Engineering ethics case study assignment

Art & Culture

Did the Sips that refuse to accept email from the black listed Sips do anything wrong? No, because they rely on blacklists, because It Is not legal to rely on blacklists. Even on investigations, investigators should not rely on blacklists. Http:// www. Cert.. Org/blobs/cert./post. CFML? Entered= 217 c. Who benefited from the organization's action? Sips because they were able to Identify addresses or Sips that contain spasms without taking a lot of actions. Many types of blacklists are legal. For example, a store may malignant a list of Individuals who have not paid their bills and deny them credit privileges. Similarly, credit reports can effectively function as blacklists by Identifying individuals who are poor credit risks. " http://elocutionary. Differentiator. Com/' Datelining d. Who was hurt by the organization's action? The innocent computer users that are affected by the actions of Sips. " Libel is a tort governed by State law.

State courts generally follow the common law of libel, which allows recovery of damages without proof of actual harm. Under the traditional rules of libel, injury is presumed from the fact of publication. " – http:// www. Law. Cornell. Due/wax/libel e. Could the organization have achieved its goals through a better course of action? No it's the best way to do it by not taking any big actions, they were still able to achieve its goals. F. As a computer engineer, is your course of action the same with the presented solution above? Why?

Or if different, what would that be? Yes, because I have no right to block an address who commits spam. " The real problem in blacklisting is proof, or rather, lack of proof. Very rarely will you have evidence that your old employer sabotaged you. More than likely, you will never discover anything other than you were suddenly terminated, or you didn't get the Job that had

seemed so promising moments before. This is one situation where an ounce of prevention is worth a couple of pounds of cure. ” http://www. Fascinate. Com/ defamation. Tm 2. Tatty JDK, Vice President for Legal and Human Resources Department of TABOO Corp.. , issues a memorandum advising all employees of TABOO that the corporation had acquired a SAPPHIRE which is capable of monitoring the activities done by each employee in their PC’s including personal email messages, chats and all the sites they visited in the net. Ms. Faying Banished, President of the Employee’s Union, criticized the memorandum and opined that such regulation is a violation of their of their rivalry rights guaranteed by the constitution.

Will you support the contention of Ms. Faying? Why or Why not? No. I will not support Ms. Faying Banished, because I know that employers may implement monitoring applications on all business-owned computers. Monitoring software can identify and circumvent any potential computer problems that might interfere with a workforces ability to perform their paid tasks but somehow the inclusion of personal e-mails should not be included in the monitoring system because it really violates the privacy and human right of an employee. Check the law below.

Employee Monitoring – Private Rights and Public Policy Employers should have an Acceptable Use Policy (AUP) in place that is made known to all their employees and they should be made aware that their computers and Internet activity are being monitored. Basically the law states that you can do whatever you want because the computers and the work done on them is your property. The following article appeared in the Journal “ Computer Law & Security Report”, Volvo 19 No 5. The Information Commissioner published

the final code of practice for the use of personal data obtained by employers as a result of monitoring at work (the “ Code”) n 11 June 2003.

I Nils article reviews ten coco Ana compares It to ten earlier rats published by the Data Protection Commissioner in October 2000 (the “ EDP Draft Code”) and the Information Commissioner in July 2002 (the “ ICC Draft Code”). The comparison will examine how in the field of data protection public policy resolves the common tensions between upholding private rights and supporting commercial interests. The proportionality and lawfulness of any monitoring is therefore determined by the employer’s Judgment of the benefits of any monitoring against the adverse impact of hat monitoring.

The Code sets out factors that should be considered when assessing adverse impacts, which include consideration of the level of intrusion into the private lives of the employees via interference with their private e-mails, telephone calls or other correspondence. In considering alternatives to monitoring, the Code recommends use of targeted or automated monitoring to reduce intrusion to employees in the workplace. The Code calls for employers to come to “ a conscious decision as to whether the current or proposed method of monitoring is Justified”.

This can only be achieved after a proper examination of the adverse impact of any monitoring and consideration of all alternatives to it. If employers wish to monitor their workers, they should be clear about the purpose and satisfied that the particular monitoring arrangement is Justified by real benefits that will be delivered. Workers should be aware of the nature, extent and reasons for any monitoring, unless (exceptionally) covert

monitoring is Justified. In any event, workers' awareness will influence their expectations. The area of most controversy has been the monitoring of electronic communications of employees.

The Code recognizes this by setting out a number of data protection issues and points that should be incorporated into employers' policies on the use of electronic communications. The Information Commissioner also includes under each guidance note in the Guidance a helpful list of key points and possible actions for employers to consider. The Guidance includes an explanation of the regulations made under the Regulation of Investigatory Powers Act 2000 that permit businesses in most cases to be able to intercept electronic communications (the " Lawful Business Practice Regulations").