Compliance and Security Risks for Bring Your Own Device Applications

7 Sep 2015

It has become a regular requirement for employees to work outside of the office, or while on the move. It is not uncommon to see people working with their smartphones on public transport, or in shopping malls, restaurants, and even holiday villages. The ability for employees to do business remotely increases productivity, while considerably reduces their need to stay at the office. However, given the lack of regulation and variety of practice in Turkey, it is advisable for companies to approach the topic with caution and take active steps to protect sensitive and confidential company data from inappropriate disclosure.

A short time ago, companies only provided smartphones or tablets to their senior managers. However, in recent years, these have become accessible to employees in all ranks through their own means, providing an important opportunity for companies to keep employees engaged in their business and workplace.

On the other hand, accessing employees through mobile devices or transferring information through such devices may lead to problems with company servers or programs, as well as with application compliance problems, blocking issues, or communication problems resulting from version incompatibilities or updating problems. In addition, using such devices raises risks in terms of compatibility, as well as security and compliance problems that can arise if a device is stolen or lost.

Each device poses a significant security and confidentiality risk for companies, depending on the device owner's position in the company and the degree of access which the employee has to important company data.

Despite this, technological developments in mobile devices, as well as portable and wearable computers, incline companies to take these risks by allowing use of Bring Your Own Device ("**BYOD**") applications and programs.

Surveys show that the number of mobile devices connected to networks has more than doubled since employees have been granted access to company data and information networks1. While this requires caution in network management and resource planning, it is an important method for enabling employees to work, even when they are outside of the office.

BYOD applications have become an irreplaceable part of business life on the basis that they increase employee satisfaction and productivity while decreasing company expenses. However, companies often struggle to keep up with technological developments and usage practices, so fail to introduce and maintain adequate measures to protect themselves against the changing risks.

Turkey lacks operational procedures which set rules and principles for mobile devices and BYOD applications. It is important to determine how companies should proceed in order to prevent disclosure of sensitive company data and to address conflicts of interest in cases where devices are stolen or lost. Conflicting interests in this context include the need to protect company data, competing with employees' privacy rights.

In Turkey, an employer's right to monitor and interfere with computers and e-mail addresses possessed by employees is uncontroversial, including e-mails communicated through such e-mail addresses. Turkish courts have held that deleting information through remote access from mobile devices provided to employees by the company will

not constitute invasion into the private life or privacy rights of the employees2.

However, there is no regulation or established precedent in Turkey addressing whether employers are entitled to monitor or interfere with devices which are owned by an employee but used for business purposes at the employee's own consent or request.

Consequently, if an employer monitors an employee's device, or interferes with the device in a loss/theft situation, these actions may be deemed to be an invasion of the employee's privacy. The determining factor will be whether the employer has obtained employee consent to interfere with devices used by the employees within the scope of BYOD applications and programs.

Due to understandable security reasons, if a personal portable device is stolen or lost, companies may choose to delete sensitive data through remote access methods. However, if employees have not given prior consent to delete data in this way, companies may encounter objections and complaints on the grounds of an invasion of privacy.

If a company is able to selectively delete only company data contained on the device, this reduces the risk of committing an invasion of privacy. However, it is not possible to prove that all company data contained on a stolen or lost device has been deleted via remote access. Therefore, the most secure method continues to be deletion of all data on the device, provided the employee has given prior consent.

A similar situation may arise when an employee resigns or is dismissed. It is natural for companies to consider it necessary to obliterate all company data from the employee's device. The most secure method for companies in this situation is again to delete all data contained on the portable devices, provided the employee has given prior consent. In practice, it is advisable to obtain such consent from employees during signing of the employment contract, since employees may resist cooperation in situations where the employee is being dismissed.

Accordingly, it is advisable for companies to take steps to avoid being deemed to have invaded their employee's private lives in the process of protecting confidential and important company information. For example, companies may choose to obtain an explicit written statement from employees who wish to use their own portable devices for business purposes within the scope of a BYOD program. If the statement gives unconditional authorization to the company to delete data from such devices, either directly or through remote access and the authorization applies to a wide scope of possibilities, including theft, loss, resignation, and employee dismissal, such statement may be a preferable method for protecting the employer against risks of data and confidential information leaking.

Furthermore, employee training may be held to raise awareness of how portable or wearable devices should be used within the scope of BYOD applications and programs, along with the associated risks. The training may include information about the circumstances under which the employee's consent to the company intervening and deleting data. Such training could be beneficial in mitigating the risks and preventing later disputes.

For example, the United States government published an instruction manual "toolkit" in 2012 addressing federal employees' use of personally-owned devices. Likewise, IBM adopted a BYOD policy in 2010. IBM prohibited employees using certain applications on devices which are used for business purposes. The prohibition was introduced on the grounds of "tremendous lack of awareness as to security risks". The ban applied to use of Dropbox and Siri, among others. IBM's concern was that since such applications are uncontrollable, employees may intentionally or unintentionally disclose confidential company data.

Companies should approach BYOD applications and programs with caution to ensure they are protected and risks are mitigated as far as possible. It is advisable for companies to provide training for their employees, establish procedures to mitigate data leakage and loss, acquire remote access technology, and inform their employees in this regard. Most importantly though, employers should obtain express consent from their employees to intervene in the devices within the scope of these procedures.

1. Cisco IBSG Horizon Survey Report

2. Court of Cassation 9 HD E.2009/447 K. 2010/37516 T. 13.12.2010

Related Practices

- Securities and Capital Markets
- Privacy and Data Protection
- Employment Disputes

Related Attorneys

- BURCU TUZCU ERS?N, LL.M.