Technology in the Workplace: A Balance of Power

An STS Research Paper
presented to the faculty of the
School of Engineering and Applied Science
University of Virginia

by

Tierra J. Peerman

March 25, 2020

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.

Signed: _________________________Tierra Peerman__________________

Approved: _____________Peter Norton_________________ Date ________4/29/2020______
Peter Norton, Department of Engineering and Society

Technology in the Workplace: A Balance of Power

Technology companies compete to sell personal electronic devices that are portable, easy to use and versatile. Such devices are now ubiquitous especially in the workplace. The devices introduce new complications at work, where they affect standards of efficiency and productivity. They have also changed how employees interact with each other, with their employers and with their clients. Personal devices have created a gray area in the workplace where there is a struggle for influence among employers and employees. This struggle affects how productive the workplace can be. This can determine how successful a company or other organization can be. Clients are involved too; if they feel that a company is not dependable or that they are not a priority, then they will find another place to take their business elsewhere. Experts in technology and human relations also influence the workplace norms by showing how devices affect productivity. The traditional workplace environment has changed, but this doesn't mean that employers should give in to every trend. Instead, there needs to be a balance of power that optimizes personal device use.

Review of Research

It is traditional for workplaces to reject the use of personal devices. However, devices have become smaller, more portable, and more user friendly, making them more desirable (Smith 2019). Personal devices are easily accessible, even where they are not permitted, blurring lines that divide work from home and personal spaces (Anandarajan 2016). Employees therefore must often assume more responsibility for time management. Some employees see uninterrupted access to their phones as a practical necessity (BYOD 2015). There is the compulsion to be in touch with resources and people at any and all times. Some companies try using company phones and devices, but it requires employees to have at least two sets of devices, making them rely on more than what is necessary (Messmer 2011). Employees want to avoid the “two pocket syndrome and prefer Bring Your Own Devices (BYOD) programs (Totten 2014). This dissatisfaction takes a toll on employees’ interests in their jobs (Messmer 2011). Company devices can relieve some communication restrictions, but they may not be up to date or user friendly. Many clients want to know they have access to the most advanced and efficient people and products working towards their needs (Calloway 2016). They want to be able to contact the company when they need to, for customer service or other needs (Calloway 2016). Clients want to feel like a priority. It’s concerning to clients when they see that a company has many internal struggles. Clients, employers and employees believe that at their best, technological advances can improve efficiency and simplify processes, including major enterprises and personal tasks (Kruse 2013). However, easy access to familiar personal devices can lead to certain attachments. The World Health Organization warns that personal devices and technology, especially video games and the like, can be addictive (Dodgen 2019). An employer cannot easily detect when personal devices use has become less of a tool for productivity than a tool abused. Employers who favor traditional standards agree how Roger Lipson, the founder of the accounting organization the Lipson Group Inc, says “executives [find] smartphone or tablet use in meetings is one of the most frequent comments in the ‘behaviors to stop’ category” (Kruse 2013). Because of such concerns, many employers, especially those over 40 and those earning higher incomes, see phone use at work as a symptom of slowing production (Washington 2013).

Resistance to Tradition

Traditionally, personal devices are not meant to be used within the office space or in meetings. This cannot continue to be the rule because of the resistance of the employees. The traditional methods and environments cannot survive and still remain productive and efficient. There needs to be a compromise. Aspects of the traditional workplace are needed and should continue as it progresses. Modifications can be added to help highlight and assist the company and the aspects that are essential in having a productive workplace. However, there are resistances on both sides. James Brown, chief executive of Brown, Parker, DeMarinis Advertising, banned phones during meetings when his employees were distracted at his presentation. Brown found that when the new rule went into effect, he, like many employers with similar tactics, faced resistance (Simmons 2018). Extreme measures lead to strong resistance. The more the employer pushes for limitations and restrictions, the more the employee will do to push back or find a way around them. In a survey among employees aged 21 - 31 conducted by Fortinet, a network security firm, over 50 percent said that they would seek to find a way around company policies banning personal device use at work (Dillow). One way is to just sneak their devices around. For example, a Twitter user was at work when he chose to pull out his phone and record a music video of his favorite group, that he felt was underrated, playing close by. He captioned it with, "...We're not allowed to use/bring [a] phone at work, but my babies are worth the risk" (Twitter 2020). Employees feel that using their personal devices in certain situations is worth pushing back for. Another way employees try to find a way around the rules is by looking for flaws in the rules. An example of this is when an employee decided to ask fellow members in the Reddit community about what he titled his entry as "Employment Law" (Reddit 2020). He writes, ".... my employer told everyone we cannot have our phones on us at all and have it in our bags...someone told me it’s illegal for them to do so… . Is it illegal?” He believes it is worth questioning his employer’s authority, along with others he has talked to, to enforce phone restrictions. With employees focus shifting to ways to circumvent policies, their work pays the price by being an afterthought. The resistance of employees stems from not wanting the rigidness of the traditional work environment and its limiting ability to advance like in areas of their job. One twitter user was so happy about her job making the switch to a BYOD program that she posted, “... It’s important to use the right technology to support our work, especially when out supporting midwives in practice. #DigitalTransformation” (Twitter 2020). She not only supports her company’s decision, but she is willing to share with others how transforming the workplace is for a greater good. Many employees are accustomed to spending most of their waking hours interacting with screens (Osusch 2019). Having to drastically cut ties off from their personal devices and the connections they hold isn’t the way to avoid distractions from work. It could create distractions. This is where compromise is key. Allowing employees to know that they have access to their devices for certain means but could face consequences if they take advantage of it shows employees that they have a responsibility without making the employers completely powerless. Employees love the flexibility and the freedom to choose devices and know the means of access to those devices (Totten 2014). Thus, employers can get their employees to put forth more effort and provide better work by allowing them to work in more natural settings.

Compromising on how different work spaces can be adjusted to fit the needs of the employees as well as employers shrinks the level of resistance met by employers. At their best, technological advances can improve efficiency and simplify processes, including major enterprises and personal tasks (Kruse 2013). Tech companies rely on this advantage in order to help sell their products. Apple claims it makes its products accessible by “bringing the best user experience to its customers through its innovative hardware, software, and services" (Apple 2019). Tech companies give off the impression that they want their customers to thrive in many areas of their personal and professional lives and their products allow for this. Traditional work spaces, on the other hand, are not typically seen as environments that allow large growth or innovation. The restrictions of traditional environments compete with the social pressures to use personal devices in daily tasks, leading employees to resist conventional work spaces. It becomes easier for employees to develop their skills and work if all their tools aren't as spread out and interchangeable. Connections become stronger with personal devices being introduced into work spaces. Employees now have the opportunity to keep in touch with their employers, their clients and their families as they change environments (BYOD 2015). The midwife's twitter post encompassed this idea. By using the BYOD program, she can now help clients more out in her field of work and express how her clients appreciate the better connection they can now have with her. It's a win win for both parties.

With BYOD programs, companies can also reduce costs in some areas and employees can use devices they are familiar with. However, reduction of cost should not be the primary reason for integrating BYOD. Bulk discounts and simple IT systems reduce cost more when implementing company devices (Totten 2014). However, this usually outweighed by BYOD offering more opportunities for the company and the majority of employees encouraging BYOD spaces.

Building on Trust

Giving employees the responsibility that comes with having personal devices strengthens the trust between the employees and employers. Tech companies encouraging employees to use their devices to simplify tasks can be translated into their professional lives (Kruse 2013). Employers and employees sharing ways to use their devices to be more productive helps build a solid ground on personal device use. Feedback from both sides allow each side to reach an agreement on what policies work best for their environment and to provide the best relationships with clients. Those disinterested in personal device use push for less programs that integrate personal devices, aiming to eliminate practices of “behaviors to stop” (Kruse 2013). This line that is being drawn is meant to distinguish work from home, but it builds on the misunderstandings between employer and employee. Consultants and human resources can be a medium to help employees and employers meet in the middle (Prochepan 2018). Building this trust further allows for employees to focus more on their work than on their limitations.

Developing trust and reliability maintains a level of security of the company as well as the employers and employees professional and personal lives. As employers promote responsibility among their employees, they must show they are serious in protecting sensitive data (Top 10, 2019). Employees have to feel secure in order to effectively use their personal devices to promote their work. This doesn’t mean they have free range, but it does show that there is respect being given on both ends. If BYOD is used to monitor their info and their use of the devices, employees will feel that this is an invasion of privacy and ruin some levels of trust. Employers need to address what is considered company property and what protocols are put in place that monitor personal device use. A woman in her early 20s informed her twitter timeline that she had not been on twitter lately because, “ 1) my work is claiming they’re monitoring out laptop use at home ... 2) If I go on my phone I’ll get sucked into a hole and never do work” (Twitter 2020). This shows that her company has not clearly defined what spaces she has for personal use and to what level of monitoring they are doing. This does prevent her from being distracted on her laptop, but now she is more tempted to find other means of distraction and knows it will not help her work. If policies don’t lay out when and who can monitor what on personal devices, there will be more resistance met within BYOD environments. The problem with building trust then shifts to how to properly enforce guidelines when it is difficult to tell when use is personal or professional. Making this distinction clearer lies in how thorough policies are on personal device use in different spaces.

The Custom Fit Workplace

In order for personal devices to be integrated into the workplace successfully, there needs to be clear and precise rules customized for each workspace. These expectations should be determined prior to the integration. Before adopting a BYOD program, an employer must explain the driving forces behind this decision to ensure that the program and its implementation is what is best for the company (Totten 2014). In order to acquire a balance in the workplace, programs such as BYOD should only be used where it makes sense and is useful. Before BYOD can be useful, the rules must be understood (Top 10, 2019). At a minimum, any effective policy must define the scope of covered devices, appropriate use, cost, and support issues, implement security protocols, outline the consequences for violations, contain a mechanism for monitoring employee access and appropriate use, and require employee training (Totten 2014). As the company decides what their motives and goals are with BYOD programs, these are the areas that will set a strong foundation for their employees to develop and for the company to optimize its resources.

One of the biggest challenges with BYOD is the risk of misunderstandings with lost or stolen devices. Each personal device will enter and leave the workplace each day with company data. Thus, loss of device policies are crucial. The Juniper Networks' Third Annual Mobile Threat Report outlines: "A lost or stolen device, especially those without security settings like passwords, can present a significant risk to enterprises and consumers" (Totten 2014). The security of the company becomes vulnerable to outside forces, removing the power from the company if policies are not put into place to combat this. Survey found that half of their respondents said their company did not contain the ability to wipe data from a phone if lost, 28 percent said they were unsure if the company was able to remotely wipe data and majority did not know who to contact when in the situation of a lost or stolen phone (Totten 2014). This confusion shows their companies inadequately installed personal device use policies. Misunderstanding can also rise from improperly laying out the expectations of their employees. Taking steps to create a solid framework to protect sensitive data is often oversimplified (Top 10, 2019). If policies and expectations are not clearly defined in the beginning stages, it becomes difficult to handle the crisis of a lost or stolen device when it inevitably comes. The policies must be accompanied with viable methods that resolve lost device threats. Employers and employees need to know how and where to back up company data as well as how to separate it from personal info. A number of vendors now provide products that can control storage devices plugged into USB ports, and most offer the ability to control any mass-storage device plugged into other user-controlled interfaces (Garrity). Security settings like passwords and physical locks need to be required to protect devices, at an appropriate level, that store information from outside components.

Determining who has access to the devices' security features becomes another area to manage. Employers need to have well defined policies outlining procedures if devices are lost or stolen, including permission to track, locate, lock and wipe devices (Totten 2014). The legal costs of inappropriate handling of security features need to be understood with verbal and written agreements. The Computer Fraud and Abuse Act (CFAA) is the federal law that prohibits the intentional access of a computer without authorization or in excess authorization (NACDL 2020). The Stored Communications Act (SCA) prohibits intentionally accessing a facility through electronic communication services without authorization and intentionally exceeding authorization in order to obtain, alter or prevent authorized access to wire or electronic communication while it's in electric storage (U.S.C. 2010). These laws ensure consequences when broken, but it is the company's and employers' responsibility to define what "authorization" means and who has it in what areas. As authorization and who has it is being defined, employees and employers must understand what the punishments are. It also must be decided who is in charge of enforcing policies and who must report infractions. Human resource departments are a great enforcer because they can recommend ways to enforce policies and to ensure they are both reasonable and effective (Prochepan 2018). They also have power to explain and track what is expected of those in the company through written agreements and training. Employees and clients, along with employers, need to be ensured that their devices and data cannot be viewed without their permission. The policies put in place should reinforce security protection law while being able to take action when security is compromised. Security vulnerability like with data breaches, loss of intellectual property, trade secrets and the loss of personal and company information also presents the risk of legal costs (Totten 2014). This means that employees and employers need to have an understanding of what wifi networks are acceptable in joining. There also needs to be training to show what different networks can access. In a reddit thread titled "Don't use the office wifi on personal devices. You may be tracked," employees express their concerns about network tracking (Reddit 2020). Employers explaining safe practices to use with their secured networks against other networks will help build trust and secure data.

Expectations on what type of viruses and malware protective measures are expected need to be addressed. (Totten 2014). The distinction of what protective measures are the employees' responsibility and what measures are the company's responsibility must be understood to provide the best protection of devices and information.

There are experts in leadership such CEOs and entrepreneurs that offer their resources to those trying out certain programs (Simmons). It is advised not to ban the use of devices as a solution. Rather, the key is to minimise the possibility of data leakage without adversely affecting employee's ability to do their jobs (Garrity). The success of customizing the workplace depends on how well a community can implement the advantages of personal devices into a workspace through appropriate policies.

Challenging the Addiction

Understanding their addictive aspects and converging them with useful skills, takes full advantage of the pros of personal devices. Instead of training employees to fight the urges, there are ways to transform brain stimulation and evoked emotions into tasks that will make employers and employees feel more comfortable taking on new or more tasks. Millennials are three times more likely than those over the age of 40 to consider checking their devices in formal and informal settings as acceptable (Kruse 2013). It feels more natural for them to have access to certain information and devices. This may cause some companies to label spaces as personal device friendly or limited access. U.S. addiction expert Nicholas Kardaras asserts that screen addiction is harder to treat than heroin addiction, in part because screens, unlike heroin, are "so ubiquitous in our society that people inevitably have to interact with them on some level" (Ferranti 2016). Even in personal device friendly environments, there is still the difficulty making sure that employees don't fall into social media in the middle of the work day. Employers can promote incentives for limiting their device use or incorporate tools that limit access to certain sites. Encourage resources that help employees and employers manage their time on devices. HR and consultant resources can also extend help to those who want to improve their technology dependence (Kruse2013). There should be opportunities to improve oneself. Interacting with devices can trigger the brain to release dopamine and alters mood inducing addictive behavior (Smith 2019). Utilizing applications that trigger this release to help with organization and developing new skills, allow for employees to use their devices while employers highlight their expectations to encourage productivity.

As research has shown, large amounts of accessibility can produce addiction (Smith 2019). Tech companies have responded to technology dependence and these tools can be intertwined into the workplace. Google and Apple have built-in system software that shows how much time they are spending on their devices and how the time is spent (Simmons 2018). An employee enjoyed these features so much that he took to twitter to explain to others how to find this information (Twitter 2020). Employees now can monitor themselves and reflect on what areas they can improve on to work more efficiently. The Occupational Safety and Health Administration (OSHA) teamed up with the Dept. of Transportation to combat distracted driving on the roads and on the job (Totten 2014). This limits employees from relying on their autopilot modes to get jobs done. Autopiloting and unnecessary multitasking puts the employee at risk and the others working with them at risk of making more mistakes and vulnerable environments. Policies allow spaces to restrict distracted driving on the job to protect the company and those within it. It also puts responsibility into the employees' hands, so they control what's on their screen as well.

Conclusion

In order to obtain a balance in personal device use within the workplace, employers and employees must be willing to both be responsible for their use. The policies should reflect the compromising of power over the devices in different workspaces. No two workspaces may be the same, but it should be clear what is tolerated within each space. As expectations are implemented through the policies, they can change with time and experience. Remember that customization and clarity are also important to the success of a productive workplace.

References

Anandarajan, Murugan, et al. (2016). *The Internet and Workplace Transformation*. Routledge.

Apple Inc. (2019) “Supplier Responsibility.” Apple, 2019.

R&G (2015). “Bring Your Own Device (BYOD): What It Is and Why It Matters.” R & G Technologies.

Callaway, Joseph, and JoAnn Calloway (2016). *Client First: Knowledge Solutions for Southeast Asia: an Update of Southeast Asia Dept. Knowledge Management, 2012 to Mid- 2015.* John Wiley & Sons.

Dillow, Clay (2013, 21 Oct.). “Employees Really Want to Use Their Personal Devices at Work.” *Fortune.*

Dodgen-Magee, Doreen (2019, Mar. 18). “Tech Addiction Is Real. We Psychologists Need to Take It Seriously.” *Washington Post.*

Ferranti, Seth (2016, Aug. 6). “How Screen Addiction Is Damaging Kids’ Brains.” *Vice.*

Garrity, S., & Weir, G. R. (2010). Balancing the threat of personal technology in the workplace. *International Journal of Electronic Security and Digital Forensics, 3*(1), 73-81.

Kruse, Kevin (2013). “Why Successful People Never Bring Smartphones into Meetings.” *Forbes*.

Messmer, Ellen (2011, Nov. 2). “Corporate-Owned vs. Employee-Owned Mobile Devices.” *Network World.*

NACDL (2020). “Computer Fraud and Abuse Act (CFAA)” *NACDL*, National Association of Criminal Defense Lawyers.

Osuch Michale, and Turner, Steven (2017). “Addiction to Modern Technology: What the Science Says.” Elsevier Connect.

Pochepan, Jeff (2018, April 27). “Employees Working on Their Personal Devices? How You Can Protect Your Business Data.” *Inc.*

Simons, John (2018, May 16). "'I Lost It': The Boss Who Banned Phones, and What Came Next." *Wall Street Journal.*

Smith, Melinda, et al. (2019, Oct. 8). "Smartphone Addiction" HelpGuide International.

Movius (2019, March). "The Top 10 Mistakes Employees Make with Their Personal Devices for Work." *Movius.*

Twitter (2020). "Twitter. It's What's Happening." Twitter twitter.com.

Totten, J. A., & Hammock, M. C. (2014). Personal electronic devices in the workplace: Balancing interests in a BYOD.

U.S.C. Title 18 (2010). Crimes and Criminal Procedure Part I - Crimes Ch. 121: Stored Wire and Electronic Communications and Transactional Records Access, Stanford University 2010.

Washington, Melvin C., et al. (2014). "Perceptions of Civility for Mobile Phone Use in Formal and Informal Meetings." Association for Business Communication.