Ethical Issues: Privacy Issues on Using Personal Mobile Devices for Work

Employers and employees alike have duties and responsibilities when it comes to work-related activities including the use of information technologies. Employers practically and legally have the ownership rights on the company computers and information technology devices that include mobiles devices such as smart phones and such give them the rights to monitor the communication exchanges and see what the employees are doing and working on with the devices used. The situation can get quite complex when the employees use their personal mobile devices in work-related activities. Employers have the rights to control and monitor the computer and mobile devices used. Common laws practically suggest the employees may also have the rights to their personal property, personal information, and personal activities. Things, however, change with due legal considerations in work-related activities. Employees allowed to use personal mobile devices practically loss much of their privacy rights.

Employers generally have the rights to monitor the company computers to check on all activities that could have impacts to the workplace. The companies have legal obligations to abide to and that puts risks of liabilities to the employers. That has compelled and have legally allowed the employers to monitor all electronic devices and electronic communications and activities of the employees particularly that electronic evidences have become significant in lawsuits and investigations (Privacy Rights Clearinghouse, 2016). Practically and legally, employees generally have limited rights on their privacy when using computer devices at work. The constitutional First Amendment confers protection on freedom of speech but legislations also set conditions on the employees’ freedom of speech at workplaces. The issue can get complex when the employees bring and use their personal mobile devices and continuously using it for personal activities and for work purposes. Such device then becomes a gadget that
contains both personal and work-related information. As the mobile device contains company information, the employee owning the mobile personally losses rights to privacy as employers can legally put control and gain access to the mobile device. It is one device and the employers may not be prevented or prohibited to check on and even delete personal information of the employee owning the device. With employer monitoring software, the employers can even access the mobile remotely and do the surveillance even when the employee is off from the work (Privacy Clearinghouse, 2014).

Looking at the laws, the employee using personal mobile may assume legal rights. Starting with US Constitution, nowhere has the constitution clearly stated conferring protection on rights to privacy. The Bill of Rights does have provisions on rights to privacy but nothing, so far, related to personal technology devices and communication. Generally, the US Constitution and labor-management laws that include the National Labor Relations Act (NLRA) cover too limited coverage on matters about interception of electronic communications (Privacy Rights Clearinghouse, 2016). Furthermore, with the advent of the revolutionizing information technology, information-technology related laws also evolved such as the data protection act. The legislation confer some protection on privacy and confidentiality of personal information while using information technology but applicable laws also exist with regards to personal data protection at workplaces. While employees wish to protect their privacy, the employers also fulfill their obligations to protect the company data and information such as the trade secrets and confidential information to safeguard the business interests and brand integrity. The use of mobile devices opens lots of risks to the company and that support giving full rights to the employers to closely monitor the mobile devices used in company-related activities (Privacy Rights Clearinghouse, 2014).
The Fourth Amendment states protection from unreasonable searches and seizures the personal effects (Privacy Rights Clearinghouse, 2016). In the situation the employee uses personal mobile device, such legislation become questionable. The employers with rights to access to the employees personal devices can do the searches and activities of the employees such as looking at all files that can include going through the employees’ personal files, emails, and all activities done using the gadgets. Access to the gadget no longer needs passwords and such cannot be considered illegal access and would be hard to determine if employers carry out unreasonable searches (Blaauw, 2013).

Employees allowed to use personal mobile devices, indeed, practically loss much of their privacy rights. Whatever legal rights the employees have largely depend on the company policies and agreement with the employers with regard to the use of personal mobile devices for work purposes. For personal privacy protection, it would be hence wise for any employee to think many twice before using personal mobile devices both for personal and work use.
References


