Employee Responsibilities and Rights Journal
https://doi.org/10.1007/s10672-024-09498-1

Bring Your Own Device (BYOD): Organizational Control and Justice Perspectives

Helen Lam[1] · Terry Beckman[1] · Mark Harcourt[2] · Sandra Shanmugam[3]

Accepted: 28 February 2024

Abstract
Bring your Own Device (BYOD) is an increasingly popular phenomenon at work, with several potential benefits (e.g., cost reduction, convenience and flexibility) and concerns (e.g., security risk, blurring of work-life boundary, and privacy infringement). Yet, systematic research incorporating theoretical perspectives on BYOD has been limited. This paper analyzes BYOD by integrating organizational control and justice frameworks. For control, approaches advanced by Hopwood, Ouchi and Edwards were adopted, covering simple control, administrative/bureaucratic control, technical/technological control, social control, and self control. The justice framework includes both distributive and procedural fairness. It is posited that justice/fairness mediates the effects of the control mechanisms. Practices under various controls that are seen as fair or unfair are discussed and recommendations provided.

Keywords Bring your own device (BYOD) · Organizational control · Distributive justice · Procedural justice · Organizational justice

✉ Mark Harcourt
mark.harcourt@waikato.ac.nz

Helen Lam
helenl@athabascau.ca

Terry Beckman
tbeckman@athabascau.ca

Sandra Shanmugam
shanharcourt@xtra.co.nz

[1] Faculty of Business, Athabasca University, 1 University Drive, Athabasca, AB T9S 3A3, Canada

[2] Waikato Management School, University of Waikato, Private Bag 3105, Hamilton, New Zealand

[3] Accounting and Tax Consultancy Services, Hamilton, New Zealand

Published online: 20 March 2024

Introduction

In the employment context, Bring Your Own Device (BYOD) programs refer to the company initiative of allowing employees to use personal electronic devices, such as smart phones or tablets, to access organizational applications and data to perform work. These programs have gained popularity in recent years, with the upward trend expected to continue. Many benefits associated with such programs include reduced costs, increased mobility and flexibility, more convenience for employees, enhanced employer attraction to job candidates, as well as improved employee satisfaction, efficiency, and productivity (e.g., Ansaldi, 2013; Fiorenza, 2013; Garba et al., 2015; Gewald, 2023; Gökçe & Dogerlioglu, 2019; Mordor Intelligence, 2024; Ntwari et al., 2022; Sharif et al., 2019; Totten & Hammock, 2014; Waterfill & Dilworth, 2014; Zahadat et al., 2015). At the same time, these programs can also give rise to a host of concerns, including increased information technology security risk and cost of system re-design and monitoring for the organization (e.g., Armando et al., 2015; Crossler et al., 2014; Gökçe & Dogerlioglu, 2019; Rathnayaka et al., 2023; Totten & Hammock, 2014), and the blurring of work-life boundary and infringement of privacy for employees (e.g., Degirmenci et al., 2023; Gökçe & Dogerlioglu, 2019; Leclercq-Vandelannoitte, 2015; Weeger et al., 2015).

According to a 2023 Pew Research Center survey, 90% of adults in the US (and 97% of those aged 18 to 29 and aged 30 to 49) have a smart phone, while 90% have internet access, including 80% with broadband internet at home (Gelles-Watnick, 2024). Another 2022 Pew Research Center survey across 18 advanced economies shows a similar trend for mobile phone use, with a median of 85% owning a smartphone, and 11% owning a mobile phone that is not a smartphone (Wike et al., 2023). We can generally expect most of these individuals to always carry their mobile devices with them, whether at or away from their workplace. For example, a 2012 survey shows that 80% of adult respondents with a smartphone would not leave home without the device while 71% would use it at their workplace (Ipsos OTX MediaCT & Google, 2012). A survey by Coalfire, an IT risk management firm, shows 84% of employees in the sample used the same smartphone for work and leisure (Coalfire, 2012). Zippia, a career resource company, reported that 75% of US employees used their personal cell phones for work even before the pandemic and the average BYOD employee works 2 h extra per day (Zippia, 2022). A 2022 Samsung study of over 1,000 employees found an estimate of 30.5% of respondents' personal phone usage was for work-related matters (Samsung for Business, 2022). Another recent study indicates that 70% of respondent employees preferred to use their personal devices for work tasks due to reasons as convenience, familiarity, and flexibility (Gewald, 2023). Indeed, a Microsoft survey involving over 9,000 employees in 32 countries shows 31% of the respondents would be even willing to pay for a new device themselves to enable them to work more efficiently (James, 2014, p 35). From the perspective of organizations, a 2018 Samsung survey of 500 US senior executives found that while only 17% of companies provided company phones to all employees, the remaining 83% were allowing employees to use personal phones for work (including 31% that did not provide company phones at all) (Samsung, 2018, p. 3). The survey report also mentions that "smartphones and similar tools are highly important or quite important to employee productivity (82%), agility and the speed of decision-making (82%), customer service and satisfaction (76%), and innovation and collaboration (75%)" (p. 4). The significance of smartphone use for work is such that "61% of organizations expect employees to

be available remotely, even if they don't provide a company phone" (p. 4). A 2021 BYOD Security Report involving 271 cybersecurity professionals reveals that 70% of respondent organizations had a BYOD program involving employees (82% when including contractors and other business partners) and 68% saw an increase in productivity because of BYOD (Cybersecurity Insiders, 2021, p. 2, 4, 5). The popularity of mobile device use, and the BYOD trend are evident.

Despite many publications available on this increasingly important topic, most are written in relation to cost efficiency and technology or security aspects (Leclercq-Vandelannoitte, 2015), with some touching on privacy issues. Moreover, many are practitioner oriented and published in trade journals. There has been little systematic academic research on BYOD's broader implications for the employment relationship, particularly work-life balance, and even less published involving a theoretical framework. This paper is intended to fill this gap by offering a systematic review of BYOD, through the application of the organizational control and organizational justice frameworks. The choice of these two frameworks is based on employers' need to control work to ensure better organizational performance, and employees' need to ensure that such controls are applied in a just manner. The analysis highlights the issues of concern for organizations and employees and provides corresponding recommendations for effective BYOD implementation.

Organizational Control

Edwards (2003) describes the workplace as one of "structured antagonism", where cooperation and conflict co-exist, in the sense that employer and employees must work together to create value, but the former needs to exploit the latter for profit. As such, control mechanisms ensure that employees act in a coordinated manner to achieve organizational goals and objectives, and despite employees having more autonomy in today's workplaces, "control is still a major responsibility of management" (Daft, 2001, p. 108). Below, we describe three sets of the most adopted control strategies and approaches, as discussed by Hopwood (1974), Ouchi (1979) and Edwards (1979).

Hopwood (1974) proposes three types of control: administrative control (exercised explicitly by management usually through rules and procedures), social control (exerted informally through organizational culture, group norms and peer influence), and self control (exerted informally and voluntarily by the individual employee). These three forms of control are not mutually exclusive, and indeed, "for administrative control mechanisms to be effective, they must become social and ideally self-control mechanisms" (Byers, Anagnostopoulos, & Brookie-Holmes, 2015, p. 137).

Ouchi's (1979) control strategies are categorized into the following three types: bureaucratic, market, and clan. Bureaucratic control is similar to administrative control mentioned above, as it relies on rules and procedures to control employee behaviour. Such control assumes acceptance of the authority making the rules and the control subsystems that could include budget, statistical reports, reward systems and operating procedures (Daft, 2001). Market control is efficiency-based and relies on price competition to determine output and productivity levels but may not be applicable universally as not all organizations are in competitive markets nor do explicit prices always exist for evaluating output and productivity efficiently (Daft, 2001). Clan control influences behaviour via shared values and beliefs,

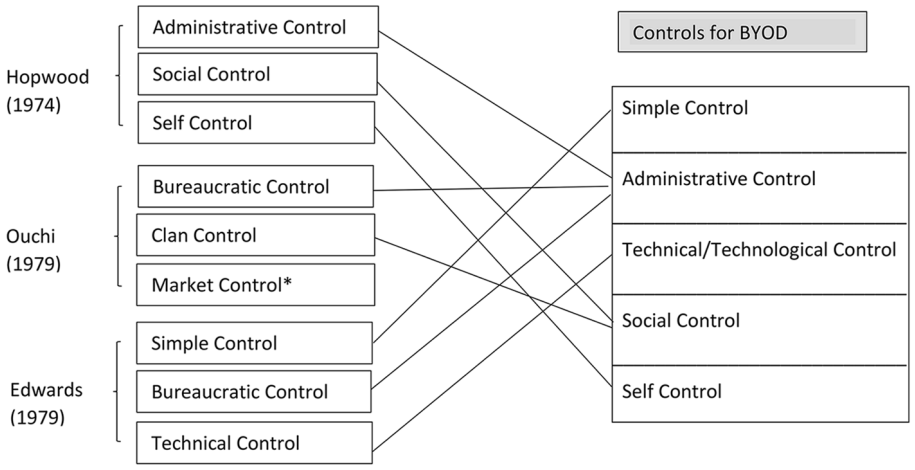
often embedded in a firm's culture, and is comparable to the social control under the Hopwood model.

Another set of control approaches suggested by Edwards (1979) includes simple control, technical control, and bureaucratic control. Simple control is most applicable to small organizations, where control is directly exerted by managers who basically "rule" the firm, combining "both incentives and sanctions in an idiosyncratic and unsystematic mix" (p. 19). Technical control is exercised through the control of operations, as when machines and/or an assembly line sets the pace of the labour process. Bureaucratic control is "embedded in the social and organizational structure of the firm and is built into job categories, work rules, promotion procedures, discipline, wage scales, definition of responsibilities, and the like" (p. 131).

For the BYOD analysis, we adopt Hopwood's (1974) framework, involving administrative control, social control, and self control, supplemented by two additional types of control in the Edwards (1979) model, namely simple control and technical/technological control. Bureaucratic control in the Edwards and Ouchi models is discussed under administrative control, while Ouchi's clan control is covered by the focus on social control. Ouchi's market control is of limited application in the BYOD context. Where pricing and compensation are involved, they are discussed with reference to justice theories. Figure 1 illustrates the match of the control types identified by Hopwood, Ouchi and Edwards with those selected for analysis in this paper.

Organizational Justice

Organizational justice is the employees' perception of fairness regarding treatment received from the organization, and has been empirically linked to job satisfaction, employee performance and organizational commitment (Greenberg, 1988; Haar & Spell, 2009; Tyler & Caine, 1981). Organizational justice is usually an implicit but important aspect of an



*Market control is not matched to the selected controls for BYOD and is not considered applicable.

Fig. 1 Match of the reviewed control mechanisms to the selected ones for BYOD analysis

employee's psychological contract with the employer (Rousseau, 1995), because fairness is not just a virtue. It also reflects how much control employees have over decisions that affect them, and signals how much they are valued by the organization (Tyler, 1987; Lind & Tyler, 1988; Folger, 1998). There are two main dimensions to organizational justice: distributive justice and procedural justice. Distributive justice deals with fairness in the distribution of outcomes (e.g., rewards or punishment) while procedural justice involves fairness in the process of determining outcomes (Cropanzano, et al., 2007; Konovsky, 2000). Since employees tends to think that a flawed process leads to flawed outcomes, the absence of procedural justice typically also means an absence of distributive justice as well. More on each of these two justice dimensions is presented below.

Distributive Justice

Distributive justice theories are predicated on using allocation rules to ensure a fair distribution of outcomes. For example, Deutsch (1973, 1985) proposes three social justice allocation rules, equity, equality and needs, that can be readily applied to an organizational setting. Equity refers to allocating outcomes according to the contributions made and is best suited to helping organizations achieve efficiency goals. Equality ensures everyone gets the same outcome regardless of input and is best for fostering harmonious workplace relationships. The needs principle bases allocations on individual need and is most appropriate for demonstrating organizational concern for individual well-being. Similarly, Lerner (1982) proposes four allocation rules: competition, equity, parity, and Marxian. The parity rule is like the equality rule described above, whereas the Marxian rule is comparable to the need-based rule. With the equity rule, outcomes (rewards) are allocated in accordance with inputs/ contributions (e.g., skills, effort), but with the competition rule in accordance with performance or achievements (Vogelaar & Vermunt, 1991).

Procedural Justice

Procedural justice concerns the "structural characteristics of a system" and how a decision is made, including considerations such as the nature of the decision authority, information collection process, safeguards to ensure proper procedures are followed, information communication channels, input opportunities, and appeal options (Folger et al., 1992). According to Leventhal et al. (1980), there are six aspects that affect the perception of procedural fairness, namely, consistency in application of rules, bias suppression, accuracy of information gathered, decision 'correctability' (when erroneous), representation of interests involved, and ethicality. Folgers and Bies (1989) offer similar criteria for fairness in management decisions, but also include timely feedback, honest communication, and justifications provided with decisions. Together, these conceptions provide a good foundation to understand the various procedural justice dimensions in organizational management decisions.

Organizational Analysis of BYOD

BYOD is an organizational initiative that can help with efficient and effective functioning by, for example, allowing flexible access to necessary organizational information, enabling

employees to work anytime, anywhere, facilitating social networking among employees and other stakeholders, and empowering employees. Under such circumstances, BYOD is likely to be embraced by employees as well as employers. However, if not properly designed and implemented, it could have negative effects. If control is too tight, it may give rise to employee legal challenges (e.g., infringement of privacy or labour relations rights), an organizational environment of distrust, and, worse still, a perception of employee exploitation and subsequent employee demoralization. If control is too loose, the employer can suffer losses due to inconsistent practices, confidential information leakage, and resource waste. Hence, how the control mechanisms work and how much attention is paid to justice can have a significant impact on the success of BYOD.

Simple Control

With simple control, the personal leadership style of the manager is likely to greatly affect the success of any BYOD initiative. BYOD requires the voluntary use of employees' own devices for work matters, and so their commitment is critical. A participative and supportive leadership style is more likely to encourage employees to volunteer not just their device, but also some of their personal time to stay on top of work matters. Haywood's (2010) framework for engaging employees with their head, heart and gut can also be suitably applied to this BYOD context.

To engage employees with the head, it is important for the leader to set and communicate clear goals for BYOD, and ensure employees know that the initiative is not solely to increase output, but rather is mutually beneficial to both employer and employees. To engage with the heart, the leader can set a good example by refraining from emailing, instant messaging, or calling in the after hours, other than in emergency situations. Where non-urgent emails are sent to employees' devices, the proposed action time-line should not pertain to after working hours. Setting the right expectations can avoid unnecessary stress and conflict for employees. To engage with the gut, all communications by leaders should be honest. As BYOD is supposed to be voluntary, it should truly be so without undue pressure for employees to sign on to the program. There should be appropriate compensation for the use of the program to ensure fairness and alignment with the objectives of the program as well as other organizational initiatives. This is further addressed in a later section involving justice.

Administrative Control

Administrative or bureaucratic control involves "the use of rules, policies, hierarchy of authority, written documentation, standardization, and other bureaucratic mechanisms to standardize behavior and assess performance" and is commonly used in large organizations where simple control using supervision is not sufficient (Daft, 2001, p. 197). In establishing administrative control for BYOD, the major concerns are related to access, ownership, and authority issues. First, there should be a policy on the use of company infrastructure. Who should have access to the infrastructure through their own device? Perhaps not all employees need to have such access, as need depends on the level of the position, the nature of the work and the urgency involved. Also, what online activities are employees allowed in using the company infrastructure (e.g., web sites, social network links) to receive information or communicate with other employees or clients?

The second policy area concerns the protocols for governing employees' work-related use of social media. When employees use their own device, do they have unlimited freedom to say anything about the employer on social media? Case law has clearly indicated employees can be held responsible for insubordination and violating their duty of loyalty if they deride the company and its managers. See, for example, the Lougheed Ltd. (2010) [BCLRB B190/2010] Canadian case in which the employee was disciplined for inappropriate after-hours comments about the organization, and the *Escape Hari Design* (2010) [204 IR 292] and *Good Guys* (2011) [FWA 5311] Australian cases that reinforce employer rights in disciplining employees for off duty activities (Lam, 2016). Hence, the fact that employees are using their own devices and communicating after work hours does not protect them from discipline in many jurisdictions. A social media policy should also indicate who has the authority to represent the organization in communicating online with internal and external stakeholders.

The third type of policy involves access to and use of company information. Code of conduct policies on confidentiality usually already exist in many organizations, but a more explicit linkage with BYOD might need to be made, as again, employees may be less careful when using their own device in the after hours. Moreover, when employees have access to organizational information, are they allowed to download and keep this on their device, and if so, what administrative safeguards are required? Is it sufficient to just have employees sign off on reading and understanding the policy?

The fourth relevant type of policy is the organization's right to access the employee device. Who owns the information on the device? To what extent can the employer intrude into the employees' device to ensure that company information and infrastructure are properly accessed, stored, and used? In extreme situations, can the employer remove information on employees' devices and in what circumstances? Can all information be removed or only company-related information? Is a blanket policy giving the employer unilateral rights to do so at anytime enforceable? These issues are discussed in later sections covering technological control and organizational justice.

The fifth type of policy relates to compensation and after hours work expectations. If employees work on their own devices, should the company contribute to any ongoing cost, such as for internet or phone services? Should any device cost be covered at all, in some appropriate proportion commensurate with work use, even though the device is selected by the employee and used for personal matters as well? If employees are expected to do BYOD work in the after hours, it should be made clear in the employment contract or collective agreement. The payment for such work is also a contentious issue. More on this is discussed under the justice section.

In general, for company rules to be enforceable, the KVP arbitration award criteria (*Lumber & Sawmill Workers' Union, Local 2537, and KVP Co. Ltd.* (1965) 16 L.A.C. 73) have been well recognized and they include: clarity, reasonableness, consistency in application, proper communication to employees, and compliance with applicable laws and collective agreement. They must be well understood by employees, and as such, training that helps to deliver the meaning and expectations of the rules and procedures can be quite critical.

Technical/Technological Control

Technical/technological control involves using machinery or technology to control how and when work is performed such as using "automation to structure and monitor work" to ensure compliance (Morris et al., 2006; Wicks, 2002, p. 672). In the digital era, recent studies have focused more on how information and communication technologies, including mobile digital technologies, assert managerial control (Bisht et al., 2023). With BYOD, the concerns are mostly about security, privacy, and data ownership. Much has been written on how the organization can secure its network (e.g., Canadian Centre for Cyber Security, 2022; Garba et al., 2015; Smith & Forman, 2013; Totten & Hammock, 2014; Zahadat et al., 2015) but still allow employees to do their work effectively. Protective measures include using passwords, authentication, encryption, automatic locking after a period of inactivity, technical restrictions to limit access according to need, determining device types allowed and the software required or disallowed, virtualization (i.e., data storage and transmission are done through organizational infrastructure and not on personal device and network), vulnerability checks at the organizational system end, and remote wiping of device data, etc. Though many of these practices are necessary and reasonable, some may pose significant concerns for employees. Consider a situation: if an employee must surrender his or her device for vulnerability or other checks, is the privacy of personal information compromised? Who should control data on the device? Case law on this issue is still emerging and far from conclusive. For example, in the US litigation discovery process, organizations are supposed to preserve and produce relevant information in their possession and control (Foley, 2014). Two commonly cited cases giving diametrically opposite decisions on this are *In Re Pradaxa* [No. 3:12-md-02385-DRH-SCW, 2013 WL 6,486,921 (S.D. Ill. Dec. 9, 2013)] and *Cotton* v. *Costco Wholesale* [No. 12-2731-JW, 2013 WL 3,819,974 (D. Kan. July 24, 2013)], with the former decision confirming organizational control over BYOD information and the latter not (Richter, 2015). A clear BYOD policy spelling out its purpose, operational requirements and restrictions, and compliance expectations in law could go a long way to addressing privacy and security concerns (Foley, 2014), rendering BYOD more appealing to employees.

Another legal issue with monitoring an employees' device and information is the potential contravention of Section 7 of the National Labor Relations Act in the US. This section specifically protects employees' engagement in "concerted activities for the purpose of collective bargaining or other mutual aid or protection …." That is, employees have the right to discuss among themselves using whatever means, including their own electronic device, matters concerning their terms and conditions of employment, without any employer interference or monitoring (Clark Hill PLC, 2018; Rajendra, 2014). If an organization wants to exert any surveillance or control over such communication, it risks non-compliance with the Act.

Also, if an organization is allowed to wipe all the data off an employee's phone, as in the case of the phone being stolen, is it again taking over control of something (the employee's data) that does not belong to the organization? There could certainly be legal proceedings from employees invoking privacy and property rights, and, in some countries, wiping an employee's phone is already outright illegal (Ansaldi, 2013). Sometimes, having employees simply sign off on a BYOD policy is insufficient to fend off legal challenges, because the policy is not clear or reasonable or involves coercion, undue influence, or misrepresentation.

One possible technical control solution involves having two compartments on each device, one for work and one for personal use, where the employer only has access, monitoring, and other rights vis a vis the former. Where employees are not comfortable with using their own device for work purposes, provision of company devices should still be available when needed. This is especially important for reducing unnecessary perceptions of coercion.

Rather than just focusing on control, it might be more beneficial for an organization to prioritize the technical training and support needed for successful BYOD use (Leclercq-Vandelannoitte, 2015). For example, training and support can equip employees to deal with security risks, as with installing malware and virus detection and removal software, use of encryption and suitable passwords, filtering out spam emails and checking for fraudulent web links, safe downloading of applications, identification of various risks and vulnerability, etc. Where there is a loss of the device or vulnerability suspected by the user, technical assistance can be made available to stop access of the device to the organizational network. As part of technical support, organizations can also provide the necessary software to protect employee devices.

Social Control

Social control is a more informal and subtle form of control, exercised largely through organizational culture and group norms. Organizational culture reflects and affects work expectations and behaviours and can shape the psychological contract between employees and their employer. Organizations that promote a highly competitive culture can pressure employees to outperform each other. If most employees use their own device at all times to keep up with job demands, it is difficult for other employees not to follow suit in such an "always on" culture (Derks et al., 2015). Culture is modeled by leaders and managers as well as other colleagues' actions. If organizational members, especially those in authority, email subordinates' own device to request actions immediately, that clearly sets work expectations. These potentially coercive practices might better the organization's bottom line at the expense of employees' workload, stress, and role conflict.

On the other hand, organizations can foster a culture of respecting employees, being concerned about fairness, and emphasizing work-life balance (e.g., Arrowsmith & Parker, 2013; Mone et al., 2011; Raines, 2011; Sinha & Trivedi, 2014). Such organizations trust their employees to do what they feel is appropriate. With BYOD, the voluntary nature of a BYOD program can be stressed and additional job autonomy provided, with sufficient discretion to decide how and when the work is done. This logically brings the analysis to the next control aspect – self control.

Self Control

Self control refers to internal control initiated from within the individual as opposed to control exercised from outside. For employees to be committed to certain organizational initiatives, they need to internalize rules and procedures so that actions taken are not just in line with organizational goals, but also the employees' own goals. This type of control is particularly relevant to BYOD, because it involves personal devices and time usually in a voluntary manner.

When employees use their own devices to do work, the boundary between professional and private lives is blurred. Inevitably, some work is done outside of work hours and is supposedly discretionary. If employees are explicitly required to work outside of normal working hours, the hours worked would need to be paid even though monitoring and measuring such working time can be difficult. However, if employees are empowered, to some extent, to decide when and where to work, they are more likely to support and enjoy BYOD. They might even be prepared to work after hours without compensation if they feel the increased freedom is sufficiently worthwhile. They might see the empowerment as an intrinsic reward sufficient to compensate for their extra efforts.

Not all employees are willing or able to exercise appropriate levels of self control. With BYOD, some employees may over-exercise their discretion, as the ease of access to work through personal devices can make one "addicted" to emails and other online work communications. Workaholism is not a new phenomenon, but it may have increased as BYOD use blurs the boundary between work and private life. According to a recent survey of over 1,000 employees, work-life balance was found to be poorer for BYOD employees as compared with employees provided with company phones (Beyond Identity, 2021). Some employees might feel uncomfortable about leaving work incomplete in the after-hours. Often, the coercion to work or contribute more (or sacrifice more) to the organization has a cultural origin in organizational norms and/ or structural origin in a willingness to accept unfair treatment when the alternative is unemployment (Karlsson, 2015). An organization that allows this to happen is potentially exploiting the employees' passion for work or fear of not conforming, but there can be adverse consequences in the long run, including low morale and productivity, as well as high turnover and workplace aggression (Nikiforakis et al., 2014). According to a report on a European Values Survey, over 50% of respondents felt they were exploited at work, at least at times (Nikiforakis et al., 2014), and BYOD could exacerabate such perceptions of unfairness and exploitation, if not implemented properly.

As mentioned before, the various types of control are not mutually exclusive. Many organizations employ several control mechanisms simultaneously. Administrative and technical control are often complementary. For example, if there are administrative restrictions on BYOD access (e.g., authorizations from superiors), technical measures must be in place to enable these restrictions to be checked and enforced. Likewise, the effectiveness of some administrative controls requires acceptance and support, an alignment of cultural values, by the employees. Even simple control, with direct command exercised by a supervisor, requires subordinates to accept and support the legitimacy of the authority figure. Whatever the type of control, it is ultimately most effective if mirrored in self-control, with the employees' values aligned to the goals of the control. For this to occur, employees should understand and support the overall rationale for some kind of control, perhaps best engendered by having them involved in designing and implementing the control strategies at first instance. Many of these issues relate to organizational justice, discussed in the next section.

Organizational Justice

The control strategies discussed above are not necessarily positive or negative in themselves. Their effect on the success of BYOD depends on their design and implementation. Since employee support is essential to the success of such an initiative, we posit that employees' perceptions of justice associated with the control mechanisms play a critical role in deter-

mining BYOD outcomes. In other words, justice perceptions are expected to mediate the BYOD control-outcome relationship.

Organizations may adopt different allocation rules to ensure distributive justice, but once an allocation principle is selected and the rule established, it should be applied consistently and not arbitrarily. For BYOD, various rules concerning the use of the device, and constraints on access and disclosure of information, including the code of conduct, should be similarly applied to all employees. If employees in senior positions are subject to fewer constraints, this should be clearly based on position characteristics.

BYOD can transfer some of an employer's equipment and infrastructure costs to employees. Employees involved in such programs own the device and pay for the equipment themselves. They also normally incur the ongoing costs of, for example, cellular plans and home wi-fi access fees. To ensure a sense of distributive justice, it is appropriate in such circumstances for employers to reimburse employees for at least some of these expenses. Indeed, the California Court of Appeal, in the *Cochran v. Schwan's Home Service* case, determined that an employer must reimburse an employee for using his or her cellphone on work-related calls by paying a reasonable percentage of the employee's cellphone bill, irrespective of whether the cellphone plan had limited or unlimited minutes (Kaneshige, 2014). In this regard, the equity and equality allocation rules are most likely to be applicable. The equality rule would require compensation for the device purchase and operating costs, covered in the same way for all employees. For example, a firm could pay a fixed portion or percentage of such costs across the board. Employees are expected to spend the same amount of time (at least on average) being on-call or to deal with work matters, and as such, a fair compensation for such can be determined and applied to all employees. The equity rule would require compensation commensurate with the extent a device is used for work, especially after hours. For example, if for certain positions work usage accounts for about 10% of the normal after-hours usage, then the compensation for the cost related to the device for those position holders should be set accordingly. For work done after normal hours, appropriate compensation could be in the form of wages for the actual hours worked (at least in compliance with legal requirements on overtime pay) or banked hours for future use. Indeed, in many jurisdictions, for most categories of workers protected by employment statutes, overtime work must be paid or allowed to be banked for future time off (Totten & Hammock, 2014). Not having a good system to keep track of these hours can give rise to legal complaints and penalties and not compensating employees appropriately is unjust.

Some organizations may not have explicit rules for BYOD especially with respect to compensation. Beyond Identity (2021) found in a recent survey of over 1,000 employees that 61.8% of respondents did not receive a stipend from their employer for their mobile device use (Beyond Identity, 2021). Without explicit compensation, BYOD can still work well if employer and employee have implicit and reciprocal understandings for BYOD in and out of work. Thus, the employee might use his/ her device for work after working hours but use it for personal purposes at least some of the time at work. Such reciprocal arrangements help engender the justice of digital mutualism, which is about "the perceived balance of mutual benefit between an employee and the organization subsequent to the enactment of BYOD policy" (Putri & Hovav, 2014, p. 4). In a way, this is closely linked to employee empowerment and self control (granting them the autonomy to determine their own work time and resource allocation) and can sometimes work more effectively than having every rule spelt out in detail, trying to constrain and direct employee behaviour. Ultimately, how-

ever, whether rules and procedures are explicitly articulated or implicitly understood, they must be perceived as fair by employees.

Another compensation issue concerns the division of gains between employer and employee, if BYOD use produces a major increase in efficiency or profit. To what extent should such gains be shared with employees, if at all? For example, organizations could consider some forms of gain-sharing that rewards for savings generated. Alternatively, the organization can go with a much broader type of incentive, such as profit-sharing, to spur employee motivation. This would recognize the benefits achieved by BYOD, but not just limited to it.

Another crucial justice dimension, in addition to distributive justice, is procedural justice. In this regard, the KVP arbitration case factors with respect to company rules mentioned earlier are very applicable: reasonableness, clarity in communication, and consistency in application. To ensure employees are aware of the organization's policies and support the BYOD, ongoing communication is a key element (Ansaldi, 2013) as even the best policy means nothing if it is not known and comprehended. Training can be a useful avenue for such communication and can also help in the understanding of the detailed administrative and technological aspects. It is not enough to have just one-way communication with employees. A good BYOD policy regarding control, support, and compensation should involve consultation with various stakeholders—HR, legal and IT personnel, and more importantly, the employees in general. Employee input can also help with devising reasonable rules, as reasonableness must be established from the employees' perspective. As well, it contributes positively to the Leventhal el al. (1980) procedural justice elements of employee representation, bias suppression and accuracy of information gathered. In all, employee voice leads to better understanding and buy-in, which are critical for any BYOD program to take off and become successful. In the event there are any disputes arising out of the BYOD policy implementation, employees should be entitled to due process, where their concerns are heard, and any erroneous management decisions corrected. Indeed, feedback on issues of concern should be an ongoing two-way process and not left to the time when something goes wrong.

The Control and Justice Matrix

The various control approaches analyzed above are intertwined and their success largely relates to how they are designed and implemented. We posit that for the BYOD control mechanisms to work, employees should see them as fair in terms of both distributive and procedural justice. Figure 2 presents the proposed relationship among the control, justice and BYOD outcome factors involved.

To provide a better appreciation of this framework integrating both the control and justice concepts, we offer in Table 1 just and unjust organizational practice examples, both distributively and procedurally, for each control mechanism. The justice dimensions are understandably on a continuum, and we simply choose to describe the polar ends for illustrative purposes.

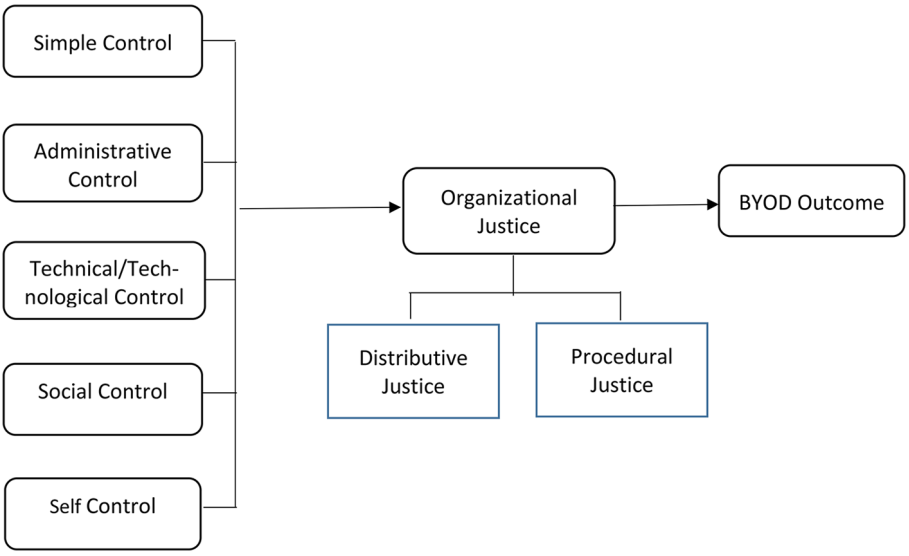


Fig. 2 Organizational control, justice and BYOD Outcome (Note: Simple control, administrative control, technical/technological control and social control can all influence each other. These four controls can also influence self control.)

Recommendations

BYOD is an increasingly popular phenomenon that can be embraced by both organizations and employees, but it also has the potential to lead to excessive and unwelcome organizational control over employees' use of their own time and resources/properties. How can organizations assure employees that they can refuse to share their devices without fear of being considered uncooperative or suffering employer reprisal? When personal devices are volunteered for work use, how can the organization ensure this is done appropriately and effectively to serve the interests of employer and employee?

Throughout the above analysis, issues have been identified and solutions to these issues suggested. Here, we recapitulate the various recommendations for organizations embarking on or revisiting the BYOD initiative. As control and justice factors are closely related and not mutually exclusive, rather than categorize the recommendations by factors discussed, we consider it more appropriate and less repetitive to group them into broader human resource management-related areas, namely, organizational culture, leadership, rewards and compensation, training and support, monitoring and control, and employee voice and communication. Such recommendations are provided in Table 2.

Conclusion

BYOD can have significant positive and negative organizational consequences, depending on how it is implemented and viewed. If not designed and implemented properly, BYOD is unlikely to be supported by employees and risks generating perceptions of being under-

Table 1 Organizational control and justice matrix

	Distributive justice		Procedural justice	
	Just	Unjust	Just	Unjust
Simple control	The leader sets a role model on what is mutually beneficial to both organization and employee in device use especially during after hours and refrains from placing unwarranted demands on employees' time or device resources.	The leader demands that the employee works any time after hours using own device without compensation or with compensation determined in an arbitrary manner.	The leader adopts a participative and supportive style that involves employee input to allow for better understanding employee needs and concerns when determining BYOD use and constraints.	The leader adopts an authoritative style and decides on the BYOD use and constraints based purely on his/her own needs and perspective.
Administrative control	Company policies reflect the voluntariness of employees using their device for work matters, respect individual privacy and rights (e.g., in social media usage) after work hours, and provide proper compensation (in money or in kind) for use of device and after hours work time. Gains from the BYOD program are shared with employees.	Company requires employees to use their own device for work matter, treat information on employee's device as if it were the company's (ignores employee property and privacy rights), and do not provide for proper compensation for the device use or employee time after work nor are BYOD gains shared.	Company rules on access, ownership, and authority issues in relation to BYOD—device usage, social media usage, confidential company information, and BYOD compensation—are reasonably established with employee input, clearly communicated, and consistently applied.	Company rules on access, ownership, and authority issues in relation to BYOD are unilaterally established and imposed/ enforced, and may or may not be clearly communicated.
Technical/ technological control	Company focuses on providing tools and support to ensure employees have the hardware and software and technical guidance needed to keep device safe and organizational infrastructure/information secure, e.g., by helping to compartmentalize the device for work and private use.	Company exercises excessive restrictions and monitoring relating to hardware and software requirements, as well as data access, storage, transmission and deletion that infringe on privacy and hinder employees' use of device even for personal purpose.	Company offers education and training to ensure employees understand the BYOD security risks and provide them with the knowledge and skills to make informed decisions on BYOD use. Company keeps good track of employee overtime via BYOD for proper compensation.	Company provides little information or training on the technical aspects and implications of BYOD to employees and yet expects them to comply without questions or errors. Company controls/ monitors employees' private information on the device without obtaining consent or with coerced consent.

Table 1 (continued)

	Distributive justice		Procedural justice	
	Just	Unjust	Just	Unjust
Social control	Company adopts a culture of work-life balance and respects employees' social life and communications with others. BYOD is intended to allow employees better social connection with others and provides intangible rewards for them.	Company uses social pressure to "force" employee to volunteer their time and resources through BYOD and denies rights to legitimate or truthful discussions among employees or between employees and outsiders on social media or other communication channels.	Company fosters a participative culture for BYOD development; offers guidelines, with rationale, on appropriate use of social media where company matters are concerned and does not monitor or interfere with employee social group formation or discussions.	Company forms preferred social groups for the sole purpose of advancing their own interests. Company gains access to social group discussions through inappropriate means, such as requiring employees to render their account access information or through misrepresentation of identity.
Self control	Company empowers employees to make their own decisions on BYOD matters and only offers guidance and support as needed, leading to intrinsic satisfaction.	Company capitalizes on employees with inclination towards workaholism, and uses that passion for work to achieve gains for the organization only.	Company acts fairly under various types of other controls to ensure employees understand their rights and obligations so they can identify with the company's needs and interests and balance it with their own.	Company misleads employees through various representations into having a false sense of self-control when they are only encouraged to do what the company wants.

valued, disrespected, and having one's rights infringed, with negative repercussions for the employee's personal life and relationship with the employer. Especially as digital devices continue to proliferate, and personal devices are used increasingly for work, a good BYOD policy and implementation plan is becoming more critical to the smooth running of organizations. Thus, establishing a clearer and more thorough understanding of this area sooner rather than later remains crucial. Yet, comprehensive research on BYOD beyond the technical aspect is just emerging and there remains a lot to learn about this initiative. Future research could further develop the theoretical model and empirically test various organizational variables involved in BYOD.

Table 2 Recommendations for successful BYOD in organizations

Human resource areas	Recommended organizational practices
Organizational culture	• Respects and empowers employees as to how work is to be done • Emphasizes fairness and work-life balance • Makes BYOD participation totally voluntary • Sets no unreasonable expectation on after-work responses on own device
Leadership	• Sets and communicates clear BYOD goals including benefits for employees such as flexibility, information access, networking, etc. • Establishes appropriate expectations on BYOD use in alignment with the organization's cultural values as listed above • Acts as good role models or examples (e.g., refraining from sending unnecessary after-work emails)
Rewards & compensation	• Pays for an appropriate portion of the employees' device and internet/cellular plan cost • Allows for reciprocal arrangements (i.e., allowing employees to reasonably use company devices for personal use during work hours) • Pays for overtime work (or allows for banked vacation hours) involved using BYOD • Considers some forms of profit- or gain-sharing to share the surplus generated by BYOD
Training & support	• Offers training to ensure BYOD and related policies are well understood • Provides the tools and knowledge needed to handle BYOD issues such as protection of device and information • Ensures technical support is available where needed
Monitoring & control	• Ensures administrative controls on access, ownership and authority issues are well addressed in BYOD policy, with reasonableness and justice in mind • Provides a company device to critical employees who do not want to use their own device • Provides technical controls that protects the security of both employee and organizational data • Offers virtualization that ensures data is stored in organizational server and not on local device • Compartmentalizes the data (e.g., using dual SIMs and different storage areas) on the device where possible so that access or wiping of information could be done only for the organizational data • Disallows organizational surveillance of or access to personal communication
Employee voice & communication	• Actively seeks input from all stakeholders—not just HR, IT or legal counsel, but more importantly the employees (end users) in the development and implementation of the BYOD policy • Clearly communicates all aspects of the BYOD and related policies and processes, including the types of support provided

Funding Open Access funding enabled and organized by CAUL and its Member Institutions

References

Ansaldi, H. (2013). Addressing the challenges of the 'Bring your own device' opportunity. *CPA Journal*, *83*(11), 63–65.

Armando, A., Costa, G., Merlo, A., & Verderame, L. (2015). Formal modeling and automatic enforcement of bring your own device policies. *International Journal of Information Security*, *14*(2), 123–140.

Arrowsmith, J., & Parker, J. (2013). The meaning of 'employee engagement' for the values and roles of the HRM function. *International Journal of Human Resource Management*, *24*(14), 2692–2712.

Beyond Identity (2021). Bring your own device? Exploring the types and security of devices employees used for work. https://www.beyondidentity.com/blog/byod-exploring-evolution-work-device-practices-survey.

Bisht, N. S., Trusson, C., Siwale, J., & Ravishankar, M. N. (2023). Enhanced job satisfaction under tighter technological control: The paradoxical outcomes of digitalisation. *New Technology Work and Employment*, *38*, 162–184.

Byers, T., Anagnostopoulos, C., & Brooke-Holmes, G. (2015). Understanding control in nonprofit organisations: Moving governance research forward? *Corporate Governance*, *15*(1), 134–145.

Canadian Centre for Cyber Security (2022). End user device security for Bring-Your-Own-Device (BYOD) deployment models - ITSM.70.003. Government of Canada. https://www.cyber.gc.ca/en/guidance/end-user-device-security-bring-your-own-device-byod-deployment-models-itsm70003.

Clark Hill PLC. (2018). Crafting Bring Your Own Device (BYOD) policies to protect your company data and ensure compliance with the law. JD Supra, LLC.https://www.jdsupra.com/legalnews/crafting-bring-your-own-device-byod-76244/.

Coalfire. (2012). BYOD Survey: 47 percent of users lack a password on smartphones accessing company files. https://www.coalfire.com/insights/news-and-events/press-releases/byod-survey

Cropanzano, R., Bowen, D. E., & Gilliland, S. W. (2007). The management of organizational justice. *Academy of Management Perspectives, 21*(4), 34–49.

Crossler, R. E., Trinkle, B. S., Long, J. H., & Loraas, T. M. (2014). Understanding compliance with bring your own device policies utilizing protection motivation theory: Bridging the intention-behavior gap. *Journal of Information Systems*, *28*(1), 209–226.

Cybersecurity Insiders (2021). 2021 BYOD Security Report. https://pages.bitglass.com/rs/418-ZAL-815/images/CDFY21Q2BYOD2021.pdf.

Daft, R. L. (2001). *Essentials of organization theory & design (2e)*. South-Western College Publishing.

Degirmenci, K., Breitner, M. H., Nolte, F., & Passlick, J. (2023). Legal and privacy concerns of BYOD adoption. *Journal of Computer Information Systems*, 1–12. https://doi.org/10.1080/08874417.2023.2259346.

Derks, D., van Duin, D., Tims, M., & Bakker, A. (2015). Smartphone use and work-home interference: The moderating role of social norms and employee work engagement. *Journal of Occupational and Organizational Psychology*, *88*(1), 155–177.

Deutsch, M. (1973). *The resolution of conflict: Constructive and destructive processes*. Yale University Press.

Deutsch, M. (1985). *Distributive justice*. Yale University Press.

Edwards, R. (1979). *Contested terrain: The Transformation of the Workplace in the Twentieth Century*. Basic Books.

Edwards, P. (2003). The employment relationship and the field of industrial relations. In P. Edwards (Ed.), *Industrial Relations: Theory and practice in Britain* (2nd ed., pp. 1–36). Blackwell.

Fiorenza, P. (2013). Mobile technology forces study of bring your own device. *The Public Manager*, *42*(1), 12–14.

Foley, M. F. (2014). Employer E-discovery duties expand in a BYOD environment re: Employee devices. *National Law Review*http://www.natlawreview.com/article/employer-e-discovery-duties-expand-byod-environment-re-employee-devices.

Folger, R. (1998). Fairness as a moral virtue. In M. Schminke (Ed.), *Managerial ethics: Moral management of people and processes* (pp. 13–34). Lawrence Erlbaum.

Folger, R., & Bies, R. J. (1989). Managerial responsibilities and procedural justice. *Employee Responsibilities and Rights Journal*, *2*(2), 79–90.

Folger, R., Konovsky, M. A., & Cropanzano, R. (1992). A due process metaphor for performance appraisal. *Research in Organizational Behavior*, *14*, 129–177.

Garba, A. B., Armarego, J., Murray, D., & Kenworthy, W. (2015). Review of the information security and privacy challenges in bring your own device (BYOD) environments. *Journal of Information Privacy & Security*, *11*(1), 38–54.

Gelles-Watnick, R. (2024, January 31). Americans' use of mobile technology, home broadband | Pew Research Center. Pew Research Center: Internet and Technology. https://www.pewresearch.org/internet/2024/01/31/americans-use-of-mobile-technology-and-home-broadband/.

Gewald, A. (2023). Embracing BYOD: The impact of consumerization on employer appeal. *International Journal of Computer Science & Information System*, *8*(7), 5–8.
Gökçe, K. G., & Dogerlioglu, O. (2019). Bring your own device policies: Perspectives of both employees and organizations. *Knowledge Management & E-Learning*, *11*(2), 233–246.
Greenberg, J. (1988). Equity and workplace status: A field experiment. *Journal of Applied Psychology*, *73*, 606–613.
Haar, J. M., & Spell, C. S. (2009). How does distributive justice affect work attitudes? The moderating effects of autonomy. *The International Journal of Human Resource Management*, *20*(8), 1827–1842.
Hayward, S. (2010). Engaging employees through whole leadership. *Strategic HR Review*, *9*(3), 11–17.
Hopwood, A. (1974). *Accounting and human behaviour*. Haymarket.
Ipsos OTXMCT & Google (2012). Our mobile planet: United States: Understanding the mobile consumer. http://services.google.com/fh/files/blogs/our_mobile_planet_us_en.pdf.
James, H. (2014). How the interaction of social and big data influences employee engagement. *Workforce Solutions Review*, *5*(2), 35–36.
Kaneshige, T. (2014, August 18). Court ruling could bring down BYOD. *CIO*https://www.cio.com/article/250317/byod-court-ruling-could-bring-down-byod.html.
Karlsson, J. C. (2015). Work, passion, exploitation. *Nordic Journal of Working Life Studies*, *6*(2), 3–16.
Konovsky, M. A. (2000). Understanding procedural justice and its impact on business organizations. *Journal of Management*, *26*(3), 489–511.
Lam, H. (2016). Social media dilemmas in the employment context. *Employee Relations*, (3), 420.
Leclercq-Vandelannoitte, A. (2015). Managing BYOD: How do organizations incorporate user-driven it innovations? *Information Technology and People*, *28*(1), 2–33.
Lerner, M. J. (1982). The justice motive in human relations and the economic model of man: A radical analysis of facts and fictions. In V. Derlega, & J. Grezlak (Eds.), *Cooperation and helping behavior: Theories and research* (pp. 121–145). Academic.
Leventhal, G. S., Karuza, J. J., & Fry, W. R. (1980). Beyond fairness: A theory of allocation preferences. In G. Mikula (Ed.), *Justice and social interaction: Experimental and theoretical contributions from psychological research* (pp. 167–218). Springer-.
Lind, E. A., & Tyler, T. R. (1988). *The social psychology of procedural justice*. Plenum.
Mone, E., Eisinger, C., Guggenheim, K., Price, B., & Stine, C. (2011). Performance Management at the Wheel: Driving Employee Engagement in Organizations. *Journal of Business and Psychology*, *26*(2), 205–212.
Mordor Intelligence (2024). BYOD market size & share analysis - Growth trends & forecasts (2024–2029). https://www.mordorintelligence.com/industry-reports/byod-market.
Morris, M. H., Allen, J., Schindehutte, M., & Avila, R. (2006). Balanced Management Control Systems as a mechanism for achieving corporate entrepreneurship. *Journal of Managerial Issues*, *18*(4), 468–493.
Nikiforakis, N., Oechssler, J., & Shah, A. (2014). Hierarchy, coercion, and exploitation: An experimental analysis. *Journal of Economic Behavior and Organization*, *97*, 155–168.
Ntwari, R., Habinka, A. E., & Kaggwa, F. (2022). BYOD systematic literature review: A layered approach. *European Journal of Technology*, *6*(1), 69–85.
Ouchi, W. G. (1979). A conceptual framework for the design of organizational control mechanisms. *Management Science*, *25*(9), 833–848.
Putri, F., & Hovav, A. (2014). Employees' compliance with BYOD security policy: Insights from reactance, organizational justice, and protection motivation theory. Proceedings of the European Conference on Information Systems (ECIS) 2014, Tel Aviv, Israel, June 9–11, 2014. http://aisel.aisnet.org/ecis2014/proceedings/track16/2.
Raines, M. S. (2011). Engaging employees. *Professional Safety*, *56*(4), 36–43.
Rajendra, R. (2014). Employee-owned devices, social media, and the NLRA. *ABA Journal of Labor & Employment Law*, *30*(1), 47–71.
Rathnayaka, R. P. P. S., Swarnamali, I. S., Piyasekara, W. D. C., Karunathilaka, N. A., Abewardena, K. Y., & Yapa, K. (2023). Enhancing security in a corporate BYOD environment. *International Research Journal of Innovations in Engineering and Technology*, *7*(11), 329–334.
Richter, D. (2015). Bring your own device' programs: Employer control over employee devices in the mobile e-discovery age. *Tennessee Law Review*, *82*(2), 443–459.
Rousseau, D. M. (1995). *Psychological contracts in organizations: Understanding written and unwritten agreements*. Sage.
Samsung for Business (2022). How much should you reimburse BYOD employees for mobile expenses? https://insights.samsung.com/2022/05/16/how-much-should-you-compensate-byod-employees-for-mobile-expenses-3/.

Samsung (2018). Maximizing Mobile Value: Is BYOD holding you back? Oxford Economics. https://image-us.samsung.com/SamsungUS/samsungbusiness/short-form/maximizing-mobile-value/WHP-HHP-MAXIMIZE-MOBILE-VALUE-JUN18.pdf.

Sharif, M. H. U., Datta, R., Sankarasetty, S. N., Garikapati, H., Valavala, M., & Maraboyina, S. (2019). Bring your own device (BYOD) program. *International Journal of Engineering Applied Sciences and Technology*, *4*(4), 2455–2143.

Sinha, K., & Trivedi, S. (2014). Employee engagement with special reference to Herzberg Two Factor and LMX theories: A study of IT sector. *SIES Journal of Management*, *10*(1), 22–35.

Smith, K. J., & Forman, S. (2013). Bring your own device-challenges and solutions for the mobile workplace. *Employment Relations Today (Wiley)*, *40*(4), 67–73.

Totten, J. A., & Hammock, M. C. (2014). Personal electronic devices in the workplace: Balancing interests in a BYOD world. *ABA Journal of Labor & Employment Law*, *30*(1), 27–45.

Tyler, T. R. (1987). Conditions leading to value-expressive effects in judgments of procedural justice: A test of four models. *Journal of Personality and Social Psychology*, *52*(2), 333–344.

Tyler, T. R., & Caine, A. (1981). The influence of outcomes and procedures on satisfaction with formal leaders. *Journal of Personality and Social Psychology*, *41*(4), 642–655.

Vogelaar, A. L., & Vermunt, R. (1991). Allocation standards: Equity, equality, and asymmetry. In L. M. J, & R. Vermunt (Eds.), *Social justice in human relations, Volume 1: Societal and psychological origins of justice* (pp. 101–122). New York.

Waterfill, M. R., & Dilworth, C. A. (2014). BYOD: Where the employee and the enterprise intersect. *Employee Relations Law Journal*, *40*(2), 26–36.

Weeger, A., Wang, X., & Gewald, H. (2015). IT consumerization: BYOD-program acceptance and its impact on employer attractiveness. *The Journal of Computer Information Systems*, *56*(1), 1–10.

Wicks, D. (2002). Successfully increasing technological control through minimizing workplace resistance: Understanding the willingness to telework. *Management Decision*, *40*(7), 672–681.

Wike, R., Silver, L., Fetterolf, J., Huang, C., Austin, S., Clancy, L., & Gubbala, S. (2022). Internet, smartphone and social media use. Pew Research Center. https://www.pewresearch.org/global/2022/12/06/internet-smartphone-and-social-media-use-in-advanced-economies-2022/.

Zahadat, N., Blessner, P., Blackburn, T., & Olson, B. A. (2015). BYOD security engineering: A framework and its analysis. *Computers & Security*, *55*, 81–99.

Zippia (2022, October 17). 26 surprising BYOD statistics [2023]: BYOD trends in the workplace, https://www.zippia.com/advice/byod-statistics/.