Question 1

The term culture relates to a set of actions or customs which are considered normal amongst a particular group of people (Millet, 2008, p. 27-53). Ethics relates to actions which are supported by a set of moral principles that govern a person's behaviour (Millet, 2008, p. 27-53). Ethical culture is a topic that has grown in popularity since the 1970's and was investigated because it was shown to significantly improve the performance of a company (Chadegani & Jari, 2016, p. 59). For example, economic analysts attributed a large part of Japanese business success in the 1980s to the strong foundations of its ethical culture (Chadegani & Jari, 2016, p. 59).

An ethical culture is supported by moral principles that must be chosen before they can be encouraged (Chadegani & Jari, 2016, p. 59). It is exceedingly difficult to determine what is moral and these questions are determined by our judgements (Millet, 2008, p. 27-53). The leaders of an organization must make these moral judgements to determine the values that they want to adopt. Immanuel Kant specified that there are two types of judgements that are distinguished by their measurability (Millet, 2008, p. 27-53). Determining judgements are easily determinable because the answer maybe a simple right and wrong (Millet, 2008, p. 27-53). Reflecting judgements are when the thing being judged is difficult to measure (Millet, 2008, p. 27-53). The person must use their personal maxims to make reflecting judgements (Millet, 2008, p. 27-53). Reflecting judgements are generally used to determine whether a set of actions are considered moral (Millet, 2008, p. 27-53).

The 6C model is a western system of ethics that describes principles which should be used to encourage the growth, development, and maintenance of a healthy and ethical organization (Millet, 2008, p. 27-53). The first part of the 6C model is the four characteristics which define an "ethical person". The four characteristics that describe an ethical person is consistency, consequences, care, and character (Millet, 2008, p. 27-53). The second section is "communication", and this is combined with the "definition of an ethical person" to form an "ethical culture" (Millet, 2008, p. 27-53).

Consistency is the perpetual application of the principle that you want to adopt (Millet, 2008, p. 27-53). For example, one of these maxims could be “do to others what you want done to yourself” (Millet, 2008, p. 27-53). Immanuel Kant describes consistency through the idea of the “categorical imperative”. The “categorical imperative” is the idea that moral principles must be applied as if they were a “law of nature” (Millet, 2008, p. 27-53).

Consequences are the results that are generated from an action that we undertake. Consequences can be placed into categories which are divided by the type of outcomes that are generated (Millet, 2008, p. 27-53). Consequences could be divided into two separate categories, for example, egotistic hedonism or utilitarianism (Millet, 2008, p. 27-53). Egotistic hedonism are the consequences which can lead to outcomes which tend to benefit the individual. Utilitarianism is an ethical principle devised by Jeremy Bentham which supports outcomes which have the tendency to benefit all the stakeholders involved (Millet, 2008, p. 27-53). As explained earlier, we must use a reflecting judgement to determine if we want to employ a utilitarian or hedonistic culture.

Care is divided into three sectioned definitions, caring for, caring about and taking care (Millet, 2008, p. 27-53). These three types of care originate from separate psychological origins and have their own corresponding strengths and weaknesses. Caring for is when we care about the needs of someone (Millet, 2008, p. 27-53). Caring about is the emotional concern we have for someone. When we care about someone it generates a corresponding desire to take care of them (Millet, 2008, p. 27-53). Taking care is the attentive care we use when we want to ensure that we do our job correctly (Millet, 2008, p. 27-53).

Character is described as the sum of our thoughts and actions (Millet, 2008, p. 27-53). Our virtues are part of our character and are developed as we reflect about the actions that we undertake. Virtues can be divided into two sections which include intellectual virtues, and moral virtues (Millet, 2008, p. 27-53). Intellectual virtues are the things that we can learn like scientific knowledge (Millet, 2008, p. 27-53). Moral virtues are the things which need to be practiced consistently so that they become part of our character (Millet, 2008, p. 27-53). Millet (2008) stated that integrity is the constancy and consistency of our character. Integrity and character are especially important because it can determine if we can be relied on. The consistent application of our moral principles forms our character.

Communication is the way we relay our ideas, thoughts, and feelings to each other. Issues can transpire when a person attempts to interpret the ideas that another person is conveying. Communication can be divided into three sections of what is said, what is meant, what is interpreted (Millet, 2008, p. 27-53). Distinguishing communication in these three ways allows us to understand and manage communication breakdowns (Millet, 2008, p. 27-53). The most important part of communication is our ability to listen, so that we can understand what is being meant, and to correct misinterpretations by speaking out when something has been misunderstood (Millet, 2008, p. 27-53).

Reflecting judgements may be required to determine the moral principles we want to adopt. For example, you may want to choose utilitarian principles as the consequences you want to encourage. Forming our decisions and combining them with communication results in the production of our “ethical culture” (Millet, 2008, p. 27-53).

Question 2

A professional is a person who exchanges payment for a service that a customer requires. The service the professional provides must be completed according to established ethical protocols (Millet, 2008, p. 27-53). The ACS codes specify the expected ethical behaviour of a professional according to the code of conduct (Millet, 2008, p. 27-53). There are a set of professional codes of ethics written by the ACS which requires the need for honesty, loyalty, confidentiality, fairness, professional development, competency, and social responsibility (Millet, 2008, p. 27-53). There are different relationships that an employee has with the people he conducts business with (Coldwell, 2008, p. 277-302). There are three types of relationships that need to be considered for this case. The relationship types include the professional-employer relationship, professional-society relationship, and professional-client relationship (Coldwell, 2008, p. 277-302).

The ACS requires that the members of its society must abide by its code of ethics (Millet, 2008, p. 27-53). The code is divided into sections and these can be used to help guide the conduct of the professional (Australian Computing Society, 2014). The professional must look to the ACS codes as a reference in the event something has gone wrong. The main sections of the ACS code which apply to this case are "primacy of the public interest", "honesty" and "competence" (Australian Computer Society, 2014). One of the major problems with the codes is that they are an over-simplified description of ethical standards (Millet, 2008, p. 27-53). This case can be considered as a moral dilemma. Moral dilemmas are complex situations which require an extensive amount of reflection to understand, and this may not be detailed in the codes themselves (Australian Computer Society, 2014).

The employee has broken his trust with the client, employer, and his community. The code section 1.2.3 stipulates that he must not break trust with his client (Australian Computer Society, 2014). In section 1.2.1 titled, "The Primacy of the public interest", subsection "(g)", it also stipulates that he must protect the confidentiality and privacy of others(Australian Computer Society, 2014). The employee's circumstances became extremely complicated after he broke his trust with the client. In section 1.2.1 of the ACS code, it states that all conflicts should be in favour of the public interest (Australian Computer Society, 2014). In this case, the employee has gathered new information that would place the public at risk if his client were not notified to the police. His complication has become even greater because now his actions traverse the boundaries of other criminal laws. He has not notified the police about the actions of his client and has now broken his trust with his community. The client then deleted content, which can also be considered as evidence, on a computer that he does not possess the right to do so. He has also broken the trust with his employer in two ways. Firstly, he did not abide by his employer's instructions to keep the customer's information confidential (Australian Computer Society, 2014). Secondly, he did not inform his employer about the circumstances after he uncovered the videos. It also does not specify that the employee looked for guidance in the ethical codes to determine what action to undertake. I do not agree on the fact that he looked through the person's computer as he did. However, the issue with regards to his actions after what he had uncovered is much more complicated. Had he have abided by these rules, the other complicated problems would not have transpired. The employee attempted to cover his problems by acting as if he did not behave unprofessionally to begin with. The correctness of his behaviour was with regards to the outcome. The issue with the child pornography would have gone unnoticed if he had not looked through his client's files to begin with. The current outcome of the employee's decision is almost the same because it would also appear to everyone that this issue has gone unnoticed.

It was written earlier that my virtues are an extension of my thoughts and feelings. I am not a very hateful person who judges people for things that are outside of their hands. I also have other moral issues I feel should be raised with regards to these matters. For example, I have personal issues with the excessive way the police handle these types of situations. It would be easier to notify the police if the government took the approach to neutralize the threat without creating more danger for the person being incarcerated. My decision must be extended from the careful examination of the codes. The ACS codes clearly state that my decision should lean towards the favour of the public interest. This suggests that it is my obligation to notify the police. In this case, I believe the best thing to do would have been to contact the police (Australian Computer Society, 2014).

Question 3a

Social engineering is a type of fraud or "identity theft" that is used by hackers to enter a system without the direct use of a technology (Warren, 2008, p. 162-178). The criminals attempt to deceive people by manipulating their targets psychologically. The criminals then gain information from them without the targets detecting that they are being manipulated (Warren, 2008, p. 162-178). This is all done with malicious intent and is classified as criminal activity. There are many avenues that these people use to deceive their targets, for example, using email or telephone. A person can also pretend to be an employee of a company by wearing clothing and speaking as if they are part of the company. The criminals may steal the identity of a person and gain access to unauthorized information or steal money from a company (Warren, 2008, p. 162-178). These criminals can also target individuals, rather than organizations, and use the same social engineering techniques to con people into releasing information about themselves. For example, Warren (2008) stated that a social study was conducted by the University of Texas where 90% of the students entered personal information by clicking on a fake link in an email that was not part of the university (Warren, 2008, p. 162-178). The findings from this report can be demonstrated in other real-life cases. For example, in 2018 the Cabarrus County lost 1.7 million dollars because hackers impersonated county suppliers. The hackers used fake emails and convinced the customers to send payments to their personal bank accounts (*US$1.7 Million Stolen From North Carolina County After BEC Scammers Posed as Contractor*, 2019). When the money was transferred it was immediately sent to several other locations (*US$1.7 Million Stolen From North Carolina County After BEC Scammers Posed as Contractor*, 2019). The county attempted to recover the stolen money but only 800 thousand dollars of the total was ever recovered (*US$1.7 Million Stolen From North Carolina County After BEC Scammers Posed as Contractor*, 2019).

Question 3b

A honey pot is a fake server created by an organisation which is used to entice hackers to break into their systems (Warren, 2008, p. 162-178). The use of honey pots is a controversial issue and there have been some moral concerns which have been raised about its use. Some professionals have claimed that it is a form of “entrapment” which uses deceitful techniques to place people under stress (*What Is a Honeypot?*, n.d.). However, a lot of valuable information can be gathered about the techniques that hackers use and the vulnerabilities which exist in their systems (*What Is a Honeypot?*, n.d.).

The fake server is used to deceive the hacker who tries to attack this server thinking that they are attacking a real-life server (Warren, 2008, p. 162-178). When the hackers gain root access, they are monitored without raising any suspicion (Warren, 2008, p. 162-178). The organization uses a honeypot firewall that allows enough outbound traffic so as not arouse this suspicion (Warren, 2008, p. 162-178). The system administrator monitors the hacker’s movements and attempts to learn from what they are doing (Warren, 2008, p. 162-178). The system administrators can learn three things from the hacker’s behaviour. This includes the techniques the hackers use to enter the system, the tactics used to gain privileges and to learn about the different types of hacking systems out there (*What Is a Honeypot? A Trap for Catching Hackers in the Act*, 2019). Honeypots can also be used to distract hackers with the use of the fake server. This can have the effect of protecting the other valuable resources and services of an organization (*What Is a Honeypot? A Trap for Catching Hackers in the Act*, 2019).

Question 4

Professionals enter various types of relationships whilst they are working. The professional can enter relationships with users, clients, suppliers, and the society (Coldwell, 2008, p. 277-302). The ACS has codes and guidelines that are used to describe and encourage healthy professional relationships (Coldwell, 2008, p. 277-302). These codes have the tendency to overlap each other. However, there are still a lot of differences between each of these relationships and must be examined distinctly. We will elaborate on the professional-client and professional-society relationship as means to investigate these differences.

Professional-Client relationship

A professional provides a service to a client in exchange for money (Coldwell, 2008, p. 277-302). The professional must exercise their skill ethically so that it meets the respectful demands of the client (Coldwell, 2008, p. 277-302). These ethical principles are evident in the ACS codes. For example, section 4.3.2 specifies that the professional must work competently and diligently for both the clients and employers (Coldwell, 2008, p. 277-302). The professional can also protect the interest of the community and his employer by meeting the demands of his client. This is usually determined by the type of work that the professional is completing. For example, there may be circumstances where the work being completed for the client does not have a great impact on the rest of society. Various problems can arise during these types of interactions. This usually occurs when there is a conflict of interest (Coldwell, 2008, p. 277-302). An employer may ask you to do something that works against the interest of the client. This can place you at risk if you are unwilling to act on an instruction which compromises the interest of the client. In another situation, the professional may be enticed to recommend something that will directly benefit themselves (Coldwell, 2008, p. 277-302).

Employee-Society relationship

A professional's actions could have a detrimental effect on the people in his community. There are a lot of laws which exist that protects the public from products that do not meet the required standards of safety. A professional is guided by his ethical principles and these are described in the ACS code section titled "Social Implications" (Coldwell, 2008, p. 277-302). A professional has the responsibility of ensuring the safety of the public (Coldwell, 2008, p. 277-302). In section 1.2.1 of the ACS code, it states that all conflicts should resolve to favour the public interest (Australian Computer Society, 2014). The type of work being done by the professional may influence the emphasis on this relationship type, for example, when the professional is programming a car brake system. Many problems can arise in the workplace that could place the public at risk. This usually occurs when there is a conflict of interest. The employer may ask the professional to do something because it cuts costs, but this could jeopardize the public's safety. The professional may recommend something to the client that benefits himself rather than the interests of the community. The professional may also complete his job lazily and this could have a detrimental effect on the interests of the community.

Question 5a

Privacy is the right a person possesses which restricts other people or organizations from access to their information (Gibbs, 2008, p. 94-97). The Privacy Act 1988 (2020) provides privacy principles in the form of IPPs which provides standards for the collection, use, storage, security and transfer and exchange of personal information of agencies that are in connection with the Commonwealth (Gibbs, 2008, p. 94-97). The 1988 Privacy Act (2020) controls the way a person's information is handled (Gibbs, 2008, p. 94-97). In the original 1988 Privacy Act (2020), an APP entity was referred to as an "agency" which are described to be organizations that are associated with the commonwealth (*Privacy Act 1988* pt II div 1). These do not include all large-scale organizations that are part of the private sector (Gibbs, 2008, p. 94-97). This was amended in December 2001 and a new definition of "organization" was included in the act (Gibbs, 2008, p. 94-97). This amendment included changes that extended the protection to other parts of the private sector (Gibbs, 2008, p. 94-97). This does not include businesses that have revenue less than three million dollars (*Rights and Responsibilities*, n.d.). However, there are still some organizations which are covered that turnover less than three million dollars

(*Rights and Responsibilities*, n.d.). For example, these can include a private-sector health service provider or a credit reporting company (*Rights and Responsibilities*, n.d.). There are other organizations, both in a group or individually, which are not covered under this law. For example, it does not include a person who is acting in their own capacity, or a worker of a media organization who is working as a journalist (*Rights and Responsibilities*, n.d.).

Question 5b

We can determine if the law provides adequate protection by looking at four things. This includes how the 1998 Privacy Act (2020) is legally constructed, its policing, the ambiguity of the law and the entities which are regulated under the act. Privacy can be divided into three sections, secrecy, anonymity, and solitude (Gibbs, 2008, p. 94-97). Secrecy is the control of information we want about ourselves (Gibbs, 2008, p. 94-97). Anonymity is the freedom from the attention of others (Gibbs, 2008, p. 94-97). Solitude is the freedom from being placed under surveillance (Gibbs, 2008, p. 94-97).

Firstly, to live happily in our society there is some aspect of our privacy that we must lose (Gibbs, 2008, p. 94-97). For example, the law does not punish those who take and distribute images from public places. The citizens must also lose some aspect of their privacy for the government to run their organizations proficiently (Gibbs, 2008, p. 94-97). For example, the government needs information to collect taxes, perform census reports or issue a driver’s license.

Secondly, the 1988 Privacy Act (2020) does not completely extend to all entities inside Australia (Gibbs, 2008, p. 94-97). For example, the definition of “organization” does not include businesses that have turnover less than three million dollars (*Privacy Act 1988* pt II div 1). In this way, the 1988 Privacy Act (2020) is limited by the organizations which it extends to.

Thirdly, the law attempts to describe, in a finite way, something which is overly complex. There could exist limitations that are extended from the ambiguity in the description of the law. For example, a third party can collect information about a person from an organization without the person’s awareness (Attorney General’s Department, 2020).

Fourthly, the number of resources the government has is limited and this could place constraints on its ability to enforce these laws.

The 1988 Privacy Act (2020) places a lot of pressure on Australian citizens, compartments, and private organizations to act in accordance with the law. Although the law has its limitations, the 1988 Privacy Act (2020) still provides an extensive amount of protection. The protection is enough to ensure that the citizens needs are met and for the government to run its institutions proficiently.

Question 6a

Privacy is not an “all or nothing” principle, meaning that we must lose some aspect of our privacy to be part of our society (Gibbs, 2008, p. 94-97). Privacy has raised great concerns in our society and the intervention of advanced technology has heightened these concerns (*Taking Photographs and Other Images*, 2010). Images or a video may contain sensitive information and is treated as personal information by the government. This is regulated under the Privacy Act 1988 (Attorney General’s Department, 2020). The requirement for consent may vary depending upon the situation. Consent is not required if the person taking the image is not recording sensitive information about the person (*Privacy Act 1988* pt II div 3). However, you need permission to take photos if you are on private property (*Photography and the Law – When Is It Illegal to Take a Photo?*, 2019). It is not an offence to photograph or video someone in a public setting without their permission. It is also not an offence to distribute these images without their permissions (Gibbs, 2008, p. 94-97).

Question 6b

The elements which need to be taken into consideration to determine if the images are in breach of the law include, the location of the photo, the purpose, and the use of the photo (*Photography and the Law – When Is It Illegal to Take a Photo?*, 2019). There are several criminal laws that also regulate the taking of photo and videos (*Taking Photographs and Other Images*, 2010). These criminal laws punish those who take and use videos or images for offensive purposes. For example, it is illegal to photograph or video children in public areas if those images are obscene (*Taking Photographs and Other Images*, 2010). A person may not take photos of a person whilst that person is in a private setting (*Taking Photographs and Other Images*, 2010). A person may also be penalized for taking photos in venues such as entering a sporting stadium to watch a cricket match. (*Taking Photographs and Other Images*, 2010).

Question 7a

Property is something that can be owned, and the law subdivides this into real property and personal property (Thomson, 2008, p. 199-228). Personal property can also be subdivided into tangible and intangible possessions. Intangible possessions can include intellectual property which are things produced as the result of an operation conducted by your mind (*IP Explained*, 2021). Intellectual property can include inventions, trademarks, designs, brands, and other ways your ideas can be applied. Intellectual property is an intangible right which allows for the personal and exclusive exploitation of proprietary knowledge (Thomson, 2008, p. 199-228). IP Australia handles the legislation with regards to intellectual property and administers these rights for their customers (*IP Explained*, 2021).

Question 7b

Trademarks are a type of intellectual property that is used as a way of uniquely identifying a product or service (*Trade Mark Basics*, 2019). A trademark could include a word, phrase, letter, number, logo, picture, or aspect of packaging (Thomson, 2008, p. 199-228). Trademarks are used to distinguish an organization's goods and services from their competitors. For example, a trademark could be the McDonald's "M" sign or the phrase "The Yack Back" (*Trade Mark Basics*, 2019). Trademarks have been legislated by the commonwealth under the 1995 Trademarks Act (*Trade Marks Act 1995* pt I div 1). Trademarks have been divided into two categories which include registered and unregistered trademarks. A registered trademark has been reserved and accepted as a trademark from Intellectual Property Australia (*Trade Mark Basics*, 2019). An unregistered trademark is one which has not been formally registered. An unregistered trademark can still be entitled to legal protection (Hale, 2019). To get legal protection for an unregistered trademark you must prove that the goods and services have a reputation in the market and the trademark is exclusively recognizable to your company (Hale, 2019).

Question 8a

People can work on a project individually or in a group of people. A collaborative effort is when a group of people decide to complete a project attempting to meet a common goal (Thomson & Nelson, 2008, p. 303-327). When people first encounter a project, they have no knowledge about the details of the tasks. A shared understanding is the detailed knowledge that each member has acquired about the project (Thomson & Nelson, 2008, p. 303-327). Meaningful contribution is the suggestive input a team member has towards the project. It is impossible that a team member can meaningfully contribute to a project without having a shared understanding. A shared understanding also allows the members of the team to use their skills more efficiently (Thomson & Nelson, 2008, p. 303-327).

Question 8b

Groups who participate in collaborative work need to have a common understanding for them to work productively (Thomson & Nelson, 2008, p. 303-327). There are different types of projects which can be divided according to their complexity. Projects which are more complex may require a lot of different skills to complete (Glinz & Fricker, 2014, p. 372). These skills have the potential to be extremely useful if those skills have been integrated correctly (E. Bittner & Leimeister, 2013, p. 1–3). Every team member within the project must have an understanding about the details of the project so that everyone can contribute meaningfully (E. Bittner & Leimeister, 2013, p. 1–3). Projects can be divided based up on the difficulty of the objectives (E. Bittner & Leimeister, 2013, p. 1–3). It is more difficult to acquire a shared understanding when the project requires extensive skills (E. Bittner & Leimeister, 2013, p. 1–3). Without this shared knowledge and a structured way to acquire it, the project outcomes might be achieved sub-optimally (E. Bittner & Leimeister, 2013, p. 1–3).

Question 8c

A shared understanding must be constructed through an organized collaboration process (E. Bittner & Leimeister, 2013, p. 1–3). This collaborative process must involve multiple steps which are completed iteratively. It is easy to describe a system to achieve a shared understanding, however, it is exceedingly difficult to practically implement such a process (E. Bittner & Leimeister, 2013, p. 1–3). The collaborative process can achieve a shared understanding through persistent and conscious effort (E. A. C. Bittner & Leimeister, 2014, p. 132). There are various methods that can be used to attain a shared understanding. Glinz and Fricker (2014) described a multi-step collaborative process which can be used to achieve this. Three of these steps include, domain scoping, stakeholder analysis and domain understanding (Glinz & Fricker, 2014, p. 372). Domain scoping attempts to identify the parts of the project which require a shared understanding (Glinz & Fricker, 2014, p. 372). Stakeholder analysis involves identifying the ability of each member in the group (Glinz & Fricker, 2014, p. 372). Stakeholder analysis determines how tasks are to be allocated and identifies the team members which need to develop a shared understanding (Glinz & Fricker, 2014, p. 372). Domain understanding is a process which enforces team members to achieve a general understanding of important project concepts. This is extremely important if the team members want to meaningfully contribute to the objectives (Glinz & Fricker, 2014, p. 372).

Question 9

The government desires to manage the way the internet is used by implementing legal controls (Thomson, 2008, p. 125-162). The government can do this by producing regulation that is designed to target the citizens and internet service providers. One of the ways that a government can implement these regulations is through censorship. Censorship is concerned with the way the government suppresses information by and from the public (Thomson, 2008, p. 125-162). Information is like food, it can modify a person in a negative way, and because of this, some things are considered unsuitable for consumption. One of society's major concern is that the government may impose unrealistic or unethical restrictions on the public. It is imperative that the governments use their powers in a moral fashion so that censorship can be implemented correctly. The two actions the government use to implement censorship include filtering and content control (Thomson, 2008, p. 125-162).

Filtering is implemented with the use of software technology that limits access to websites. Filtering can also be used to censor unwanted educated materials (Thomson, 2008, p. 125-162). People have complained that filtering software may exclude material which may be useful to internet users. For example, Thomson (2008) stated that a website filtering program called “SurfWatch” blocked human-rights sites such as the Commissioner of the Council of the Baltic Sea States.

Content control is related to the actual information contained in a communication. In Australia, content control is regulated under the Spam Act 2003 (Cth), and Criminal Code Act 1995 (Cth) which forces the responsibility on the internet service provider. For example, the internet service provider is responsible for reporting material containing child pornography (Thomson, 2008, p. 125-162).

Reference List

Attorney General’s Department. (2020, October). *Privacy Act Review*. https://www.ag.gov.au/system/files/2020-10/privacy-act-review--issues-paper-october-2020.pdf

Australian Computer Society. (2014, April). *ACS Code of Professional Conduct* (2.1). https://www.acs.org.au/content/dam/acs/acs-documents/ACS%20Code-of-Professional-Conduct_v2.1.pdf

Bittner, E., & Leimeister, J. M. (2013, January). *Why Shared Understanding Matters -- Engineering a Collaboration Process for Shared Understanding to Improve Collaboration Effectiveness in Heterogeneous Teams*. 2013 46th International Conference on System Sciences, Maui, Hawaii. https://doi.org/10.1109/HICSS.2013.608

Bittner, E. A. C., & Leimeister, J. M. (2014). Creating Shared Understanding in Heterogeneous Work Groups: Why It Matters and How to Achieve It. *Journal of Management Information Systems*, *31*(1), 111–144. https://doi.org/10.2753/mis0742-1222310106

Chadegani, A. A., & Jari, A. (2016). Corporate Ethical Culture: Review of Literature and Introducing PP Model. *Procedia Economics and Finance*, 51–61. https://doi.org/10.1016/s2212-5671(16)30015-6

Coldwell, J. (2008). Professional ethics and responsibilities. In D. McDermid (Ed.), *Ethics in ICT: an Australian perspective* (1st ed., p. 277–302). Pearson Education Australia.

Gibbs, M. (2008). Privacy. In D. McDermid (Ed.), *Ethics in ICT: an Australian perspective* (1st ed., p. 89–123). Pearson Education Australia.

Glinz, M., & Fricker, S. A. (2014, July). On shared understanding in software engineering: an essay. *Computer Science - Research and Development*, 363–376. https://doi.org/10.1007/s00450-014-0256-x

Hale, C. (2019, November 6). *What Are the Differences Between Registered and Unregistered Trade Marks?* Legal Vision. https://legalvision.com.au/registered-and-unregistered-trade-marks-whats-the-difference/

IP Explained. (2021, February 4). IP Australia. https://www.ipaustralia.gov.au/understanding-ip/getting-started-ip/ip-explained

Millett, S. (2008). The study of ethics. In D. McDermid (Ed.), *Ethics in ICT: an Australian perspective* (1st ed., p. 27–53). Pearson Education Australia.

Photography and the law – when is it illegal to take a photo? (2019, May 9). Australian Lawyers Alliance. https://www.lawyersalliance.com.au/opinion/photography-and-the-law-when-is-it-illegal-to-take-a-photo

Posting photos and videos. (2019, June 13). Office Of The Australian Information Commissioner. https://www.oaic.gov.au/privacy/guidance-and-advice/posting-photos-and-videos/

Privacy Act 1988 (Cth). https://www.legislation.gov.au/Details/C2018C00292

Rights and responsibilities. (n.d.). Office Of Australia Information Commissioner. Retrieved March 16, 2021, from https://www.oaic.gov.au/privacy/the-privacy-act/rights-and-responsibilities/

Taking photographs and other images. (2010, August 17). Australian Law Reform Commission. https://www.alrc.gov.au/publication/for-your-information-australian-privacy-law-and-practice-alrc-report-108/69-particular-privacy-issues-affecting-children-and-young-people/taking-photographs-and-other-images/

Thomas, G & Nelson, K. (2008). Communication skills. In D. McDermid (Ed.), *Ethics in ICT: an Australian perspective* (1st ed., p. 303–327). Pearson Education Australia.

Thomson, J. (2008). Com puter law, Ethics and Intellectual property. In D. McDermid (Ed.), *Ethics in ICT: an Australian perspective* (1st ed., p. 199–228). Pearson Education Australia.

Thomson, P. (2008). Cyberspace. In D. McDermid (Ed.), *Ethics in ICT: an Australian perspective* (1st ed., p. 125–162). Pearson Education Australia.

Trade Marks Act 1995 (Cth). https://www.legislation.gov.au/Details/C2019C00085

Trade Mark Basics. (2019, June 12). IP Australia. https://www.ipaustralia.gov.au/trade-marks/understanding-trade-marks/trade-mark-basics

US$1.7 Million Stolen From North Carolina County After BEC Scammers Posed as Contractor. (2019, August 1). Trend Micro.

Warren, M. (2008). Computer crime. In D. McDermid (Ed.), *Ethics in ICT: an Australian perspective* (1st ed., p. 162–178). Pearson Education Australia.

What is a Honeypot? (n.d.). NC State University. Retrieved March 26, 2021, from https://ethics.csc.ncsu.edu/abuse/hacking/honeypots/study.php

What is a honeypot? A trap for catching hackers in the act. (2019, April 1). CSO. https://www.csoonline.com/article/3384702/what-is-a-honeypot-a-trap-for-catching-hackers-in-the-act.html