International Municipal Lawyers Association
2014 Annual Conference
Baltimore, Maryland

Work Session VI: Technology: Bring Your Own Device to Work

The Benefits and Burdens of BYOD in a Municipal Workforce

Quinton M. Herbert
Deputy Labor Commissioner
Baltimore, Maryland

©2014 International Municipal Lawyers Association. This is an informational and educational report distributed by the International Municipal Lawyers Association during its 2014 Annual Conference, held September 10-14, 2014 in Baltimore, MD. IMLA assumes no responsibility for the policies or positions presented in the report or for the presentation of its contents.

The Benefits and Burdens of BYOD in a Municipal Workforce

Contents

I. Introduction……...1
II. Background…….2
III. The Benefits of BYOD……..….2
IV. The Burdens of BYOD……...3
V. Considerations for BYOD Policies…….5
VI. Conclusion……..

The Benefits and Burdens of BYOD in a Municipal Workforce

I. Introduction

Technology once reserved for the workplace and only provided by IT Departments is now widely available to consumers from a variety of sources including big box chain stores like Walmart. The introduction of devices like Apple's iPhone and iPad as well as Google's Android devices has led people to desire the same functionality and convenience in the workplace that they now purchase for their personal use. Consequently, an increasing number of businesses and organizations are opening their networks and data to consumer handheld mobile devices.[1] This trend has created a phenomenon known as the "consumerization of IT" which refers to the circulation of consumer devices into the business enterprise.[2] Bring your own device to work ("BYOD") is how employers have sought to address the increasing consumerization of IT in the workforce by allowing employees to utilize personally owned mobile devices in the workplace for use and connectivity on an institutional network under certain circumstances.[3]

While the development of new more advanced devices has provided for this technological shift, it has also highlighted a myriad of legal issues. Moreover, while BYOD has many benefits including increased employee morale and productivity, there are also many burdens from a management perspective including security of employer documents and third party access to mobile devices. Employer data is now available on very personal devices. Considerations such as the secure maintaining, storing and destruction of employer data, as well as breach notification and legal hold need guidelines on how management will proceed with employees' devices. This paper will highlight a number of the benefits, burdens and policy considerations so that attorneys can better assist government clients in drafting effective policies that properly balance the interest in protecting government work product while giving due consideration to the conveniences that BYOD may provide to employees and managers.

---

[1] Trend Micro (2012). *Enterprise Readiness of Consumer Mobile Platforms*. Retrieved from http://trendmicro.com/cloudcontent/us/pdfs/business/reports/rpt_enterprise_readiness_consumerization_mobile_platforms.pdf?cm_mmc=Affiliates-_-Internal-_-Cesare+Garlati-_-BringYourOwnIT

[2] International Data Corporation. (2011). 2011 *Consumerization of IT study: Closing the Consumerization Gap*. Framingham, MA; Gens, F., Levitas, D., & Segal, R. at p.1.

[3] Emory, Scott. *Factors for Consideration when Developing a Bring Your Own Device (BYOD) Strategy in Higher Education*. University of Oregon Applied Information Management Program Capstone Report (2012, July) at p.16. Retrieved from https://scholarsbank.uoregon.edu/xmlui/bitstream/handle/1794/12254/Emery2012.pdf (2011, June 29).

II. Background

The current trend toward the use of personally owned handheld mobile smart devices at work can be traced back to the unveiling of Apple's first iPhone in 2007 which was the first smart phone designed with a multi-touch interface.[4] Since then, a number of notable changes have taken place in the smart phone industry, including Google's introduction of the Android operating system; Hewlett Packard's acquisition of Palm; and Nokia's partnership with Microsoft to run Windows Phone 7 on new Nokia smart phone hardware.[5] Furthermore, as a result of the technological innovations introduced in Apple's first iPhone, consumer demand for smart phones is on the rise.[6] In fact, in 2011, worldwide smart phone sales hit 472 million units, a 58 percent increase from 2010.[7] Worldwide smartphone sales are projected to reach 1.1 billion units by 2015.[8] To put that in its proper context, as of this writing the population of the United States is just over 318 million.[9]

The functionality of mobile smart devices coupled with their affordability make them more appealable and accessible to a larger percentage of the workforce. With current technological trends, traditional workstations that employ an Ethernet cable for connectivity are becoming increasingly obsolete. Municipal employers are faced with deciding whether to implement a BYOD policy and if so, what that policy should entail.

III. The Benefits of BYOD

There are a number of benefits of implementing a BYOD policy including cost, convenience, flexibility, efficiency and morale. For employers, BYOD is cost-saving because in the traditional BYOD model the employee purchases the mobile device. The cost savings to employers that historically purchased a large number of computers or tablets is a tremendous financial benefit. Not only do employers save on the initial procurement costs for the technology, but also on the ancillary costs such as maintenance costs, software upgrades, and costs for repair or replacement of machines.

---

[4] Kim, R. *The iPhone effect: How Apple's Phone Changed Everything*. Gigaom. (2011, June 29). Retrieved from http://gigaom.com/2011/06/29/the-iphone-effect-howapples-phone-changed-everything/

[5] Emory, Scott. *Factors for Consideration when Developing a Bring Your Own Device (BYOD) Strategy in Higher Education.* University of Oregon Applied Information Management Program Capstone Report (2012, July) at p.89. Retrieved from https://scholarsbank.uoregon.edu/xmlui/bitstream/handle/1794/12254/Emery2012.pdf citing Kim, R. *The iPhone effect: How Apple's Phone Changed Everything*. Gigaom. (2011, June 29).

[6] *Id*.

[7] Emory, Scott. *Factors for Consideration when Developing a Bring Your Own Device (BYOD) Strategy in Higher Education.* University of Oregon Applied Information Management Program Capstone Report (2012, July) at p.89.

[8] *Id*.

[9] Retrieved from http://www.census.gov/popclock/ on July 25, 2014.

It is no secret that most of the technology purchased by employers becomes obsolete and in need of updating or replacement. By allowing employees to bring, and use, their own devices, they can always have up-to-date technology without the employer incurring the cost of providing new technology. For many employers, this practice has been extremely beneficial as significant funding can be trimmed from operating budgets. In short, an effective BYOD policy can help employers reduce large IT procurement and maintenance budgets while ensuring that employers benefit from the use of the latest technology by the workforce.

Additionally, BYOD can increase productivity and employees' morale.[10] In fact, recent studies show that an increase in employees' flexibility may lead to an increase in satisfaction, which eventually increases productivity and morale at the organizational level.[11]

IV. The Burdens of BYOD

While BYOD has a number of benefits for both employers and employees there are a number of risks (burdens) that employers must consider in crafting an effective BYOD policy. The four most frequently identified risks associated with BYOD are data leakage, loss of control and visibility, ease of device loss and potential discovery issues regarding data stored on an employee's mobile smart device.[12]

The storage of critical employer information on employee-owned devices poses a great threat to organizations due to either the intended or inadvertent disclosure of sensitive data. This data leakage can include confidential communications or proprietary company information. For example, sensitive documents downloaded onto an employee's device have the ability to be file-shared or stored with minimum security, thus exposing the employer to the risk of data breach.

Next, BYOD introduces new control challenges that can lead to other serious risks. BYOD presents significant security risks for organizations as

---

[10] Shim, JP, Mittleman, Daniel, Welke, Richard, French, Aaron M, & Guo, John C. (2013). *Bring Your Own Device (BYOD): Current Status, Issues, and Future Directions*. Paper presented at the Association for Information Systems ("AMCIS").

[11] Lebek, Benedikt, Degirmenci, Kenan, & Breitner, Michael H. (2013). *Investigating the Influence of Security, Privacy, and Legal Concerns on Employees' Intention to Use BYOD Mobile Devices*. Paper presented at the AMCIS.

[12] *See* Dedeche , Ahmed, Fenglin Liu, Michelle Le, Saeed Lajami. Emergent BYOD Security Challenges and Mitigation Strategy pp.8-9 ; See also Ghosh, A., Gajar, P. K., and Rai, S. 2013. *Bring Your Own Device (BYOD): Security Risks and Mitigating Strategies*, Journal of Global Research in Computer Science (4:4), pp 62-70; Miller, K. W., Voas, J., and Hurlburt, G. F. 2012. *BYOD: Security and Privacy Considerations*, IT Professional (14:5), pp 53-55; Morrow, B. 2012. *BYOD Security Challenges: Control and Protect Your Most Sensitive Data*, Network Security (2012:12), pp 5-8.

they no longer control the device that company data is stored on, hence the enforcement of security policies will be difficult for issues such as data leakage, theft, and regulatory compliance.[13] The question becomes one of ownership of the contents stored on the mobile device. Organizations have less visibility of the security environment for BYOD compared to a traditional networked environment.[14] As organizations increasingly lose control over the security of their terminal devices, employees have a more critical role to play in upholding organizational security.[15] As employers lose control of the devices the risk that malware can infect their network increases significantly.

Additionally, the relatively small size and portability of smartphones and tablets exposes BYOD devices, and the information stored on them, to a higher risk of being lost or stolen.[16] Recent data suggests that nationally, a mobile smart phone is lost every 3.5 seconds.[17] Lost or stolen devices potentially make sensitive information available to third parties. What compounds the problem of lost or stolen phones is the fact that, according to a recent CNBC study, only 36 percent of the smartphone users have set a basic 4-digit PIN to lock their phone.[18]

BYOD also presents risks and challenges with litigation hold procedures and how business documents created, stored or transmitted on an employee's personal smart device are captured and stored in accordance with established document retention and litigation hold policies. A cautionary tale about the importance of strong litigation hold procedures and BYOD is found in the Canadian case of *CIBC World Markets Inc. v. Genuity Capital Markets*.[19] In that case, CIBC sued Genuity, alleging it had stolen proprietary information from CIBC. CIBC argued that Genuity did not take sufficient steps to ensure that relevant documents and data were not destroyed. An investigation discovered that Genuity was not storing copies of all its employees' messages.[20]

Because of Genuity's failure to store all work-related messages of employees, the court permitted forensics experts to go to great lengths and expense to locate e-mail. They were granted access to all PCs, BlackBerries (smart mobile phones) and similar devices under the control of the Genuity's

---

[13] *Id*. Citing Miller, K. W., Voas, J., and Hurlburt, G. F. 2012. *BYOD: Security and Privacy Considerations*. IT Professional (14:5), pp 53-55 and Morrow, B.. *BYOD Security Challenges: Control and Protect Your Most Sensitive Data*, Network Security (2012:12), pp 5-8.
[14] *Id*.
[15] *Id*.
[16] *Id.*
[17] *Good-Bye Plastic, Hello Phone: Mobile Wallets On The Rise*, Retrieved from http://www.nasdaq.com/article/goodbye-plastic-hello-phone-mobile-wallets-on-the-rise-cm180390#ixzz38XSemeOm
[18] Weisbaum, Herb, *Most Americans Don't Secure Their Smartphones*. Retrieved from http://www.cnbc.com/id/101611330#.
[19] , O.J. No. 614 (S.C.J) (QL) [2005].
[20]

employees. The court's order included devices at home (like iPods, iPhones or Androids) and belonging to spouses and children.

The lesson from the CIBC v. Genuity case is that businesses allowing employees to bring their own devices to work would be wise to keep extensive, centrally- managed archives of all business-related e-mail (including webmail, SMS, MMS [multimedia message service], text messages and instant messages) by employees and other personnel. This will avoid the expense and potential liability associated with searches of employee's home computers and other personal devices.

Another risk or burden that is often overlooked is the fact that there is virtually no legal precedent and little analytical research to guide employers tasked with implementing policies around BYOD. Municipal attorneys should advise clients of the uncertainty of potential litigation arising out of a BYOD program. Moreover, the risks associated with BYOD make clear that BYOD policies must be crafted to provide protection to employers who entrust proprietary or confidential data to employees' mobile smart devices.

V. Considerations for BYOD Policies

There are a host of considerations for whether a BYOD policy should be implemented or not. These include suitability, policy, IT support, security and training.[21] It is important to note that due to variations in job duties and responsibilities, not every employee classification will be suitable for BYOD. For example, employees who handle sensitive or regulated data may not be good candidates for using their personally owned devices. Others employees may require specialized equipment or software that would be too expensive for an employee to purchase. Not only must the job classification be suitable for BYOD, the employee's device must be suitable as well. It is vital for employers to emphasize and ensure that any employee-owned device must be capable of performing the tasks necessary for the employee's job.[22]

Next, employers considering implementing BYOD must focus on crafting an effective BYOD policy. Technology is ever evolving and governance of policies must have the ability to quickly adjust to the constant technological advances. Policy governance must also represent a cross culture of a variety of disciplines such as IT, Finance, HR, and Legal. Policies should adequately reflect management's requirements relating to the requirements for the device itself as well as requirements for syncing, or connecting the device to the

[21] *See* Slottow, Tim. *Action Learning Project: Bring Your Own Device (BYOD)*. Presented at the University of Michigan Business and Finance Leadership Academy (21 November 2012). Retrieved from http://www.bf.umich.edu/bfleadership/docs/2012/byod-research-paper.pdf
[22] *Id.*

employer's network. In addition, the policy should outline what the penalties are for an employee's failure to follow the employer's BYOD policy.[23]

Another consideration for employers considering BYOD is IT support. IT Departments can often negotiate or renegotiate flexible licensing models with key vendors to provide access to software on employee-owned laptops or smart devices.[24] IT support would also entail looking at the network. With traffic from these employee devices going over the 3G / 4G (cellular) networks as well as the wireless networks, attention must be paid to both of those infrastructures.[25] To ensure security, BYOD policies should employ on-site and cloud-based options that allow employment related data to be securely stored. This will ensure the security of sensitive data while making employment related data accessible to the employer while reducing the risk of data leakage.

VI. Conclusion

With the ever changing technological landscape, and the reduction in IT procurement budgets, BYOD is becoming an option to more employers in both the private and public sector. However, jurisdictions should weigh the benefits of a BYOD program against the risks and create BYOD policies that address the security of employer data, the privacy of employees' personal information as well as risk management considerations of implementing BYOD. This writer recommends piloting a BYOD program with a small group of employees and noting the concerns and issues. Jurisdictions should then work collaboratively with employees, IT professionals and consultants to craft a workable and effective BYOD policy.

---

[23] *See id.*
[24] *Id*. at p. 19.
[25] *Id.* at p. 20.