BYOD: Policy, Practice, & Privacy. A Conversation
Presented by Cynthia M. Lambert for LibraryLinkNJ,*TechFest 2015*
Parsippany Public Library, January 21, 2015

What is BYOD?

BYOD stands for **Bring Your Own Device.** It is when employees are allowed or encouraged to use their personal mobile devices, including notebooks, phones, and tablets, for work (either on site or off). The term first appeared in 2009 via Intel[i], but only gained widespread use in later years as other companies began discussing their employees using personal devices at work. In 2012, the EEOC adopted a BYOD policy, ushering the era of this practice in government organizations[ii]. Even the White House has a BYOD policy at this point[iii].

Who BYODs?

According to Tech Pro Research, 74% of organizations either already using or planning to allow employees to bring their own device to work."[iv]

Why Should You Care?

Research has shown that even if you are not participating formally in BYOD, it is likely that your employees with Smart Phones (or wearables or a tablet) are likely already using these devices to do work. Think about your own device usage—do you use your phone to make business calls, send e-mails, or post to social media for your job when you are at the NJLA conference or an event like today's TechFest? If you said yes, you BYOD.

In NJ, BYOD has serious implication for both employers and employees because of the Open Public Records Act. The recent 'Bridgegate' scandal involving Governor Christie's aids sending e-mails about closing of the bridge entrance has highlighted this concern of BYOD[v]. Forbes recently reported[vi]:

> "One thing Gartner emphasizes is the importance of realistic public-sector BYOD policies. The report states, "Government IT organizations may have an illusion of control by either providing and managing those devices or issuing well-articulated policies to allow and manage employee-owned devices. However, the reality is that employees…can decide how much they want to use corporate information and applications versus personal information and applications." Gryth adds that BYOD can be even more contentious in government offices because employees' work devices are subject to public records requests."

Things to Consider With BYOD:

Are your employees already doing this?
Privacy—for the employee, the employer, the patrons
Risks – to the organization, the tax payers, and the employees: who replaces broken devices; how do you safeguard patron information; how do you control where/when your employees are doing work; how will you comply with OPRA requests if BYOD is in place; how do you ensure the device is being used for work; what happens when an employee leaves; etc.

These and more topics will be discussed at today's *TechFest* presentation.

Resources for Further Research:

NJ State OPRA Information: http://nj.gov/opra/
quick guide: http://www.nj.gov/grc/public/docs/Citizen's%20Guide%20to%20OPRA%20(July%202011).pdf
exemptions to OPRA: http://www.nj.gov/grc/public/eoexempt/

IBM: IBM has a nice summary of what BYOD is, what the risks are, and some considerations when creating a policy. Full disclosure, they do sell an Enterprise Product for helping employers to manage BYOD. http://www.ibm.com/mobilefirst/us/en/bring-your-own-device/byod.html

IT Manager Daily: A very broadly drawn policy template. http://www.itmanagerdaily.com/byod-policy-template/

Tech Republic: Another template for policy. http://www.techrepublic.com/blog/it-consultant/learn-byod-policy-best-practices-from-templates/

The White House: commentary on best practices, crafting a policy, considerations for security and privacy. http://www.whitehouse.gov/digitalgov/bring-your-own-device

American Bar Association: Discussion of Employee Rights vs Employer Needs/Concerns and Rights. http://www.americanbar.org/news/abanews/aba-news-archives/2014/08/collision_courseahe.html

California Case Law: This case may (or may not) completely change the BYOD landscape. http://www.computerworld.com/article/2599121/byod/california-cell-phone-ruling-poses-big-byod-challenge.html

Privacy Rights Clearinghouse: Workplace Privacy and Employee Monitoring
https://www.privacyrights.org/workplace-privacy-and-employee-monitoring

---

[i] Mobile: Learn from Intel's CISO on Securing Employee-Owned Devices. (n.d.). Retrieved January 14, 2015, from www.GovInfoSecurity.com
[ii] Blake Johnson, N. (2013, January 7). BlackBerry Strategizes For More U.S. Government Clients. Retrieved January 12, 2015, from http://www.defensenews.com/article/20130107/DEFFEAT02/301070014/BlackBerry-Strategizes-More-U-S-Government-Clients
[iii] Digital Services Advisory Group and Federal Chief Information Officers Council. (2012, August 23). Bring Your Own Devic. Retrieved January 10, 2015, from http://www.whitehouse.gov/digitalgov/bring-your-own-device
[iv] Hammond, T. (2015, January 5). Research: 74 percent using or adopting BYOD. Retrieved January 10, 2015, from http://www.zdnet.com/article/research-74-percent-using-or-adopting-byod/
[v] Cohen, R. (2014, January 9). Six Lessons for Non Profits from Chris Christie's Bridgegate Scandal. Retrieved January 10, 2015, from https://nonprofitquarterly.org/policysocial-context/23511-six-lessons-for-nonprofits-from-chris-christie-s-bridgegate-scandal.html
[vi] EMC Voice. (2014, June 25). The Tech Trends Making Government Smarter. *Forbes*.