MODULE 6: INTELLECTUAL PROPERTY & COPYRIGHT

Intellectual property and copyright are legal concepts that protect the rights of creators and owners of original works, such as books, music, software, and inventions. They grant them exclusive control over how their works are used, distributed, and modified by others.

Digital rights management (DRM) is a technology that restricts the access and use of digital content, such as e-books, movies, and games. DRM aims to prevent unauthorized copying, sharing, or modifying of protected content. However, DRM also raises ethical and technical issues, such as limiting the fair use rights of consumers, interfering with the interoperability of devices and platforms, and creating security vulnerabilities.

Open-source software licensing is a type of software licensing that allows anyone to access, use, modify, and distribute the source code of a software program. Open-source software is often developed collaboratively by a community of developers who share a common vision and values. Open-source software licensing promotes innovation, transparency, and freedom of choice for users and developers.

6.1. INTELLECTUAL PROPERTY & COPYRIGHT

WHAT IS INTELLECTUAL PROPERTY?

Intellectual property (IP) is any creation of the mind that has commercial value. It includes inventions, designs, artistic works, symbols, names and images. IP can be protected by law through patents, trademarks, copyrights and trade secrets.

WHY IS IP IMPORTANT FOR CYBERSECURITY?

IP is one of the most valuable assets of any business. It gives a competitive edge, attracts customers and investors, and generates revenue. However, IP is also vulnerable to cyberattacks, theft, misuse, and infringement. Cybersecurity is the process of protecting IP from unauthorized access, use, disclosure, modification, or destruction.

HOW TO PROTECT IP FROM CYBER THREATS?

Here are some tips to keep IP safe from cyber threats:

- Identify your IP assets and their value. Conduct an IP audit to find out what IP you have, who owns it, where it is stored and how it is used.
- Implement appropriate security measures for your IP assets. Use encryption, authentication, access control, backup and recovery systems to safeguard your IP data.

- Educate your employees and partners about IP protection. Provide training and awareness programs on IP policies, procedures and best practices. Monitor and enforce compliance with IP rules and agreements.
- Register your IP rights where possible. Apply for patents, trademarks or copyrights to secure legal protection for your IP assets. Use notices and labels to indicate your ownership and rights.
- Monitor your IP environment and respond to incidents. Use tools and services to detect and prevent IP breaches, such as firewalls, antivirus software, intrusion detection systems and threat intelligence. Report and resolve any IP issues as soon as possible.

THE ESSENCE OF INTELLECTUAL PROPERTY & COPYRIGHT

IP is the intangible creation of the human mind, such as inventions, artistic works, designs, symbols, names and images. IP is protected by laws that grant exclusive rights to the creators or owners of IP, such as patents, trademarks, designs and copyright.

WHY IP MATTERS IN CYBERSPACE

Cyberspace is the virtual environment where people communicate and interact through computer networks. Cyberspace is becoming a hub for IP infringement, as it is easy to copy, distribute and modify digital content without the owner's consent. IP infringement can harm the owner's reputation, revenue, and competitive advantage. It can also expose the infringer to legal risks and liabilities.

Some common examples of IP infringement in cyberspace are:

- Using another person's logo, brand name or domain name without permission
- Copying or downloading another person's software, music, video, e-book or game without a licence
- Making a profit by using another person's creation without paying royalties or fees
- Modifying or adapting another person's work without authorisation
- Selling counterfeit or pirated goods online

HOW TO PROTECT YOUR IP IN CYBERSPACE

Take the following steps to protect your IP in cyberspace:

- **Identify and audit your IP assets**. Know what IP you have, who owns it, how it is used and how it is protected.
- **Register your IP rights**. Apply for patents, trademarks and designs to secure your exclusive rights in Australia and overseas
- **Monitor your IP online**. Use tools and services to detect and prevent unauthorised use of your IP on the internet.

- **Enforce your IP rights**. Act against infringers by sending cease and desist letters, filing complaints or initiating legal proceedings.
- **Commercialise your IP**. Negotiate and draft licensing, technology transfer, distribution and content agreements to generate income from your IP

WHERE TO FIND MORE INFORMATION

Visit the following websites:

- [Intellectual Property Lawyers | Gilbert + Tobin](https://www.gtlaw.com.au/expertise/intellectual-property): A leading Australian law firm that provides advice on all aspects of IP law
- [Intellectual Property, Technology & Cyber Security | HopgoodGanim] (https://www.hopgoodganim.com.au/page/expertise/services/intellectual-property-technology-cybersecurity): A market-leading team of lawyers with scientific or technical qualifications in IP, technology and cyber security
- [Intellectual Property in Cyberspace | GeeksforGeeks] (https://www.geeksforgeeks.org/intellectual-property-in-cyberspace/): A website that explains the basics of IP in cyberspace with examples
- [Intellectual Property Crime | Australian Federal Police] (https://www.afp.gov.au/what-we-do/crime-types/intellectual-property-crime): A website that provides information on how to report IP crime and what actions the AFP can take

CYBERSECURITY RISKS

One of the main challenges of digital transformation is ensuring the security of your data and software systems. Data breaches are becoming more frequent and costly, exposing sensitive information, damaging reputations and causing legal liabilities.

According to a report by Norton Rose Fulbright, there were 4,100 publicly disclosed data breaches in 2022 alone, comprising some 22 billion records that were exposed. Moreover, software systems are becoming more complex and vulnerable, especially with the rise of artificial intelligence and generative AI, which can create realistic but fake content that can deceive or manipulate users.

Therefore, it is important to adopt a proactive and comprehensive approach to cybersecurity, that includes:

- Developing a framework that aligns your technology strategy with your business goals and risk appetite.
- Implementing zero trust architectures that assume all systems can or will be compromised and require continuous verification of users, devices and data.

- Applying encryption, authentication and access control measures to protect your data at rest and in transit.
- Monitoring and auditing your systems for any anomalies or suspicious activities.
- Updating and patching your software regularly to fix any vulnerabilities or bugs.
- Educating and training your employees and customers on cybersecurity best practices and awareness

PRIVACY RISKS

Another challenge of digital transformation is respecting the privacy rights of your customers, employees and partners. Privacy laws are becoming more stringent and diverse across jurisdictions, requiring you to comply with various rules and regulations on how you collect, use, store and share personal information. For example, the General Data Protection Regulation (GDPR) in the European Union imposes strict obligations on data controllers and processors, such as obtaining consent, providing transparency, ensuring data minimization and enabling data portability. Failing to comply with privacy laws can result in hefty fines, lawsuits and reputational damage. Therefore, you need to adopt a privacy-by-design approach that incorporates privacy principles into every stage of your digital transformation process, such as:

- Conducting privacy impact assessments to identify and mitigate any potential privacy risks or harms.
- Implementing privacy-enhancing technologies that anonymize, pseudonymize or encrypt personal data.
- Establishing privacy policies and notices that inform your data subjects about their rights and choices.
- Obtaining valid and informed consent from your data subjects before processing their personal data
- Responding to data subject requests to access, correct or delete their personal data.
- Reporting any data breaches or incidents to the relevant authorities and data subjects within the prescribed time frames.

INTELLECTUAL PROPERTY RIGHTS

Finally, one of the most important aspects of digital transformation is protecting your intellectual property rights. Intellectual property rights are the legal rights that grant you exclusive ownership and control over your creations, such as inventions, designs, trademarks, logos, slogans, software code, content etc. Intellectual property rights are essential for fostering innovation, competitiveness, and differentiation in the digital economy. However, digital transformation also poses new threats to your intellectual property rights, such as:

- Copying or stealing your software code or content by hackers or competitors.
- Infringing or violating your patents, trademarks or copyrights by using them without authorization or paying royalties.
- Diluting or tarnishing your brand image or reputation by creating confusingly similar or disparaging products or services.
- Challenging or invalidating your intellectual property rights by claiming prior art or public domain status.

Therefore, you need to adopt a strategic and proactive approach to intellectual property protection that includes:

- Registering your intellectual property rights with the relevant authorities and agencies.
- Enforcing your intellectual property rights against any infringers or violators through legal action or alternative dispute resolution.
- Licensing your intellectual property rights to others for mutual benefit or collaboration.
- Monitoring the market for any potential infringements or violations of your intellectual property rights.
- Updating your intellectual property portfolio to reflect any changes or improvements in your products or services.

Digital transformation comes with significant risks that can jeopardize your cybersecurity, privacy and intellectual property rights.

NAVIGATING THE AUSTRALIAN COPYRIGHT ACT

WHAT IS COPYRIGHT?

Copyright is a legal right that gives the creator of an original work the exclusive right to control how it is used, reproduced, communicated, or performed. It covers a wide range of works, such as books, music, films, software, databases, artworks, photographs and more. It also covers some types of online content, such as websites, blogs, podcasts, and social media posts.

WHY IS IT IMPORTANT?

Protecting your intellectual property is important for many reasons. It can help you:

- Reward your creativity and innovation.
- Prevent others from copying or exploiting your work without your permission.
- Generate income from licensing or selling your work.
- Enhance your reputation and brand recognition.
- Contribute to the cultural and economic development of society.

HOW DOES IT WORK IN AUSTRALIA?

Australia has a complex and evolving legal framework for copyright protection. Some of the key features are:

- You do not need to register or apply for copyright protection. It is automatic once you create an original work in a material form.
- You do not need to use the © symbol or any other notice to indicate your ownership. However, it may be helpful to do so as a reminder to others.
- You have the right to take legal action against anyone who infringes your copyright, such as by copying, distributing, displaying, or modifying your work without your consent.
- You may also have some moral rights, such as the right to be attributed as the author and the right to object to any derogatory treatment of your work.
- You may grant or transfer some or all your rights to others through a licence or an assignment agreement. You should always read and understand the terms and conditions before signing any contract.
- You may also allow others to use your work for free under certain circumstances, such as for fair dealing purposes (e.g. research, study, criticism, review, parody or satire) or under a Creative Commons licence.
- You must respect the rights of other creators when you use their works. You should always seek permission or rely on a valid exception before using any copyrighted material.
- You must comply with any applicable laws and regulations that affect your online activities, such as the Online Safety Act 2021 (Cth), the Surveillance Legislation Amendment (Identify and Disrupt) Act 2021 (Cth) and the Security Legislation Amendment (Critical Infrastructure) Bill 2021 (Cth). These laws aim to enhance the security and safety of online platforms and services and may impose new obligations and responsibilities on you as a user or provider.

DIGITAL RIGHTS MANAGEMENT (DRM) BALANCING RIGHTS & ACCESS

Digital Rights Management (DRM) is a set of technologies and protocols that protect digital content from unauthorized access, reproduction, and distribution. It is used to enforce copyright protection, licensing agreements, and access control for various forms of digital media, such as music, videos, eBooks, software, and more.

BENEFITS OF DRM

DRM provides a crucial layer of protection for content creators and owners. It helps them safeguard their intellectual property rights and prevent piracy or data breaches. By using DRM, content creators can:

- Control how their content is used, shared, or modified by authorized users.
- Generate revenue from their content by charging fees or subscriptions.
- Monitor the usage and performance of their content.
- Enhance the user experience by providing high-quality and secure content.

DRM also benefits content consumers by ensuring that they receive legitimate and quality content. It also helps them respect the rights and wishes of the content creators.

CHALLENGES OF DRM

DRM is not without its limitations. Some of the common issues that DRM faces are:

- Compatibility. Different platforms and devices may use different DRM systems, which can cause problems for users who want to access the same content across multiple devices
- Usability. DRM may impose restrictions or requirements that can affect the user experience, such as requiring internet connection, limiting the number of devices or downloads, or preventing offline access
- Privacy. DRM may collect personal or behavioural data from users, which can raise concerns about data protection and consent
- Fair use. DRM may interfere with the rights of users to use the content for legitimate purposes, such as education, research, criticism, or parody.

BEST PRACTICES FOR DRM

To balance the rights and access of both content creators and consumers, it is important to follow some best practices when implementing or using DRM solutions. Some of these are:

- Choose a suitable DRM system that meets your needs and goals. There are different types of DRM systems available, such as encryption-based, watermark-based, or fingerprint-based. You should consider factors such as cost, complexity, security level, compatibility, and scalability when selecting a DRM system.
- Use a multi-DRM strategy to protect your streams on all platforms with strict licensing rules. A good DRM vendor will allow you to do all the following to protect your streams:
- Prevent screen capture.
- Prevent downloading of the streams by using the strictest variants of the DRM available.
- Ensure a strict expiration date in the license beyond which the stream will be inaccessible.

- Provide the option to rotate the DRM keys during the live streams to frustrate hackers.
- Communicate clearly with your users about the terms and conditions of your DRM policy. You should inform them about what they can and cannot do with your content, how long they can access it, what data you collect from them, and how you protect their privacy.
- Respect the fair use rights of your users and allow them some flexibility in using your content for legitimate purposes. You should also provide them with options to contact you or request permission if they have any questions or issues with your DRM policy.
- Keep up to date with the latest developments and trends in DRM technology and legislation. You should monitor the changes in the market and the legal environment and adjust your DRM strategy accordingly.

OPEN SOURCE & LICENSING CONSIDERATIONS

OSS is software that uses publicly available source code that anyone can see, modify, and distribute. OSS can offer many benefits, such as affordability, flexibility, and quality, but it also comes with some risks and challenges that you need to be aware of.

TYPES OF OPEN-SOURCE LICENSES

One of the main challenges of using OSS is complying with the terms and conditions of the open-source licenses. These are legal agreements that specify what you can and cannot do with the OSS and its derivatives. There are two main types of open-source licenses: permissive and copyleft.

Permissive licenses are the more business-friendly ones, as they allow you to use, modify, and distribute the OSS for any purpose if you give proper attribution to the original authors. Some examples of permissive licenses are the MIT license, the Apache license, and the BSD license.

Copyleft licenses are the more restrictive ones, as they require you to share your modifications and derivatives under the same or compatible license as the original OSS. This means that if you use copyleft OSS in your proprietary software, you might have to disclose your source code and allow others to use it for free. Some examples of copyleft licenses are the GNU General Public License (GPL), the GNU Lesser General Public License (LGPL), and the Mozilla Public License (MPL).

RISKS AND BEST PRACTICES

Using OSS can introduce some risks to your cybersecurity projects, such as:

- **Excessive access**. Open access means that anyone can see and manipulate the source code, which creates opportunities for malicious actors to introduce vulnerabilities or backdoors.

- **Lack of verification**. There are no guarantees that the OSS is tested and reviewed by qualified experts, which can make it prone to errors and security flaws.
- **Lack of support**. Most OSS does not have dedicated support teams, which means that updates and patches may not be available or timely. This can leave your software exposed to known or unknown vulnerabilities.

To mitigate these risks, you should follow some best practices when using OSS, such as:

- **Conduct a thorough due diligence.** Before using any OSS, you should check its license type, terms, and conditions, and make sure they are compatible with your intended use and distribution. You should also check its reputation, quality, security, and maintenance status.
- **Use a software composition analysis tool**. This is a tool that can help you identify and manage the OSS components in your software. It can help you track their licenses, versions, dependencies, vulnerabilities, and compliance status.
- **Implement a security policy**. You should have a clear and consistent policy for using OSS in your projects. This policy should define the roles and responsibilities of your team members, the criteria for selecting OSS components, the processes for reviewing and updating them, and the procedures for reporting and resolving any issues.

Using OSS can be a great way to enhance your cybersecurity projects with high-quality software components. However, you need to be careful about the legal and security implications of using OSS. By following the types of open-source licenses, understanding their risks, and applying best practices, you can use OSS safely and effectively.

FAIR USE & FLEXIBILITY

WHAT IS FAIR USE AND FLEXIBILITY?

Fair use and flexibility are legal doctrines that allow the use of copyrighted material without permission or payment under certain circumstances. They are essential for promoting creativity, innovation, education, research, and public interest.

In the context of cybersecurity, fair use and flexibility can enable security professionals to access, analyse, test, and improve the security of digital systems and data. For example, fair use and flexibility can allow security researchers to reverse engineer software, conduct vulnerability assessments, disclose security flaws, and develop patches or workarounds.

WHY IS FAIR USE AND FLEXIBILITY IMPORTANT FOR CYBERSECURITY?

Fair use and flexibility are important for cybersecurity because they can help:

- Enhance the security posture of organizations and individuals by allowing them to identify and mitigate risks, protect their assets, and respond to incidents.
- Foster a culture of security awareness and collaboration by allowing security professionals to share their findings, insights, and best practices with others.
- Support the development of new security technologies and solutions by allowing security professionals to experiment with different methods, tools, and techniques.
- Advance the state of the art in cybersecurity by allowing security professionals to contribute to the scientific knowledge and innovation in the field.

WHAT ARE THE CHALLENGES AND RISKS OF FAIR USE AND FLEXIBILITY IN CYBERSECURITY?

Fair use and flexibility are not absolute rights. They are subject to limitations and exceptions depending on the jurisdiction, context, purpose, nature, amount, and effect of the use. They are also balanced against the rights and interests of the copyright holders.

Therefore, fair use and flexibility in cybersecurity can pose some challenges and risks, such as:

- **Legal uncertainty and liability**. Security professionals may face legal challenges or lawsuits from copyright holders who claim that their use of the material was unauthorized or infringing. Security professionals may also face criminal charges or penalties if their use of the material violates other laws or regulations.
- **Ethical dilemmas and conflicts**. Security professionals may encounter ethical dilemmas or conflicts when deciding whether, how, when, and with whom to use or share the material. Security professionals may also face criticism or backlash from their peers, employers, clients, or the public for their use or disclosure of the material.
- **Operational difficulties and costs**. Security professionals may face operational difficulties or costs when obtaining, storing, processing, or transmitting the material. Security professionals may also face technical challenges or limitations when using or modifying the material.

DIGITAL COMMONS & COLLABORATIVE CREATION

WHAT ARE DIGITAL COMMONS AND COLLABORATIVE CREATION?

Digital commons are resources that are shared by a community of users online, such as open-source software, open data, open educational resources, and

creative commons licenses. Collaborative creation is the process of producing digital content or knowledge by working together with others, such as through wikis, blogs, podcasts, or social media platforms.

WHY ARE THEY IMPORTANT?

Digital commons and collaborative creation can foster innovation, creativity, education, and social inclusion. They can also reduce costs, increase efficiency, and improve quality of digital products and services. For example, Wikipedia is a collaborative encyclopedia that anyone can edit, which provides free and reliable information to millions of users around the world. Linux is an open-source operating system that powers many servers, devices, and applications, which benefits from the contributions of thousands of developers and users.

WHAT ARE THE CYBERSECURITY RISKS?

However, digital commons and collaborative creation also pose cybersecurity risks that need to be addressed. These risks include:

- Unauthorized access or modification of digital resources by hackers, competitors, or malicious insiders
- Theft or leakage of sensitive or personal data by cybercriminals, spies, or whistleblowers
- Infringement or violation of intellectual property rights by copycats, pirates, or trolls
- Disruption or sabotage of digital services or infrastructure by activists, terrorists, or state actors
- Misinformation or manipulation of digital content or users by propagandists, fraudsters, or bots

HOW TO PROTECT THEM?

These include:

- Implementing strong authentication and authorization mechanisms to verify the identity and access rights of users and contributors.
- Encrypting data in transit and at rest to prevent unauthorized interception or extraction.
- Applying digital signatures or watermarks to prove the origin and integrity of digital resources.
- Monitoring and auditing the activity and performance of digital systems and networks to detect and respond to anomalies or incidents.
- Educating and engaging the community of users and contributors to raise awareness and foster trust and cooperation.

WHERE TO LEARN MORE?

If you want to learn more about digital commons and collaborative creation, you can visit the following websites:

[Rebuilding digital trust for a cyber-inclusive future | World Economic Forum] (https://www.weforum.org/agenda/2021/11/rebuilding-digital-trust-for-a-cyber-inclusive-future/)

[Cybersecurity, cybercrime and cybersafety: a quick guide to key internet links – Parliament of Australia] (https://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/rp/rp1819/Quick_Guides/CybersecurityCybercrimeCybersafety)

[The Digital World Is Changing Rapidly. Your Cybersecurity Needs to Keep Up.] (https://hbr.org/2023/05/the-digital-world-is-changing-rapidly-your-cybersecurity-needs-to-keep-up)

6.2. DIGITAL RIGHTS MANAGEMENT

Digital rights management (DRM) is a term that encompasses the methods and technologies used to protect and control the access and use of digital content, such as books, music, videos, software, and data. DRM aims to prevent unauthorized copying, sharing, modification, or distribution of digital content by applying various restrictions and encryption techniques to the content or the devices that can access it.

WHY IS DRM IMPORTANT?

DRM is important for several reasons. First, it helps content creators and owners to safeguard their intellectual property rights and their financial and creative investments in their work. By limiting what users can do with their content, DRM ensures that content creators and owners can benefit from their work and prevent others from exploiting it without permission or compensation.

Second, DRM helps users to respect the legal and ethical boundaries of using digital content. By complying with the terms and conditions of DRM, users can avoid infringing on the rights of content creators and owners and avoid potential legal consequences or penalties.

Third, DRM helps to maintain the quality and integrity of digital content. By preventing unauthorized modification or alteration of digital content, DRM ensures that users can access and enjoy the original and authentic version of the content as intended by the content creators and owners.

HOW DOES DRM WORK?

DRM works by using various technologies and tools to implement different types of restrictions and encryption on digital content. Some of the common DRM methods are:

Copy protection. This method prevents or limits users from making copies of digital content or transferring it to other devices or platforms.

Access control. This method requires users to have a valid license, password, or authentication to access digital content or certain features or functions of it.

Expiration. This method sets a time limit, or several uses for accessing digital content, after which the content becomes inaccessible or unusable.

Geolocation. This method restricts access to digital content based on the user's location or IP address.

Watermarking. This method embeds a visible or invisible mark on digital content that identifies the source or owner of the content.

Encryption. This method scrambles the data of digital content using a secret key that only authorized users can decrypt.

WHAT ARE SOME EXAMPLES OF DRM?

DRM is widely used across various types of digital content and industries. Some examples are:

E-books. Many e-books use DRM to prevent users from copying, printing, sharing, or modifying them. Some e-books also use DRM to limit the number of devices or platforms that users can read them on.

Music. Many music files use DRM to prevent users from copying, sharing, or converting them to other formats. Some music files also use DRM to limit the number of devices or platforms that users can play them on.

Videos. Many videos use DRM to prevent users from copying, sharing, or editing them. Some videos also use DRM to limit the resolution, quality, or playback speed of them.

Software. Many software programs use DRM to prevent users from installing, copying, sharing, or modifying them. Some software programs also use DRM to require online activation, registration, or subscription to use them.

Data. Many data sets use DRM to prevent users from accessing, copying, sharing, or analysing them. Some data sets also use DRM to require payment, permission, or attribution to use them.

BENEFITS AND DRAWBACKS OF DRM

DRM can have positive effects for both content providers and users. For content providers, DRM can help them:

- Protect their intellectual property rights and prevent revenue loss from piracy and unauthorized copying.
- Enhance their reputation and brand image by ensuring the quality and authenticity of their content.
- Increase their market share and customer loyalty by offering different options and incentives for accessing their content.
- Innovate and create new business models and revenue streams by leveraging the potential of digital technologies.

For users, DRM can help them:

- Access a wide range of digital content at affordable prices and convenient formats.
- Enjoy a better user experience and quality of service by avoiding malware, viruses, glitches and errors.
- Support their favourite content creators and contribute to the development of the digital economy.
- Exercise their rights to privacy, security, anonymity and fair use by choosing the content providers and platforms that respect these rights.

However, DRM can also have negative effects for both parties. For content providers, DRM can:

- Increase their costs and complexity of developing, maintaining and updating their DRM systems.
- Reduce their flexibility and adaptability to changing market conditions and customer preferences.
- Expose them to legal risks and liabilities if their DRM systems violate users' rights or infringe on other parties' intellectual property rights.
- Damage their reputation and customer satisfaction if their DRM systems are perceived as intrusive, restrictive or unfair.

For users, DRM can:

- Limit their access, use and enjoyment of digital content by imposing technical or contractual restrictions.
- Interfere with their legitimate activities and expectations, such as sharing, lending, reselling or modifying the content.
- Violate their rights to privacy, security, anonymity and fair use by collecting, storing or disclosing their personal data or monitoring their online behaviour.
- Harm their devices or data by introducing malware, viruses, glitches or errors.

CHALLENGES & CONTROVERSIES OF DRM

DRM is not without its challenges and controversies. Some of the common issues are:

User rights. Some users argue that DRM violates their fair use rights or their right to own and control their purchased digital content. They claim that DRM restricts their ability to make personal copies, backups, modifications, or adaptations of digital content for their own purposes.

User experience. Some users complain that DRM negatively affects their user experience by making digital content less accessible, convenient, compatible, or functional. They claim that DRM causes technical problems, errors, glitches, or incompatibilities with their devices or platforms.

User privacy. Some users worry that DRM invades their privacy by collecting their personal information, tracking their online activities, or exposing them to security risks. They claim that DRM requires them to share their personal data with third parties, such as content providers, service providers, or advertisers.

User activism. Some users resist or challenge DRM by circumventing it using various tools or techniques, such as cracking codes, hacking systems, or creating alternative platforms. They claim that they are exercising their civil disobedience rights or their freedom of expression rights.

DESIGN PRINCIPLES FOR DRM SYSTEMS

Given these benefits and drawbacks, how can we design and implement DRM systems that balance the interests of both content providers and users? Here are some principles and guidelines that I suggest:

Respect the law. DRM systems should comply with the relevant laws and regulations in the jurisdictions where they operate. They should not infringe on other parties' intellectual property rights or violate users' rights to privacy, security, anonymity or fair use.

Respect the ethics. DRM systems should follow the ethical standards and values of the society where they operate. They should not harm or exploit users or other stakeholders. They should promote social justice, human dignity and public interest.

Respect the users. DRM systems should consider the needs, preferences and expectations of the users. They should provide clear information about the terms and conditions of accessing the content. They should offer choices and options for different user groups. They should ensure a high quality of service and user experience.

Respect the content. DRM systems should protect the integrity and authenticity of the content. They should not degrade or distort the content. They should not interfere with the artistic or creative expression of the content creators.

Respect the innovation. DRM systems should foster innovation and creativity in the digital economy. They should not stifle or hinder the development of new technologies, products or services. They should not create artificial barriers or monopolies in the market.

ETHICAL IMPLICATIONS OF DRM

Digital rights management (DRM) applies to the copying, sharing, or modifying of digital content such as music, movies, software, or e-books. DRM can be seen to protect the rights and revenues of the creators and distributors of digital content, but it can also raise ethical issues for the users and consumers of such content.

WHAT IS RESTRICTIVE DRM?

Restrictive DRM is a type of DRM that imposes strict limitations on how users can access, use, or transfer digital content. For example, restrictive DRM may:

- Stop a cell phone from working with a different wireless provider.
- Make a DVD from a certain region unplayable in other regions of the world.
- Encrypt software to prevent copying or installing on multiple devices.
- Prevent children from accessing adult content.

- Require online verification or authentication to use certain products or services.

Restrictive DRM can be implemented through hardware, software, or legal means. Some examples of restrictive DRM technologies are:

- Region codes on DVDs or Blu-ray discs.
- Activation codes or serial numbers for software products.
- Digital locks or encryption keys on e-books or music files.
- Online platforms or services that require subscription or registration.

Restrictive DRM can also be enforced through legal measures such as the Digital Millennium Copyright Act (DMCA) in the United States, which prohibits the circumvention of DRM technologies or the distribution of tools or devices that can bypass them.

WHY IS RESTRICTIVE DRM ETHICAL?

Some of the arguments in favour of restrictive DRM are:

- It protects the intellectual property rights and interests of the creators and distributors of digital content, who invest time, money, and effort to produce and deliver quality products and services.
- It prevents piracy and illegal use of digital content, which can harm the revenues and reputation of the content industry and reduce the incentives for innovation and creativity.
- It enables new business models and revenue streams for the content industry, such as subscription-based services, pay-per-view models, or dynamic pricing strategies.
- It provides users with features and benefits that they want or need, such as parental controls, trial versions, or personalized recommendations.

Some of the sources that support restrictive DRM are:

- The Entertainment Software Association of Canada (ESAC), which represents the video game industry in Canada. ESAC argues that DRM is necessary to protect the investments and innovations of game developers and publishers, and to provide consumers with diverse and high-quality gaming experiences.
- The Alliance of Canadian Cinema, Television and Radio Artists (ACTRA), which represents performers in the audiovisual media sector in Canada. ACTRA advocates for DRM to ensure fair compensation and recognition for artists whose works are distributed digitally.
- Microsoft Corporation, which is one of the leading developers and providers of software products and services in the world. Microsoft uses DRM technologies to secure its products and platforms, such as

Windows operating system, Office suite, Xbox console, or Azure cloud service.

WHY IS RESTRICTIVE DRM UNETHICAL?

Some of the arguments against restrictive DRM are:

- It infringes on the rights and freedoms of users and consumers of digital content, who may face restrictions or barriers to access, use, or share content that they have legally acquired or paid for.
- It creates technical and legal challenges for users and consumers of digital content, who may encounter compatibility issues, performance problems, privacy risks, or legal liabilities when using or transferring content across different devices, platforms, or regions.
- It stifles innovation and competition in the content industry, as it creates entry barriers for new entrants or alternative providers who may offer better quality or lower prices for digital content.
- It reduces the social and cultural value of digital content, as it limits the possibilities for remixing, reusing, or transforming content into new forms of expression or knowledge.

Some of the sources that oppose restrictive DRM are:

- The Electronic Frontier Foundation (EFF), which is a non-profit organization that defends civil liberties in the digital world. EFF campaigns against DRM as a threat to user rights, fair use, privacy, security, accessibility, and innovation.
- The Canadian Library Association (CLA), which is a national association that represents libraries and librarians in Canada. CLA opposes DRM as an obstacle to access to information, education, culture, and democracy.
- The Free Software Foundation (FSF), which is a non-profit organization that promotes free software and free culture. FSF rejects DRM as a form of digital restriction management that violates user freedom and autonomy.

Restrictive DRM is a controversial topic that involves ethical dilemmas for both producers and consumers of digital content. On one hand, restrictive DRM can be seen as a legitimate and necessary way to protect the rights and interests of the content industry, and to provide users with features and benefits that they want or need.

On the other hand, restrictive DRM can be seen as an illegitimate and unnecessary way to infringe on the rights and freedoms of users and consumers, and to create technical and legal challenges, stifle innovation and competition, and reduce the social and cultural value of digital content. The ethical implications of restrictive DRM depend on the perspective, values, and interests of the

stakeholders involved, as well as the context, purpose, and effects of the DRM technologies or measures used.

6.3. OPEN-SOURCE SOFTWARE LICENSING

THE ESSENCE OF OPEN SOURCE

Open-source software is software that allows anyone to use, modify, and share its source code. The source code is the set of instructions that tells the computer what to do. By making the source code available, open-source software enables collaboration, innovation, and transparency.

WHY OPEN-SOURCE MATTERS

Open-source software has many benefits for users, developers, and society. Some of these benefits are:

Users can choose from a variety of software options that suit their needs and preferences. They can also inspect the source code to verify its quality, security, and functionality.

Developers can learn from other developers' work, improve existing software, or create new software based on existing code. They can also contribute to the development of software that they use or care about.

Society can benefit from the collective knowledge and creativity of the open-source community. Open-source software can also promote social good by addressing common problems or serving public interests.

HOW OPEN-SOURCE WORKS

Open-source software is governed by licenses that define the terms and conditions for its use, modification, and distribution. There are many different open-source licenses, but they generally fall into two categories: permissive and copyleft.

Permissive licenses allow users to do whatever they want with the software, provided they give credit to the original author. Examples of permissive licenses are the MIT License and the Apache License.

Copyleft licenses require users to share their modifications of the software under the same or compatible license as the original. This ensures that the software remains open-source and accessible to everyone. Examples of copyleft licenses are the GNU General Public License and the Mozilla Public License.

HOW TO CHOOSE AN OPEN-SOURCE LICENSE

Choosing an open-source license depends on your goals and preferences as a software developer. Some factors to consider are:

- How much control do you want to have over your software and its derivatives?
- How much credit do you want to receive for your work?

- How compatible do you want your license to be with other open-source licenses?
- How important is it for you to protect your software from potential legal risks?

Choose a License website to compare different open-source licenses and find one that matches your needs. You can also consult a lawyer or an expert in IT governance, policy, ethics, and law if you have specific questions or concerns.

By choosing an open-source license, you can define how others can use, modify, and distribute your software. You can also join a community of developers who collaborate on creating and improving open-source software.

THE ETHICS OF COLLABORATION & INNOVATION

OPEN-SOURCE SOFTWARE LICENSING

Open-source software (OSS) is software that is distributed with a license that allows anyone to use, study, change, or share its source code, without restrictions on how the software is used or by whom.

OSS has become ubiquitous across all areas of software development, as it enables developers to reuse existing code and create more functionality at greater speed. OSS also promotes the adoption of transparent standards and makes applications more interoperable.

However, OSS also raises some ethical questions about how the software is used and who benefits from it. Some developers do not want their work to be used for harm, such as military or surveillance purposes, while others think that restricting OSS is contradictory or impractical. Moreover, some OSS licenses may impose obligations on the users or distributors of the software, such as disclosing the source code, providing attribution, or sharing modifications.

THE HIPPOCRATIC LICENSE

One example of an ethical OSS license is the Hippocratic License, created by Coraline Ada Ehmke in 2019. This license is based on the MIT license but adds a condition that the software may not be used for systems or activities that violate the United Nations Universal Declaration of Human Rights. The Hippocratic License aims to give developers more control over how their software is used and to prevent it from being used for evil.

However, the Hippocratic License is not approved by the Open-Source Initiative (OSI), which governs the most widely used OSS licenses. The OSI argues that the Hippocratic License is not conformant with the Open-Source Definition (OSD), which requires that OSS licenses do not discriminate against persons, groups, or fields of endeavour. The OSI also claims that the Hippocratic License is vague and

subjective, as it relies on the interpretation of human rights by different users and jurisdictions.

THE OPENCHAIN PROJECT

Another approach to address the ethical issues of OSS licensing is the OpenChain Project, which is an initiative by the Linux Foundation to establish best practices for OSS compliance. The OpenChain Project provides a specification and a certification program for organizations that use OSS in their products or services. The OpenChain Project aims to ensure that OSS users respect the rights and obligations of OSS developers and licensors, and that they provide clear and consistent information about the OSS components they use.

The OpenChain Project does not impose any ethical restrictions on how OSS is used, but rather focuses on improving the transparency and accountability of OSS usage. The OpenChain Project also helps organizations to avoid legal risks and reduce costs associated with OSS compliance.

Developers who create or use OSS should be aware of the different types of OSS licenses and their implications for collaboration and innovation. Developers should also respect the intentions and expectations of other developers who contribute to or depend on OSS. By following best practices and standards for OSS compliance, developers can ensure that they use OSS in a responsible and ethical manner.

WHAT IS AN OPEN-SOURCE LICENSE?

An open-source license is a type of software license that complies with the Open-Source Definition. In brief, it allows software to be freely used, modified, and shared by anyone for any purpose, if the license terms are respected. There are many different open-source licenses, and they vary based on the restrictions or conditions they impose on the software users.

CHOOSING AN OPEN-SOURCE LICENSE

Some general factors to consider are:

Compatibility. Some open-source licenses are compatible with each other, meaning that you can combine or distribute software under different licenses without violating any terms. Some licenses are incompatible with each other, meaning that you cannot do so without obtaining additional permissions or agreements. You should check the compatibility of your chosen license with other licenses that you may want to use or interact with in the future.

Copyleft. Some open-source licenses are copyleft, meaning that they require any modified or derived versions of the software to be distributed under the same or equivalent license. This ensures that the software remains open-source and preserves the original author's rights and intentions. Some licenses are permissive, meaning that they do not impose such a requirement and allow more

flexibility for the software users. You should decide whether you want your software to be copyleft or permissive, depending on your preferences or objectives.

Popularity. Some open-source licenses are more popular or widely used than others, meaning that they have more recognition or acceptance in the open-source community. This can affect how easy it is to find or collaborate with other projects that use the same or similar licenses. You should consider whether you want your software to use a popular or less popular license, depending on your needs or expectations.

ETHICAL CONSIDERATIONS

OSS comes with several ethical challenges and responsibilities for both contributors and users.

WHY ETHICS MATTER FOR OSS

OSS is not just a technical matter; it is also a social and political one. OSS can have positive or negative impacts on society, depending on how it is used and by whom. For example, OSS can be used for military purposes, surveillance, misinformation, or discrimination.

OSS can also be vulnerable to security breaches, bugs, or malicious code. Therefore, OSS contributors and users should consider the ethical implications of their actions and decisions.

AVOIDING ETHICAL DILEMMAS

OSS also poses some ethical challenges for developers and users, such as:

- How to respect the human rights and dignity of those who may be affected by the software?
- How to ensure the quality and security of the software and prevent harm or misuse?
- How to balance the freedom of OSS with the responsibility of its creators and contributors?
- How to deal with ethical conflicts or dilemmas that may arise from the use of OSS in different contexts or for different purposes?

RESPECT THE HIPPOCRATIC PRINCIPLE: DO NO HARM

The Hippocratic principle is a moral principle that states that one should do no harm or avoid doing harm. It is derived from the Hippocratic oath, a code of ethics for physicians that dates to ancient Greece. The Hippocratic principle can be applied to OSS development and use, as a way of ensuring that the software does not cause harm to individuals, groups, or society at large.

One way of respecting the Hippocratic principle is to adopt an ethical license for OSS, such as the Hippocratic License, which was created by Coraline Ada Ehmke, a software developer from Chicago. The Hippocratic License is a license that puts ethical restrictions on the use of OSS code, such as prohibiting its use for violating human rights or dignity. The Hippocratic License aims to give developers more control over how their software is used and to prevent its use for harmful purposes.