EAST WEST UNIVERSITY

Department of CSE

Project 3 Report

Course Name: Cyber Security, Law and Ethics

Course Code: CSE 487

Section No: 03

Submitted To:

Rashedul Amin Tuhin

Senior lecture

Department of Computer Science and Engineering

East West University.

Submitted By:

Name: Nisarga Mridha

ID: 2020-2-60-010

Name: Sofia Noor Rafa

ID: 2020-1-60-226

Name: Md. Farhad Billah

ID: 2020-2-60-213

Date of Submission: 16/09/2023

Navigating Workplace Surveillance Ethics

Using Navigation Tools is useful to improve the work time. Consequently, employees will be unable to evade their work commitments. The company has the potential to generate significant profits and substantially boost its market share. Those handling these Tools programs should exercise caution to prevent any data leaks.

Scenario

A tech startup installs a keystroke logging software on its employees' computers. The company claims that the software is necessary to detect and prevent security breaches. However, some employees are concerned that the software could be used to track their personal browsing habits and communications.

One employee, in particular, is worried that the software could be used to expose his political views, which are different from the company's. He also worries that the software could be used to blackmail him.

Dilemma

Privacy vs. security: Keystroke logging software can collect a vast amount of personal data about employees, including their passwords, email communications, and web browsing history. This raises concerns about employee privacy. However, employers argue that keystroke logging software is necessary to protect the company from security breaches and data theft.

Accuracy vs. fairness: Keystroke logging software can be used to track employee productivity and identify employees who are spending too much time on non-work-related activities. However, this data can be inaccurate and unfair, especially if employees are using their work computers for personal tasks that are related to their job, such as checking social media for industry news or working on a side project.

Consent vs. coercion: Employers may argue that employees consent to having their keystrokes logged by using the company's computers. However, in many cases, employees may feel that they have no choice but to agree to the use of keystroke logging software, especially if they need the job. This raises concerns about employee coercion.

Brainstorming Phase

Stakeholders:

Employees, Tech Startup, Customers, Shareholders, Government Regulators, Civil Society Organizations.

Risks:

I. **Invasion of employee privacy:** Keystroke logging software can collect a vast amount of personal data about employees, including their passwords, email communications, and web browsing history. This raises concerns about employee privacy.

II. **Security breaches:** Keystroke logging software can be vulnerable to hacking and other security breaches. If an attacker were to gain access to keystroke logging data, they could use it to steal sensitive information or launch cyberattacks.

III. **Employee morale and productivity:** Employees may be less likely to be productive or innovative if they feel that their privacy is being invaded. They may also be more likely to experience stress and anxiety.

Issues:

I. **Invasion of employee privacy:** Keystroke logging software can collect a vast amount of personal data about employees, including their passwords, email communications, and web browsing history. This raises concerns about employee privacy.
II. **Security breaches:** Keystroke logging software can be vulnerable to hacking and other security breaches. If an attacker were to gain access to keystroke logging data, they could use it to steal sensitive information or launch cyberattacks.

Problems:

I. **Cost:** Keystroke logging software can be expensive to purchase and maintain.
II. **Complexity:** Keystroke logging software can be complex to install and operate.
III. **Scalability:** Keystroke logging software may not be scalable to large organizations.

Consequences:

I. Reduced employee morale and productivity
II. Increased stress and anxiety among employees
III. Increased risk of security breaches
IV. Negative publicity for the company
V. Potential legal action

Benefits:

I. **Improved security:** Keystroke logging software can help to improve security by detecting and preventing malicious activity.
II. **Increased productivity:** Keystroke logging software can be used to track employee productivity and identify areas where improvement is needed.
III. **Compliance:** Keystroke logging software can be used to ensure that employees are complying with company policies and procedures.

Possible Actions:

I. Disable the keystroke logging software. This is the most straightforward action, and it would completely eliminate the risks and concerns associated with using this technology.
II. Limit the data that is collected by the keystroke logging software. For example, the company could choose to only collect data on keystrokes that are made on work computers and during work hours.
III. Provide employees with more information about how the keystroke logging software is used and how their data is protected. This could be done through training sessions, company policies, or other forms of communication.
IV. Allow employees to opt out of having their keystrokes logged. This would give employees more control over their privacy.
V. Implement a policy that requires employees to consent to the use of keystroke logging software before it is installed on their computers. This would help to ensure that employees are aware of the potential risks and benefits of using this technology before they agree to it.
VI. Conduct regular audits of the keystroke logging software to ensure that it is being used in accordance with company policies. This would help to prevent the software from being misused or abused.

Analysis Phase

Responsibilities of the Decision Maker:

I. General ethical responsibilities:

a) **Respect for autonomy:** The decision maker should respect the autonomy of employees and allow them to make informed decisions about their privacy.
b) **Non-maleficence:** The decision maker should avoid harming employees by installing keystroke logging software without their consent.
c) **Beneficence:** The decision maker should weigh the potential benefits of installing keystroke logging software against the potential risks to employee privacy.
d) **Justice:** The decision maker should ensure that the use of keystroke logging software is fair and equitable.

II. **Professional ethical responsibilities, ACM/SE Code of Ethics:**

a) **Competence:** The decision maker should have the necessary competence to evaluate the risks and benefits of installing keystroke logging software.

b) **Responsibility:** The decision maker should take responsibility for the consequences of their decision.

c) **Fairness:** The decision maker should be fair and impartial in their decision-making process.
d) **Honesty:** The decision maker should be honest and transparent in their communication with employees about the use of keystroke logging software.

Rights of Stakeholders:

I. **Employees:**
a) Negative rights:
i. The right to privacy
ii. The right to freedom from surveillance
iii. The right to control their own personal data
b) Positive rights:
i. The right to be informed about the use of keystroke logging software
ii. The right to opt out of having their keystrokes logged
iii. The right to have their keystroke data protected

II. **Tech startup:**
a) Negative rights:
i. The right to protect its intellectual property
ii. The right to maintain the security of its systems and data
b) Positive rights:
i. The right to use keystroke logging software to protect its systems and data
ii. The right to use keystroke logging software to improve its security

Impact of the action options on the stakeholders:

I. **Action option 1: Disable the keystroke logging software.**
a) **Impact on employees:** Employees would be relieved to know that their keystrokes are no longer being monitored. They would have more privacy and control over their personal data.
b) **Impact on the tech startup:** The tech startup would lose some of the security benefits of keystroke logging software. However, the tech startup would also avoid the potential negative impacts of keystroke logging software, such as decreased employee morale and productivity.
c) **Impact on other stakeholders:** Consumers and competitors would be reassured that their personal data is being protected.

II. **Action option 2: Limit the data that is collected by the keystroke logging software.**

a) **Impact on employees:** Employees would still have some of their keystrokes being monitored, but the amount of data that is collected would be limited. This would reduce the impact on employee privacy.

b) **Impact on the tech startup:** The tech startup would still have some of the security benefits of keystroke logging software, but the benefits would be reduced.

c) **Impact on other stakeholders:** Consumers and competitors would still be concerned about the potential for keystroke logging software to be used to collect personal data.

III. **Action option 3: Provide employees with more information about how the keystroke logging software is used and how their data is protected.**

a) **Impact on employees:** Employees would be more informed about the use of keystroke logging software and would be able to make more informed decisions about their privacy.

b) **Impact on the tech startup:** The tech startup would demonstrate its commitment to employee privacy and would build trust with its employees.

c) **Impact on other stakeholders:** Consumers and competitors would be reassured that the tech startup is taking steps to protect employee privacy.

IV. **Action option 4: Allow employees to opt out of having their keystrokes logged.**

a) **Impact on employees:** Employees who are concerned about their privacy would be able to opt out of having their keystrokes logged. This would give employees more control over their privacy.

b) **Impact on the tech startup:** The tech startup would lose some of the security benefits of keystroke logging software, but the tech startup would also avoid the potential negative impacts of keystroke logging software on employees who are concerned about their privacy.

c) **Impact on other stakeholders:** Consumers and competitors would be reassured that employees have the ability to opt out of having their keystrokes logged.

V. **Action option 5: Implement safeguards to protect employee privacy, such as limiting the data that is collected and stored, and encrypting the data.**

a) **Impact on employees:** Employees would be more confident that their keystroke data is being protected.

b) **Impact on the tech startup:** The tech startup would be able to demonstrate its commitment to employee privacy.

c) **Impact on other stakeholders:** Consumers and competitors would be reassured that the tech startup is taking steps to protect employee privacy.

Analysis of consequences, risks, benefits, harms, and costs for each action considered:

I. **Action option 1: Disable the keystroke logging software.**

a) Consequences:

i. Employees would have more privacy and control over their personal data.

ii. The tech startup would lose some of the security benefits of keystroke logging software.

iii. Consumers and competitors would be reassured that their personal data is being protected.

b) Risks:

i. The tech startup could be at increased risk of security breaches.

ii. The tech startup could be at risk of legal liability if it is found to have failed to protect employee data.

c) Benefits:

i. Employees would have more trust in the tech startup.

ii. The tech startup could avoid negative publicity.

d) Harms:

i. The tech startup could be at increased risk of security breaches.

ii. The tech startup could be at risk of legal liability if it is found to have failed to protect employee data.

e) Costs:

i. The tech startup would lose some of the security benefits of keystroke logging software.

II. **Action option 2: Limit the data that is collected by the keystroke logging software.**

a) **Consequences:**

i. Employees would still have some of their keystrokes being monitored, but the amount of data that is collected would be limited.

ii. The tech startup would still have some of the security benefits of keystroke logging software, but the benefits would be reduced.

iii. Consumers and competitors would still be concerned about the potential for keystroke logging software to be used to collect personal data.

b) **Risks:**

i. The tech startup could be at increased risk of security breaches if the limited data that is collected is not properly protected.

ii. The tech startup could be at risk of legal liability if it is found to have collected more personal data than is necessary for security purposes.

c) **Benefits:**

i. Employees would have some privacy protection.

ii. The tech startup could still benefit from some of the security benefits of keystroke logging software.

d) **Harms:**

i. Employees could still be concerned about their privacy.

ii. The tech startup could still be at risk of security breaches and legal liability.

e) **Costs:**

i. The tech startup would need to implement safeguards to protect the limited data that is collected.

III. **Action option 3: Provide employees with more information about how the keystroke logging software is used and how their data is protected.**

a) **Consequences:**

i. Employees would be more informed about the use of keystroke logging software and would be able to make more informed decisions about their privacy.

ii. The tech startup would demonstrate its commitment to employee privacy and would build trust with its employees.

iii. Consumers and competitors would be reassured that the tech startup is taking steps to protect employee privacy.

b) **Risks:**

i. Employees may still be concerned about their privacy, even if they are provided with more information.

ii. The tech startup could be at risk of legal liability if it is found to have failed to protect employee data, even if employees were provided with information about how the data is collected and protected.

c) **Benefits:**

i. Employees would have more trust in the tech startup.

ii. The tech startup could avoid negative publicity.

d) **Harms:**

i. Employees may still be concerned about their privacy.

ii. The tech startup could be at risk of legal liability.

e) **Costs:**

i. The tech startup would need to develop and implement a privacy policy and training for employees on how to use the keystroke logging software.

IV. **Action option 4: Allow employees to opt out of having their keystrokes logged.**

a) **Consequences:**

i. Employees who are concerned about their privacy would be able to opt out of having their keystrokes logged.
ii. This would give employees more control over their privacy.
iii. The tech startup would lose some of the security benefits of keystroke logging software, but the tech startup would also avoid the potential negative impacts of keystroke logging software on employees who are concerned about their privacy.
iv. Consumers and competitors would be reassured that employees have the ability to opt out of having their keystrokes logged.

b) Risks:

i. The tech startup could be at increased risk of security breaches if employees who opt out of having their keystrokes logged are still able to access sensitive data.
ii. The tech startup could be at risk of legal liability if it is found to have failed to protect employee data, even if employees had the ability to opt out of having their keystrokes logged.

c) Benefits:

i. Employees would have more privacy protection.
ii. The tech startup could avoid negative publicity.

d) Harms:

i. Employees who opt out of having their keystrokes logged may still be concerned about their privacy.
ii. The tech startup could still be at risk of security breaches

Kant’s, Mill’s, and Rawls’ approaches:

I. Kant's Deontological Theory

Kant's categorical imperative states that we should act only according to maxims that we can will to be universal laws. In the context of scenario 2, this would mean that the tech startup should not use keystroke logging software unless it is something that it would be willing for all companies to do.

Kant would argue that keystroke logging software is a violation of employee privacy, and therefore it would be wrong for the tech startup to use it, even if it believes that it is necessary for security purposes. Kant would also argue that it is wrong for the tech startup to use keystroke logging software without the consent of its employees.

II. Mill's utilitarianism

Mill's utilitarianism states that we should act in a way that produces the greatest good for the greatest number of people. In the context of scenario 2, this would mean that the tech startup should weigh the potential benefits of using keystroke logging software against the potential harms.

Mill would argue that the potential benefits of using keystroke logging software include improved security and reduced risk of fraud. However, Mill would also argue that the potential harms of using keystroke logging software include a loss of employee privacy and trust.

Mill would likely conclude that the tech startup should not use keystroke logging software unless the potential benefits outweigh the potential harms. However, if the tech startup does decide to use keystroke logging software, Mill would argue that it should take steps to mitigate the harms, such as by providing employees with more information about how the software is used and how their data is protected.

III. Rawls's veil of ignorance

Rawls's veil of ignorance is a thought experiment in which we imagine ourselves behind a veil that prevents us from knowing our own identity, social status, or other personal characteristics. From behind the veil, we are asked to design a society that is fair and just for everyone.

Rawls would argue that the tech startup should not use keystroke logging software if it would not be acceptable for all companies to do so. Rawls would also argue that the tech startup should not use keystroke logging software without the consent of its employees.

Rawls would believe that employees have a right to privacy, and that the tech startup should not violate that right without a compelling reason. Rawls would also believe that employees should have the right to choose whether or not they want to be monitored by keystroke logging software.

Categorization of ethically obligatory, ethically prohibited, and ethically acceptable:

I. Provide employees with more information about how the keystroke logging software is used and how their data is protected.

II. Allow employees to opt out of having their keystrokes logged.

Decision Phase

I. Ethically acceptable options:

a) Report the project to supervisor. This is the most direct way to address the ethical concerns, and it is ultimately your responsibility to ensure that your work is being used for good. However, it is important to be aware that your supervisor may not be receptive to your concerns, or may even retaliate against you.

b) Talk to other engineers on the project about your concerns. This can help to build support for your position and to develop a plan of action. However, it is important to be careful about who you talk to, as you don't want to put yourself or your colleagues at risk.

c) Report the project to a higher authority, such as the agency's ethics board or the government's inspector general. This can be a more difficult and risky option, but it may be necessary if your supervisor is not willing to address the problem.