenues for greater protection and commercialisation of digital innovation, particularly in fields such as data analytics, algorithmic processes, and online business models. At the very least, ASEAN could collectively explore whether a broader scope

of patentable subject matter might contribute to regional tech and industrial development.

ASEAN patent laws do not presently accept non-human inventors; however, many inventions now use AI at least partially. What happens to these patents now being filed?

Integrating AI tools into the patent examination process to assist with prior art searches, classification, and document analysis could significantly reduce costs and time. This would be especially valuable for ASEAN inventors and SMEs, who often lack the substantial resources of foreign MNCs. Full automation may not be feasible, but augmenting human examiners with AI-powered systems is already being adopted in some countries and offers a practical pathway to improve efficiency and accessibility.

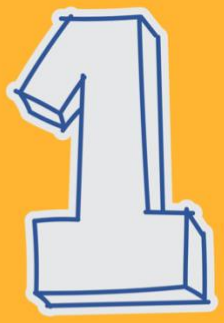
F. Unfair competition and passing off

Despite an obligation to apply unfair competition rules in the Paris Convention and TRIPS, some countries do not, and many apply them differently. Common law countries use passing off, which can be expensive to prove. A clear, detailed set of rules on how business IP unfair competition should be protected across the region would benefit most ASEAN businesses, for whom the costs of building up large, registered rights portfolios can be prohibitive. The types of IP area this refers to include slavish product and service trade dress imitation and comparative advertising; often hard or impossible to protect in some AMSs.

Rights of Publicity a.k.a. image or personality rights are not harmonised, requiring further study and a clear ASEAN plan for how to enable cross-market protection either through copyright law expansion or a sui generis right. AI deepfakes and other infractions are rapidly increasing in ASEAN.

G. Geographical Indications

GI producers now have to learn to trade in the digital era, using e-commerce and e-marketing. They face online misuse of their GIs, fake products and digital marketing by competitors that might misuse elements of their product or reputation. They must register domain names, URLs, social media handles and may have to prevent others from trying to register them. This is often a challenge as GI producers are usually associated with limited funding and are sometimes based in remote locations. To compete effectively, they need to develop expertise in digital IP protection. ASEAN could offer more support to them.



Summary of Chapter 9: Harmonisation of IP Rights in the Digital Era; Future Directions & Policy Recommendations

Urgent Need for Digital IP Harmonisation

ASEAN's borderless digital market (driven by UGC, AI, blockchain) necessitates harmonised IP rules beyond the outdated TRIPS agreement to foster digital trade and innovation.

Copyright Reforms

Recommendations include a single ASEAN online copyright deposit system, harmonised secondary ISP liability, consistent protection against DRM/TPM circumvention, clear fair use guidelines for digital content, potential sui generis rights for databases, and consistent updates for AI-related copyright issues (creation, fair use, LLM training/outputs).

Trademark Streamlining & Liability

Calls for better digital searching, faster/cheaper registration, and urgent harmonisation of secondary ISP liability for e-commerce platforms, potentially through Codes of Conduct.

Trade Secret Clarity

Harmonisation is needed for trade secret definitions (civil vs. criminal treatment), clarification of "know-how" protection, and clear distinctions between personal and business data for online traders.

Summary of Chapter 9: Harmonisation of IP Rights in the Digital Era; Future Directions & Policy Recommendations

Design Protection Evolution
Proposals include exploring unregistered design systems or instant low-cost regional deposit systems for fast-moving designs, consistent protection for virtual/AI-created designs, and harmonised secondary ISP liability for design infringement.

Patent Modernisation
Suggests widening patent eligibility to include software, business methods, and AI-related inventions, addressing AI inventorship, and integrating AI tools into patent examination for efficiency.

Unfair Competition & Publicity Rights
Advocates for clear, detailed regional rules against unfair competition (e.g., slavish imitation, comparative advertising) and a harmonised approach to publicity/image rights, especially concerning AI deepfakes.

Support for GI Producers
Recommends increased ASEAN support for Geographical Indication (GI) producers to navigate digital trade, combat online misuse, and secure digital identifiers.

10. Intellectual Property Symbols and Their Meanings

In the world of intellectual property, various symbols are used to indicate legal protection for different types of rights. Understanding these symbols helps businesses and creators safeguard their work effectively. Below is a quick summary table:

Symbol	IP Type	Purpose	Example Usage
©	Copyright	Protects creative works	© 2025 SME Productions
TM	Trademark (Unregistered)	Brand name/logo not yet registered	Team Wang™
®	Trademark (Registered)	Officially registered trademark	Nike®
Pat. Pending	Patent	Patent application filed but not yet granted	Pat. Pending - Invention XYZ
Patent No.	Patent	Officially granted patent	Patent No. 123456
Reg. Design No.	Industrial Design	Protects the appearance of a product	Reg. Design No.

These symbols play an essential role in intellectual property protection, ensuring that creators, businesses, and inventors receive recognition and legal rights for their work.

Glossary

Terminology	Description
Algorithm	A set of instructions for solving a problem or completing a task
Application Programming Interface (API)	A set of rules and protocols that allows different software applications to communicate with each other
Artificial Intelligence (AI)	The simulation of human intelligence processes by computer systems
ASEAN	Association of Southeast Asian Nations
Blockchain	A decentralised, digital ledger system that records transactions across multiple computers in a secure and transparent manner
Brand Equity	The value of a brand
Civil Law	A legal system based on written codes
Cloud Computing	The practice of using a network of remote servers hosted on the internet to store, manage, and process data, rather than a local server or a personal computer
Common Law	A legal system based on precedent and judicial decisions
Comparative Advertising	Advertising that compares a product or service to a competitor's
Confidential Information	Business information that offers a competitive edge and is kept secret
Copyright	A legal right granted to creators of original works, including literary, artistic, musical, and software
Counterfeiting	The production of imitation goods passed off as authentic
Cyberlocker	An online file storage service
Cybertheft	The theft of information through digital means
Data Aggregators	Companies that collect data from various sources
Data Breach	A security incident where sensitive, protected, or confidential data is copied, transmitted, viewed, stolen, or used by an individual unauthorised to do so
Deepfake	A manipulated video or audio clip that convincingly depicts someone saying or doing something they did not say or do

Designs	Protect aesthetic creations, usually physical objects but increasingly digital designs like user interfaces and digital icons
Digital Rights Management (DRM)	Technologies used by copyright holders to control access to and use of their digital content
Dropshipper	A seller who accepts customer orders but does not keep goods in stock
E-commerce	Commercial transactions conducted electronically on the Internet
Fair Use	The doctrine that allows limited use of copyrighted material without permission for purposes such as criticism, news reporting, teaching, and research
FRAND	FRAND licensing stands for Fair, Reasonable and Non-Discriminatory licensing
Geographical Indications	A name or sign used on products that have a specific geographical origin and possess qualities or a reputation that are due to that origin
Harmonisation	The process of aligning laws, regulations, and standards across different jurisdictions
Industrial Espionage	The practice of stealing trade secrets or other confidential information from a business competitor
Infringement	The unauthorised use of intellectual property rights such as copyrights, trademarks, and patents
Intangible Assets	Non-physical assets that provide value to a business, such as intellectual property, brand reputation, and goodwill
Intellectual Property (IP)	A category of property that includes intangible creations of the human intellect
Know-how	Practical knowledge, skills, and expertise that are not widely known or easily accessible
Licensing	Granting permission to use intellectual property rights under specific terms and conditions
Madrid System	An international system for registering trademarks
Metatags	Data that provides information about other data

Micro-licensing	Granular licensing of content for specific uses, enabling small revenue streams for creators
Nice Classification	An international classification of goods and services used for trademark registration
Non-Disclosure Agreement (NDA)	A legal contract that establishes a confidential relationship between parties
NFT	A non-fungible token is a unique digital asset, representing ownership of a digital or physical item
Originality	The quality of being new and not copied from something else
Passing Off	A common law tort that protects unregistered trademarks and prevents traders from misrepresenting their goods or services as those of another
Patent	An exclusive right granted for an invention
Patent Pools	Agreements between patent owners to license their patents collectively
Personal Data	Information relating to an identified or identifiable natural person
Phishing	A cyberattack that uses disguised email, websites, or other communication channels to trick individuals into revealing personal information
Piracy	The unauthorised reproduction or distribution of copyrighted material
PPH	Patent Prosecution Highway is an agreement between two or more patent offices that allows a faster examination process by sharing previous work done in another country
Quasi IP	Rights that are similar to intellectual property rights but not fully recognised or protected as such
Secondary Liability	The liability of a party who is not the primary infringer but contributes to or facilitates the infringement
Safe Harbour	Provisions that offer protection to online service providers from liability for copyright infringement by their users, provided they comply with certain conditions
Smart Contracts	Self-executing contracts with the terms of the agreement directly written into code

Social Media Handles	User-specific names used on social media platforms
Standards Essential Patents	Patents that are essential for complying with technical standards
Takedown Procedures	Processes for removing infringing content from online platforms
Technological Protection Measures (TPMs)	Technological tools used to protect copyrighted works
Trade Dress	The overall appearance and image of a product or service that identifies its source
Trademark	A symbol, design, or phrase legally registered to represent a company or product
Trade Secret Databases	Digital collections of trade secrets
Unfair Competition	Business practices that deceive or exploit consumers or competitors
Unregistered Designs	Design rights that exist without formal registration
User Generated Content (UGC)	Content created by users of a platform or service
URLs	Website addresses
Virtual Reality (VR)	The use of computer technology to create a simulated environment
World Intellectual Property Organization (WIPO)	A global organisation dedicated to promoting and protecting intellectual property