ACS Code of Ethics at TELSTRA Limited

Student Name (ID)
Faculty of Science, Engineering, and Technology
Swinburne University
Hawthorn, Australia
student@student.swin.edu.au

Telstra is one of the largest telecommunication firms in Australia. Founded more than 43 years ago, the firm has enjoyed rapid growth based on high-quality products it supplies in the market and strong customers' bases. However, in 2014 the company suffered from the breach of privacy of its customers. More than 15,000 private information about Telstra's clients were exposed to the public between 2012 to May, 2014 (Sharma, 2019). This information was however, made public by the Fairfax Media in May, 2014, a spread with various data relating to the consumers were found online with a google search. The data available in these spreadsheets included telephone numbers, the names of customers, their homes and business addresses (Sharma, 2019). Telstra is said to have been operating for all these period without tight security systems. The company was operating without passwords. As a result of this action, Telstra and the Australian investigative agencies were forced to take tough actions over the incident. Among them, the mitigation actions that were taken included the deactivation of more than 1200 information on some of the phone lines of the customers.

Investigations by the Australian Privacy Commission discovered that there were three National Privacy Principles that were breached by Telstra Limited. First, the company did not put in place appropriate strategies to ensure personal information of the customers were safe (Sharma, 2019). Second, the Telstra went ahead to destroy critical information that would assist in conducting further investigation on this incident. Additionally, the firm prevented the disclosure of this information to people. From this incident, Telstra agreed to take actions. (Sharma, 2019). The company replaced the software platform on which the breach of customers' privacy occurred. Telstra also reviewed its contracts relating to the handling of information with the third parties. The incident, however, was a clear breach of Ethical codes and Principles as required by the Australian Computer Society standards.

The Ethical Issue at Telstra

The ethical issue arising from this case is Honesty. According to this Code of Ethics, one is required to be honest in his presentations of knowledge, skills, products and services offered in the market. The code requires that any ICT manager should not breach some specific trusts vested to him by the stakeholders (ACS, 2014). The code further acknowledges that in the course of performing a duty, circumstances arise that where it appears to be beneficial for one to be deceptive. It, therefore, warns that such actions are likely to spoil the reputation of an institution and the individuals perpetrating them. In this particular case, it is clear that the company failed the honesty test upon the discovery of the violation of the customers' privacy. Upon identification of the flaws in their system, the company decided to destroy personal information it held and further prevented the exposure of this information to people. This was a clear act of dishonesty and violation of the ACS code of conduct.

ICT Profession

The ICT profession which was involved in this particular issue was the IT security. IT security is one of the modern professions in the ICT sector that works to ensure organizations data are kept away from the malicious digital attackers. With the help of Network Engineer, the IT security sets up, administers, maintains and upgrades the local and extensive areas of security network and system of an organization. IT security experts are also responsible for ensuring strong security of data, adequate storage, supporting steady billing and quick response to the disasters when realized (Burmeister, 2013). The flaws noted at the Telstra were due to lack of robust security system which made it easy for individuals to access the data on the spreadsheet just by google search. The IT security experts failed to put in place the security passwords which is critical in protecting the essential features of a company.

ACS Ethical Codes and their Associated Requirements

Honesty is one of the ACS ethical Codes that were violated in this case. The company failed the honesty test as entrusted to them by the clients. Upon the discovery of the leakages that were everywhere on the internet, they were unable to communicate with the clients or to the public the causes and impact of this incident. Telstra only communicated this act to the investigative authority (the Australian Privacy Commission) and was only willing to give the information enquired by the authorities. Further, the company's act of destroying the data to hide some of the evidence on the breach of customers' privacy was a sign of dishonesty to customers. Specifically, the *Principle 3.1* which requires that the ICT Practitioners should never knowingly mislead their clients or the potential customers on the suitability and the usability of the product or services was significantly violated in this case (ACS, 2014).

Competency is one of the ACS Ethical Codes arising from this case. The competency of the IT department of this company is a subject of further debate. The fact that the information of the customers could be found online just through a google search exposed the incompetence in the management. Even after the discovery of such flaws, the management failed to take appropriate mechanisms in time to the extent that private information of more than 1200 customers was exposed. The second principle of ACS code requires that every IT manager must perform his work comprehensively and with a lot of diligence. The inability of the IT department to conduct a thorough audit of their IT infrastructure and systems implies that due diligence was inadequately and inappropriately done. Under the same principle of competence, there was the violation of *Principle 2.1* which states that every ICT practitioner should endeavor to provide services that match both financial and operational needs of his employers and the clients were seriously violated in this case (ACS, 2014).

References

ACS. (2014). CS Code of Professional Conduct Professional Standards Board Australian Computer Society. Retrieved from: https://www.acs.org.au/content/dam/acs/rules-and-regulations/Code-of-Professional-Conduct_v2.1.pdf

Burmeister, O. K. (2013). Achieving the goal of a global computing code of ethics through an international-localisation hybrid. *Ethical Space*, *10*(4), 25-32.

Sharma, M. (2019). Telstra breaches the privacy of thousands of customers. Retrieved from https://www.smh.com.au/technology/telstra-breaches-privacy-of-thousands-of-customers-20140311-hvh92.html