Task 9.1P - SIT223

Truong Khang Thinh Nguyen

September 21, 2024

1 Ethical Considerations in Data Sharing for Targeted Advertising Case Study

Data sharing for targeted advertising raises a number of ethical concerns. To begin, **privacy considerations** are crucial, as gathering and selling personal data, including demographics, playing habits, and even background conversations, can impinge on players' privacy if not managed clearly. Even though customers agree to data collection when they purchase the game, there is an implied ethical dilemma of whether they are completely aware that their data may be sold to third parties. **Transparency** in data use and sale is critical, as customers may be uncomfortable with their personal information being shared without their explicit authorization for these secondary objectives. The company's **trust** connection with its consumers is also at risk; if customers believe the company prioritizes profit over privacy, it could affect the brand's reputation and result in **legal consequences**, such as violations of data protection regulations such as the Australian Privacy Act. The Australian Computer Society (ACS) Codes of Ethics [1] offer guidance, emphasizing the need to respect user privacy, acquire informed consent, and ensuring data is used responsibly. To avoid ethical violations, the company could take a different approach, such as providing **opt-in mechanisms** for data sharing, ensuring data **anonymization** before sharing, or developing clear, user-friendly privacy policies that educate customers on how their data will be used, allowing them to make informed decisions about participating.

2 IP Case Study

2.1 Intellectual Property Identification

CyberSolutions most likely owns multiple types of intellectual property (IP) linked to its main product, "DataGuard." The most visible would be **copyright** protection, which includes the original code, user interface design, and software documentation. This grants CyberSolutions the sole right to control the reproduction, distribution, and modification of their work. Furthermore, they may possess **trade secrets**, notably proprietary encryption techniques or methodologies that provide a competitive advantage. These are covered by confidentiality agreements. If CyberSolutions has invented a novel encryption technology or a unique technique, they may have **patents** that protect these innovations under Australian law for a fixed length of time, preventing others from exploiting them without their permission.

2.2 Infringement Analysis

The emergence of InnovateTech Systems' "SecureShield" software, which has many similarities to "DataGuard," raises concerns about **intellectual property infringement**. The most likely

infraction is **copyright infringement**, in which InnovateTech may have copied parts of CyberSolutions' software code or interface design. Another major risk is the unlawful use of trade secrets, which may occur if InnovateTech obtained private information through former workers or other sources. A careful comparison of the two software packages is required to uncover direct duplication or appropriation of distinguishing characteristics that would constitute a violation of CyberSolutions intellectual property rights.

2.3 Legal Framework

In Australia, the **Copyright Act of 1968** [2] protects original software code and interface designs. CyberSolutions, the creator, has exclusive rights to reproduce and distribute "DataGuard.". If CyberSolutions has patented any unique technology or encryption techniques contained within the software, the **Patents Act of 1990**[3] will apply. Trade secrets are also protected under Australian common law and commercial arrangements, such as non-disclosure agreements (NDAs). Breaching these could potentially result in legal action if InnovateTech got unauthorized access to confidential knowledge.

2.4 Potential Legal Consequences

If InnovateTech is found accountable for copyright infringement or misappropriation of trade secrets, they may face a number of legal consequences. CyberSolutions may seek an **injunction** to prevent InnovateTech from continuing to sell or distribute "SecureShield." They may also seek compensation for any financial losses caused by the infringement, such as lost revenue and statutory **damages**. If InnovateTech is proven to have illegally used CyberSolutions' trade secrets, they may face fines for breach of confidentially, which could jeopardize their operations and financial status.

2.5 Protection and Management

To properly safeguard its intellectual property, CyberSolutions should take four critical actions. First, they must guarantee that their copyrights and patents are completely registered and up-to-date, especially for crucial software components and new encryption techniques. Implementing non-disclosure agreements (NDAs) for all personnel and contractors involved in critical development areas will help to protect trade secrets. CyberSolutions should also implement a mechanism to monitor competitors for potential infringements, allowing them to respond quickly if their intellectual property is breached. CyberSolutions could also utilize **encryption** and **limited access controls** to protect proprietary code from illegal use or disclosure.

2.6 Ethical Considerations

The ethical consequences of intellectual property infringement are serious. If InnovateTech cloned software from CyberSolutions, they are not only breaking the law, but also acting unethically by capitalizing on another company's creativity without acknowledgment or recompense. This lowers the value of original work and discourages future innovation. Ethical business practices in the technology industry necessitate respect for others' intellectual property rights, ensuring that creators are appropriately compensated for their efforts. Fostering an atmosphere in which intellectual property is safeguarded stimulates competitiveness based on creativity and innovation, which is critical to the industry's overall success.

References

[1] ACS, *Ethic and discipline*, www.acs.org.au, 2023. [Online]. Available: https://www.acs.org.au/memberships/professional-ethics-conduct-and-complaints.html.

[2] F. R. of Legislation, *Copyright act 1968*, www.legislation.gov.au, Jan. 2019. [Online]. Available: https://www.legislation.gov.au/C1968A00063/2019-01-01/text.

[3] S. scheme=AGLSTERMS. AglsAgent; corporateName=Industry and Resources, *Patents act 1990*, www.legislation.gov.au, Nov. 2023. [Online]. Available: https://www.legislation.gov.au/C2004A04014/latest/text.

[4] I. Australia, *Ip australia —*, Ipaustralia.gov.au, 2019. [Online]. Available: https://www.ipaustralia.gov.au/.

[5] OAIC, *Home - oaic*, Oaic.gov.au, 2019. [Online]. Available: https://www.oaic.gov.au/.

[6] F. González-Pizarro, A. Figueroa, C. López, and C. Aragon, "Regional differences in information privacy concerns after the facebook-cambridge analytica data scandal," *Computer Supported Cooperative Work (CSCW)*, vol. 31, Feb. 2022. DOI: 10.1007/s10606-021-09422-3.

[7] A. C. Plane, E. M. Redmiles, M. L. Mazurek, and M. C. Tschantz, *Exploring user perceptions of discrimination in online targeted advertising*, www.usenix.org, 2017. [Online]. Available: https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/plane.

[8] A. Bleier and M. Eisenbeiss, "The importance of trust for personalized online advertising," *Journal of Retailing*, vol. 91, pp. 390–409, Sep. 2015. DOI: 10.1016/j.jretai.2015.04.001.