# Essay on legal and ethical issues in information technology

Business, Company

## Abstract

The workplace of today is not the workplace of even a decade ago. As electronic communications and applications change the way companies do business, employees also change behavior that have not been previously addressed. For instance, the ACM and IEEE computer societies have a common goal of promoting computing and their members by providing resources and behavior guidelines. Each society established a Code of Ethics to address legal and ethical questions that may arise in the pursuit of computing professions.

While employees adopt ethical behavior, companies face the need to monitor the behavior. Data theft, irresponsible access to sensitive information, and breach of confidentiality are only some of the issues businesses address in the current age of electronics.


## Legal and Ethical Issues in Information Technology

The Association for Computing Machinery (ACM) and the Institute of Electrical and electronics Engineers (IEEE) are scientific and educational computing societies providing resources to members. These resources include career assistance, conferences, and publications. Both societies promote the standing of computing as a profession and science. The ACM and the IEEE have developed a Code of Ethics as reference for their members when occasions arise concerning ethical or legal questions. While similar in many ways, there are some differences in the Codes.

First, the IEEE addresses the possibility of conflict of interest and full disclosure in the event this occurs (IEEE Computing Society 2014). The

equivalent may have been included in two statements in the ACM code about honoring property rights and having honesty with trustworthiness, but that is unclear (ACM. com 2014). Next, the IEEE mentions refusing bribes, also probably under statements of honesty and avoiding harm in the ACM Code. They both promote competency and quality of work, accepting criticism, and giving credit to others when appropriate. The IEEE is explicit in discrimination policy while the ACM merely states not to discriminate. Neither society advocates harm to others, but the IEEE encourages its members to help others in their development of professionalism.

The ACM Code of Ethics has four sections grouped under Moral, Professional, Organizational Leadership, and Code of Compliance. The IEEE lists ten statements in its Code, and they are less general than those used by the ACM. The Code of Ethics for the ACM is much longer and addresses ethics for leadership, but this does not render the Code for the IEEE as inadequate. The IEEE puts more narrow focus on issues such as bribery and conflict of interest while the ACM Code offers generalized guidelines that allow a person latitude to read specifics into them.

The Code of Ethics for both societies could benefit from the example of each. The ACM Code allows too much latitude by vague generalizations. The IEEE Code restricts itself by its brevity and specific instances. A more applicable Code of Ethics would bring specificity to statements while still allowing interpretation across circumstances.

## Employee Right to Privacy

A company has a right to maintain security within the operation of its business, but where does the rights of the company violate the rights of the employees? According to EmployeeIssues. com (2014), employees have no rights to privacy as long as the surveillance is for the protection of the company's data. There are a number of ways an employer tracks the actions of its employees. Sophisticated software records use of the internet and emails, telephone numbers dialed and conversations, computer keystrokes and the files accessed, and how long an employee stays on a particular call. Employees see cameras in sensitive areas, but they may not see hidden monitoring devices. It is not required for employees to notify employees of any type of surveillance.

In fact, some companies go so far as monitoring blogs, personal websites such as Facebook, and other social networks. According to the law, this activity is not illegal, as long as it doesn't violate the National Labor Relations Act. The NLRA states an employee cannot be penalized for taking part in a group activity that is protected (National Labor Relations Board 2014). For instance, an employee was terminated following the posting of a YouTube video complaining about hazardous workplace conditions. The NLRB investigated and the employee received back pay, although he decided not to return to employment at that company.

On the other hand, the surveillance of employees is only for the purpose of protecting the interests of the company. If the activities cross into the area of voyeurism, employees have grounds for lawsuit for violation of privacy. Managers understand that use of personal emails and telephones in the

workplace are a drain on productivity, as is any other time spent on personal matters. The use of cell phones is a potential threat to security since mobile phones have the ability to type sensitive information and take photographs; it is also possible to overhear conversations with other clients in the background. In terms of lost productivity, a policy limiting the use of cell phones in designated areas on breaks is effective. The policy requires explanation of penalties in the event the employee uses the phone inappropriately. Provisions need to be put in place for contact in case of emergency. Any other reason can wait until a time when the employee is on break.

When discussing the use of the internet for personal use, the issue of productivity and security returns. Many company install locks on workplace computers to prevent employees at certain levels from accessing the internet. Management may need access, but this level of job responsibility assumes reliability. If an employee has the ability to use the internet from a work station during periods when he is expecting to be performing his job, he may check his personal email or go to websites for entertainment. Security issues come into play when he can send sensitive information to himself or someone else. The following statistics are only a few of the disturbing numbers concerning employee use of the internet:

- 70% of all workplace internet visits to pornographic sites occurs between the hours of 9am and 5pm.
- 58% of industrial espionage is performed by former or current employees.
- 64% of surveyed employees state they use the internet during working hours for personal purposes.

- 37% of employees surveyed state they surf websites not related to work constantly while on the job.

In light of these statistics, it’s not surprising 78. 7% of major companies operating in the United States monitor employees by videotape, checking their email, reviewing internet usage and files accessed, and listening to telephone calls (Staff Monitoring Software Solutions, 2014).

## Conclusion

Companies have an obligation to their clients and a responsibility to their business to maintain security measures with employees. Evaluating productivity is a constant activity for management, and employees using time of the job for personal business is a concern. The creation of societies resembling the ACM and the IEEE are a step toward promoting ethical computing behavior, looking to prevent legal problems for both the employee and the company for which they work.

## References

Acm. org. (2014). Welcome — Association for Computing Machinery. Retrieved 3 December
2014, from http://www. acm. org/

Employeeissues. com. (2014). Employee Workplace Privacy Rights. Retrieved 3 December
2014, from http://employeeissues. com/workplace_privacy. htm

Computer. org. (2014). IEEE Computer Society - Premier Organization of Computer
Professionals. Retrieved 3 December 2014, from

http://www. computer. org/portal/web/guest/home

Nlrb. gov. (2014). National Labor Relations Act | NLRB. Retrieved 3 December 2014, from http://www. nlrb. gov/resources/national-labor-relations-act

Staffmonitoring. com. (2014). Useful Employee Internet Abuse Statistics. Retrieved 3 December 2014, from http://www. staffmonitoring. com/P32/stats. htm