Helmut Cespedes

Professor O'Neill

11/21/2025

CSCI 419

Social, Ethical, and Legal Issues Paper

With the explosive era of data that the world is currently experiencing, great risks come, especially in the workplace. We are given the scenario in which a newly hired database administrator is asked by the company owner to design a system capable of storing and analyzing employee monitoring data. The data includes the employee's keystrokes, phone interactions, and work emails. From the point of view of the company owner, this serves to boost company productivity by keeping employees under wraps, but it also raises some concerns about the legality and ethics of this practice. This paper will go over the legal and ethical implications of collecting such information with the goal of providing a middle ground in which personal ethics and the law are not violated.

To evaluate whether the proposed monitoring system is advisable, we will begin by examining the legality of it. Clyde's request for the data is mainly governed by two federal laws. The Electronic Communications Privacy Act of 1986 regulates the monitoring of electronic communications, including email and computer use. While businesses are free to monitor these, and when you are employees of said business, you relinquish the right of privacy. The business must still adhere to a legitimate business purpose and must provide the employees with prior consent to said monitoring (18 U.S.C. § 2511(2)(a)(i)) (18 U.S.C. § 2511(2)(d)). Since Clyde confided to me that he has already been collecting this information, he is in violation of the law.

As to his statement of reasoning for this monitoring, getting a "good day's work" out of your employees can be seen as too vague of a description to hold up in court; thus, he is in complete violation of the ECPA of 1986. Furthermore, the Stored Communications Act, a part of the ECPA, specifically addresses the legality of stored communications, such as emails and phone calls. It states that violations of these privacies without prior authorization are a federal crime (18 U.S.C. § 2701-2712). Thus, Clyde is in complete violation of the statute and can face criminal charges as well as fines per employee.

Having established that the in-place monitoring practices already violate federal law, we must now examine the ethical dimensions. Even if the legal violations were corrected through proper notification and consent procedures, there remain underlying personal and Christian ethical concerns that must be addressed.

The main issue is whether an extensive consent form given to employees prior to further monitoring will truly respect the privacy of workers who are "honest workers," or whether it merely provides legal cover for invasive spying. This is a difficult situation that presents a conflict of interest. On one side, the company must have productive workers; on the other, it's important that workers don't feel forced into this invasive monitoring simply to keep their jobs.

As the DBA, I am asked to design a system that, as it currently stands, violates both legal standards and my own professional ethics codes. This conflict places me in a position where I must choose between employment security and professional integrity.

ACM Principle 1.6 states "only the minimum amount of personal information necessary should be collected in a system." The proposed system would cause me to violate this principle in several ways.

ACM Principle 1.7 states "respect the privacy of others, and honor confidentiality." I must adhere to this and handle sensitive information diligently. By implementing a system that scans personal correspondence and monitors private conversations, I would be violating this employee confidentiality.

IEEE Principle 1 states "Hold paramount public safety, health, and welfare." This principle requires professionals to prioritize the wellbeing of the public; this includes the workers I am being asked to store information on.

As a Christian, this monitoring should also raise concerns to you, Clyde. While I respect your view of "the Christian value of a good day's work for a good day's wage," I believe we must examine whether your proposed system is supported by the teachings of our Lord.

As commanded in Colossians 4:1, "Masters, treat your bondservants justly and fairly, knowing that you also have a Master in heaven" (The Holy Bible, Colossians 4:1). While not directly related to an employee-employer relationship, it serves to prove a point: justice and fairness to your employees.

In Proverbs, King Solomon wrote, "A false balance is an abomination to the LORD, but a just weight is his delight" (The Holy Bible, Proverbs 11:1), in which he declares that the Lord detests dishonesty and unfairness, especially in business dealings. I present these scriptures respectfully, recognizing that you have identified Christian values as foundational to your business philosophy.

This is a difficult situation that presents a conflict of interest. On one side, the company must have productive workers; on the other, it's important that workers don't feel forced into this invasive monitoring. As the DBA, I am asked to design the system that, as it stands, violates legal

standards and my own professional ethics. There are several factors we must look at to clarify this situation. First, employees not only have a right to privacy but also a natural personal interest in privacy. Second, Clyde needs to improve business productivity and ensure employees fulfill their obligations. Third, the company must adhere to the law in order to become a long-term successful business. Fourth, once this privacy practice is in place, future company employee-employer relationships can be harmed.

We must determine the implications of this system. If we move forward with the monitoring protocol (after some revising), potential benefits include increased employee productivity, less theft, and company growth. Downsides include damaged employee-employer relationships, increased workplace stress, increased dissatisfaction, and the creation of fear of management. If monitoring is not placed, potential benefits include employee trust and increased morale, as well as avoidance of legal risks. It could also cause some potential harm, like failing to address the current productivity concern. Based on the legal analysis, professional ethics requirements, and Christian principles ethics examination, I have decided that I cannot implement the monitoring system as currently proposed.

In conclusion, my recommendation is to not implement the system as proposed. You must immediately act and stop the current data collection system to avoid criminal charges. While I cannot in good conscience complete this system I am asked to do, I can propose a different approach. Instead of invasive spyware, the company can implement a limited monitoring system. With employee consent, the system can monitor business emails and business-related phone calls. While harder to implement, it can work as a safeguard from the law and also allow employees to still have the freedom they deserve, such as using their personal accounts at work. With this

information, the business can see how to improve the work being done rather than just forcing productivity through fear.

Works Cited

United States Code, Title 18, §§ 2510–2522. ***Legal Information Institute***, Cornell Law School, https://www.law.cornell.edu/uscode/text/18/part-I/chapter-119. Accessed 21 Nov. 2025.

United States Code, Title 18, §§ 2701–2712. ***Legal Information Institute***, Cornell Law School, https://www.law.cornell.edu/uscode/text/18/part-I/chapter-121. Accessed 21 Nov. 2025.

Association for Computing Machinery. ***ACM Code of Ethics and Professional Conduct***. 2018, www.acm.org/code-of-ethics. Accessed 21 Nov. 2025.