The Technological Panopticon - Electronic Monitoring and Surveillance within the Workplace: Employee Turbulence through Perceptions of Privacy Infringement

Charlie Hinde[1] and Jacques Ophoff[1,2]
[1] University of Cape Town, Cape Town, South Africa
[2] Abertay University, Dundee, United Kingdom
HNDCHA003@myuct.ac.za, j.ophoff@abertay.ac.uk

Abstract

As organizations work towards securing their digital assets and intellectual property from external threats, so the latest information security reports indicate that the biggest threat remains from inside. The insider threat has become one of the biggest exploitable vulnerability's corporates face as a level of trust is placed in their staff, or authenticated users, on their network, to ensure corporate objectives and goals are achieved. While monitoring and surveillance in the workplace are considered symbiotic and go hand in hand as part of the employee relationship, the advancement in technological capability for electronic monitoring and surveillance (EMS) has escalated to such a degree that all aspects of an employee's workplace routine can be recorded. This research-in-progress paper hopes to utilize the communication privacy management (CPM) theory to understand if increasing levels of EMS in the workplace affect employees' perception of privacy infringement.

1 Introduction

In December 2008, there were 1.5 billion Internet users; ten years later this has grown to 4.3 billion users - more than half of the global population (Miniwatts Marketing Group, 2019). As organisations introduce digital innovation to engage with this emerging economy the latest World Economic Forum report on global risks, rates cyber-attacks and data fraud and theft as two of the top five risks faced by companies (World Economic Forum, 2019). In 2017 for example, Maersk, the world's largest shipping conglomerate, was infected by the NotPetya ransomware virus which resulted in more than US$300 million in damages. As the virus cascaded around the globe, it totalled more than US$10 billion in damages – this from a single cyber-attack (Greenberg, 2018).

The top five information security breaches of 2018 resulted in 2,190 billion customer data records being exposed (Leskin, 2018) through either malicious outsiders, malware, or system weakness. However, the most damaging security threats are considered to come from trusted insiders (Cybersecurity Insiders, 2018), either malicious or negligent - the insider threat. The Computer Emergency Response Teams (CERT) at the Software Engineering Institute of Carnegie Mellon University has recently updated the definition of the insider threat to "an individual who has, or had, authorized access to an organization's assets to use their access, either maliciously or unintentionally, to act in a way that could negatively affect the organization" (Elifoglu & Abel, 2018, p. 62). Trusted users are therefore in an ideal position to exploit their privilege to compromise the information assurance (confidentiality, integrity or availability) of an organisations network system, data or premises (Ernst & Young, 2016). While organisations secure their digital perimeter with technical controls such as firewalls, insiders are already authenticated and have access to the network and knowledge of where critical assets reside; and because they are already within the organisations perimeter, traditional detection systems used against external threats (hackers), is bypassed.

Until recently the insider threat did not mean much to organisations, and even after the WikiLeaks (BBC, 2017) and Edward Snowden cases (Wikipedia, n.d.), most organisations continued to mitigate threats from external sources. As trusted users, the belief that insiders usually do what is in the best interest of the organisation remains a reality. Whether intentional or not, the examples of the WikiLeaks and NSA breaches show how devastating the insider threat can be (Elifoglu & Abel, 2018), and multiple threat reports (Accenture & Ponemon Institute, 2019; CA Technologies, 2018; Kroll, 2018) outline the impact insider threats will pose in the foreseeable future. Unfortunately, the persistence of the insider threat will continue based on the required trust organisations place in their staff, or authenticated users, on their network.

Securing a corporate network, of any size, requires many steps, and both researchers and cybersecurity professionals recommend approaching information security in a multi-layered approach. Schou and Trimmer (2004) introduced the term "defense in depth" in relation to Information Technology (I.T.) security. This encompasses the additional security layers that need to be implemented to provide cover for the failure, or breach, of the initial security layer. Defense in depth controls are usually divided into three areas: physical, technical, and administrative (Stewart, Chapple, & Gibson, n.d.). Combining administrative controls such as user awareness training with traditional technical controls such as firewalls and encryption have shown positive results in raising awareness to external threats (Eminağaoğlu, Uçar, & Eren, 2009; Hagen, Albrechtsen, & Hovden, 2008; Shaw, Chen, Harris, & Huang, 2009). The defence in depth concept becomes an important security consideration when the end-user is the first line of defence (Maconachy, Schou, Welch, & Ragsdale, 2001; Schou & Trimmer, 2004), and is considered by many to be the weakest link in information security (Crossler et al., 2013; Willison & Warkentin, 2013).

Monitoring and surveillance in the workplace are considered symbiotic and go hand in hand as part of the employee relationship (Ball, 2010). Job titles which include the word "supervisor", one who inspects and directs the work of others[1], have been used for centuries, and have been included in theories of management dating back to Henri Foyal's 1916 "Administration industrielle et générale" (Fayol, 2016). The implication is that monitoring or surveillance is part of the working environment and that "employees expect to have their performance reviewed, objectives set, and information gathered on their working activities" (Ball, 2010, p. 89).

While previous supervisory intrusions may have simply been a manager looking over an employee's shoulder (Townsend & Bennett, 2003), technological advancements in electronic monitoring and surveillance (EMS) allows for a more intrusive view of employee behaviour. Email and internet surveillance are well established channels for monitoring employee behaviour (Ball, 2010; Friedman & Reed, 2007; Oliver, 2002) and should form an integral part of a corporate defense in depth security strategy. However, there is limited research into broader EMS strategies that utilise new technologies such as Big Data and advanced analytics. While the nature of present-day EMS poses greater challenges to the employee relationship as the level of monitoring and surveillance can be considered intensive, continuous and unrelenting (Adler, 2001), the importance of surveillance within a layered defence is proving a critical component (Accenture & Ponemon Institute, 2019; CA Technologies, 2018; Kroll, 2018).

The advanced nature of next generation EMS technologies allows organisations to build employee data-sets characterising behaviour patterns and assigning risk attributes not previously considered. While studies of organisational infringement have shown a negative impact on employee-employer trust (Eastlick, Lotz, & Warrington, 2006; Kim & Kim, 2011; Taddei & Contena, 2013; Wu, Huang, Yen, & Popova, 2012), the level of data collection and profiling of an employee's behaviour patterns through advanced EMS technologies could drive employee fears of an infringement of their privacy thus also negatively impacting the employee-employer trust relationship.

While monitoring and surveillance has been a tacit aspect of the employee relationship for decades, the shift in legislative requirements to secure data and personal information within the scope of doing business[2], coupled with

[1] Dictionary.com: mid-15century., from Medieval Latin supervisor, agent noun from supervidere "oversee, inspect"). https://www.dictionary.com/browse/supervisor

[2] South Africa: Protection of Personal Information Act (POPIA)
Europe: General Data Protection Regulation (GDPR)
Australia: Australia Privacy Principles (APP)

the ongoing advancement and diminished costs in information communication technology (ICT), provides organisations with the opportunity to extend their EMS capability. The extended technology-creep in providing monitoring and surveillance capabilities leads to the primary research question:

How do increasing levels of EMS in the workplace affect employees' perception of privacy infringement?

While organisations may be implementing EMS solutions as part of a defence in depth strategy, the legal requirements placed on organisations to take due care in how they process and store sensitive information is becoming an operational requirement. Extending the primary research question of increased levels of EMS within the workplace is the notion of the acceptance of the increased levels of monitoring. This leads to a secondary research question:

How do regulatory requirements influence the acceptance of EMS in the workplace?

Having contextualised the research questions this research-in-progress paper continues with the theoretical framework and proposed methodology for the study.

2 Theoretical Framework

2.1 Introduction

As EMS has expanded and become more advanced in its ability to monitor, so have the corresponding theories, frameworks and models developed to understand it. Procedural justice theory (e.g., Alge, 2001), information boundary theory (e.g., Stanton & Stam, 2003), the structural–perceptual model (e.g., D'Urso, 2006), and agency theory (e.g., Sewell & Barker, 2006), have all been used. As this study focuses on how the increasing levels of EMS in the workplace effect employees' perception of privacy infringement, and therefore the primary tension between an employer's interest in implementing or extending EMS, and an employee's interest in privacy, it will utilise the communication privacy management (CPM) theory (Petronio, 2002).

At its core CPM theory "presumes that people believe they own their private information" (Petronio, 2004, p. 202), and control of the this information is critical as disclosure makes them vulnerable. Therefore, ownership and control are primary elements in defining how individuals handle their private information. Based on this need to control private information, a dialectical tension naturally exists between maintaining privacy and disclosing private information (Allen et al., 2007). Based on Altman's Social Penetration Theory (Altman, 1977), Petronio extended the metaphor of individuals setting privacy boundaries around their private information – the dialectical concept that privacy is based on the opening and closing of boundaries to others. EMS by its nature has the ability to cross these privacy boundaries and therefore create turbulence (Petronio, 2004). This boundary turbulence, where an employee loses control of their private information and potentially impacts their working relationship, forms the practical element of CPM in evaluating EMS within the workplace.

CPM has been used in many studies since Petronio created the theory in 1991[3], including social media (see Waters & Ackerman, 2011), e-health (see Jin, 2012), familial privacy (see Romo & Vangelisti, 2014) and children's privacy orientation (see Bridge & Schrodt, 2013). While this section outlines the broader CPM theory, figure 1 summarises the elements this study intends to follow – how boundary turbulence potentially impacts an employee's sense of organisational privacy which is tied to organisational justice (Alge, 2001; Ball, 2002), organisational trust (S. Lee & Kleiner, 2003; Rosenberg, 1999; Snyder, 2010; Tabak & Smith, 2005) and organisational commitment (Brown, 1996; Fairweather, 1999; Snyder & Cistulli, 2011).

2.1.1 CPM Foundations

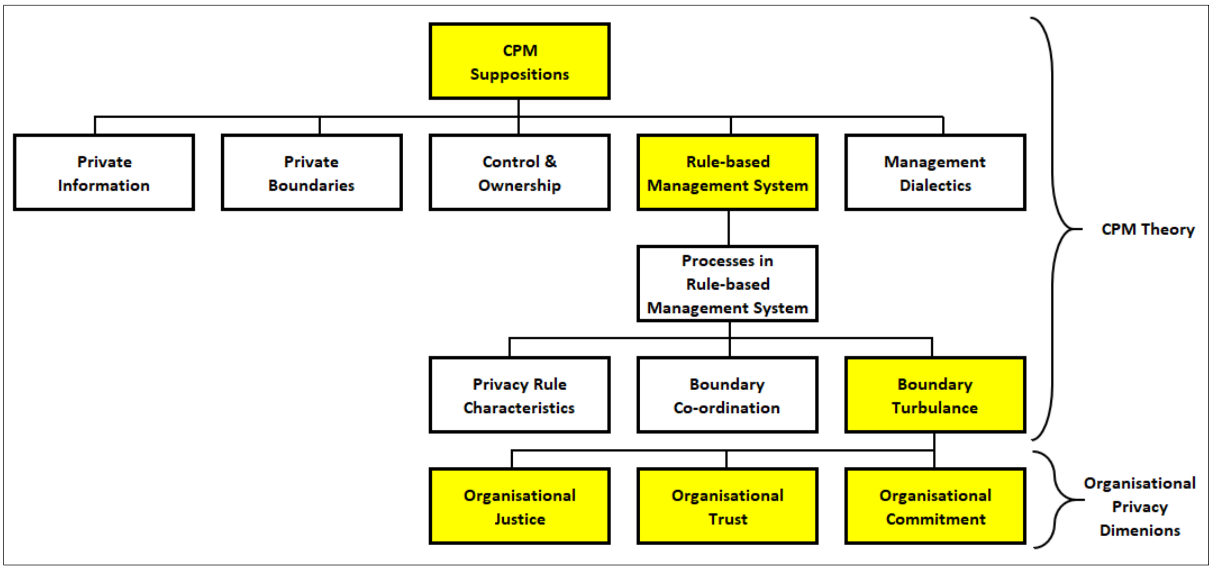

Figure 1: CPM and Organisational Privacy Dimensions

Petronio (2002) positions five basic suppositions that define CPM theory:

1. **Private Information:** Individuals believe they own their private information. "Irrespective of legal rights, individuals often assume they have the right to control their private information, including when at work" (Allen et al., 2007, p. 176).
2. **Private Boundaries:** Individuals assume they have the right to control their private information. This sense of control establishes a boundary where individuals can decide what and to whom private information is disclosed based on personal privacy rules.
3. **Control and Ownership:** Private information that is shared or exposed to another party becomes co-owned and forms a collective boundary. Co-ownership of a boundary can lead individuals to feel a sense of vulnerability as the establishment of shared boundary rules offers greater permeability depending on the co-owner's management of the boundary rules (Petronio, 2002).
4. **Rule-based Management System:** Individuals depend on privacy rules to control their information flow. When information is shared, co-owners not only own the information but also the boundaries to that information

[3] Google Scholar indicates over 9000 citations for Petronio's journal articles and books.

(Petronio, Sargent, Andea, Reganis, & Cichocki, 2004). Privacy rules control who receives private or personal information; when, how much, and where this information disclosure occurs; and how this information might be concealed (Petronio, 2002). This rule management system relies on three processes to regulate the revealing and concealing of private information: privacy rule foundations, boundary coordination, and boundary turbulence.

While all three processes regulating the rule-based management system provide insight to an individual's perception of privacy, *boundary turbulence* is of interest to this study in relation to EMS. As the management of information between co-owners is not fully understood, and private information is either intentionally or mistakenly shared, conflict can arise between co-owners if there are differing expectations of these information boundaries.

Management Dialectics: Dialectical tensions arise as individuals make "judgments about the degrees of privacy and publicness they wish to experience in any given interaction" (Petronio, 2002, p. 15). Individuals apply a cost-benefit analysis to the sharing of private information and the feeling of vulnerability associated to this (Caughlin & Afifi, 2004). Consideration is given to how the information will be owned, used and spread – the establishment of boundaries, and the permeability of them (Petronio & Reierson, 2009).

2.1.2 Boundary Turbulence in the Workplace

The workplace offers the perfect environment for boundary turbulence. Employers typically take the position of information ownership irrespective of the personal nature of the information – if it's on the corporate network, or within the corporate environment (email, phone calls etc.) the organisation retains ownership; often in opposition to an employee's view (S. Lee & Kleiner, 2003; Townsend & Bennett, 2003). In addition, it is generally accepted by employees that organisations constantly monitor the quality and quantity of their work based on an employment contract.

"For boundary maintenance to work, everyone must agree on the rules. When one person has a different idea about the way rules are formed and used, the management system may be disrupted and lead to turbulence" (Petronio, 2002, p. 49). The uneven power distribution of boundary ownership between employers and employees (Petronio, 2002) through the implementation of EMS provides the mechanism leading to the contestation of boundary ownership thereby resulting in turbulence (Mattson & Brann, 2002). This is exacerbated due to EMS (particularly e-mail) being "covert and unobtrusive" (Snyder & Cornetto, 2009, p. 479) and employees may form a privacy boundary under a false sense of privacy. Petronio's (2002, 2004) *boundary coordination* (permeability, linkage and ownership) talks to areas where this boundary turbulence originates: where boundaries are fuzzy, ambiguous, or differences in the risk-perception of revealing or concealing private information exist (permeability); linkages are created that contravene ownership expectations, or one set of boundary rules are applied to another boundary (linkage); or boundaries are ignored, misunderstood, intentionally violated, or the privacy rules are misused (ownership). Alge's (2001) study on privacy invasion through workplace surveillance indicated that an individual's personal identity, their estimation of self, as well as their public persona can be threatened when privacy is impinged. In addition, the quality of an individual’s work life can suffer due to misunderstandings and knowledge gaps created by surveillance (Stanton & Stam, 2003).

With the extent of potential monitoring undertaken within the workplace, it could be concluded that employee boundaries do not exist. However, a study undertaken by Allen et al. (2007) around email EMS within the workplace concluded that ‘‘interviewees reported no employee input into the development of privacy rules and limited expectations for even having private information, although they did articulate some privacy boundaries’’ (2007, p. 192). While employers have the overall power in establishing privacy rules, there is still an understanding by employees of boundaries that employers should not breach. Upholding this notion is the recent 2017 judgement from the European Court of Human Rights in the case of Barbulescu v. Romania where the Court held that an employer’s instructions could not reduce “an employee’s private social life in the workplace to zero” (Raimondi et al., 2017)[4].

While inter-personal boundary management is a fundamental component of CPM, the dialectical tension that exists in managing personal information within the workplace, especially the violation of these boundaries with the implementation of advanced EMS, is of particular interest in this study as it provides an intersection between an employee’s feelings of privacy (and a desire to protect their personal information), and an organisation’s right to monitor their digital environment through EMS.

2.1.3 Workplace EMS, Privacy and Employee Attitudes

Privacy is an important element of both the formal and psychological employment contract for both employees and employers (Ball, Daniel, & Stride, 2012). Workplace EMS and privacy are related, yet distinct, constructs. While monitoring and surveillance convey the automated collection of information for decision making by management (Botan, 1996), privacy describes the ability a person has in controlling access to that information (Altman, 1977; Botan, 1996; Snyder, 2010). When individuals feel a loss of control of their personal information through EMS (boundary turbulence), they feel their privacy has been invaded (Alge, 2001). This loss of privacy, and the perception of control they have over their personal information due to EMS, influences their work-related attitudes (see Snyder, 2010). Employee attitudes based on EMS extend to organisational justice, trust in upper management and their commitment to the organisation.

1. **Organisational Justice:** Organisational justice concerns itself with people’s perceptions of fairness in organisations (Cropanzano & Greenberg, 1997). Fairness extends beyond the size of the organisation, whether it’s pay structures within corporate environments, or leave scheduling in a small office environment – the question of fairness is seemingly universal.
2. **Organisational Trust:** Within the workplace it has been found that organisational trust develops from interpersonal relationships between managers and employees based on a “mutual degree of reliability,

[4] In this case, an employer had accused an employee of using an internet instant messaging service for private conversations on a work computer. The Court held that an employer’s instructions could not reduce private social life in the workplace to zero. The right to respect private life and for the privacy of correspondence continue to exist, even if these may be restricted as far as necessary. Article 8 of the European Convention on Human Rights provides for the respect for one's "private and family life, his home and his correspondence".

confidence, and security" (Nyhan, 2000, p. 89). Interpersonal trust is characterised as a "positive force from which cooperation is derived" (Scott, 1980, p. 158) and is considered to have three major, but overlapping constructs: fairness, confidence, and risk taking (Nyhan, 2000). The employee-manager trust relationship is further established through a mutual feeling that workplace engagements are considered fair and ethical (Nyhan, 2000). While developing and maintaining trust is a mutual, reciprocal process (Chory, Vela, & Avtgis, 2016), studies indicate that email EMS is interpreted by employees as an organisation not trusting them, and in turn this is reciprocated by employees not trusting managers (S. Lee & Kleiner, 2003; Rosenberg, 1999; Snyder, 2010; Tabak & Smith, 2005). Perceptions of a loss of control over their privacy can lead employees to mistrust both management and the organisation they work for (Tabak & Smith, 2005).

3. **Organisational Commitment:** Organisational commitment can be defined as an individual's strong sense of involvement and identification with a particular organisation (Mowday, 1998; Steers, 1977). While the understanding of employee-organisation commitment has developed over time: O'Reilly and Chatman's (1986) work on compliance, identification and internalisation; and Meyer and Allen's (1991) three elements of commitment covering affective, continuance and normative forms; it is Porter's narrower, emotional definition of commitment as a "bond characterised by acceptance of an organization's goals" (Mowday, 1998, pp. 389–390) that provides input to this thesis.

   Porter et al. (1974) identified three components forming employee-organisation commitment: 1) acceptance of the organisation's goals and values, 2) a willingness to work toward achieving the organisation's goals, and 3) a desire to remain a part of the organisation. Psychological contract violations occur when an "employee's perception that the organization has failed to fulfil one or more of its obligations" (Turnley & Feldman, 2000, p. 26), of which an infringement on an employee's privacy through email EMS has been shown to be one (Brown, 1996; Fairweather, 1999). A reduction in employee-organisation commitment due to email EMS (Snyder & Cistulli, 2011) follows the same pattern as the employee-trust relationship.

By its nature EMS is invasive, be it CCTV, email or voice recording, personal details or behaviour patterns are exposed to employers. While employees may be aware of or have become more accepting of EMS within their working environment, a right to privacy and personal boundaries can be maintained (however tenuous this may be). This privacy/boundary position can be in stark contrast to employers who feel they have the right to protect their assets – either physical or intellectual.

The communication privacy management (CPM) theory developed by Petronio (2002) provides an opportunity to understand the notion of privacy, the establishment of personal information boundaries, and the resulting turbulence created when these boundaries are violated. The dialectical nature of maintaining control over personal information and sharing the information relates directly to EMS within the workplace. Previous studies involving workplace e-mail monitoring and privacy (Alge, 2001; Allen et al., 2007; S. Lee & Kleiner, 2003; Snyder, 2010) indicate that CPM is the "ideal framework to illustrate employees' ability to maintain healthy relationships with top management through the control of the open–closed dialectic" (Snyder & Cistulli, 2011, p. 127).

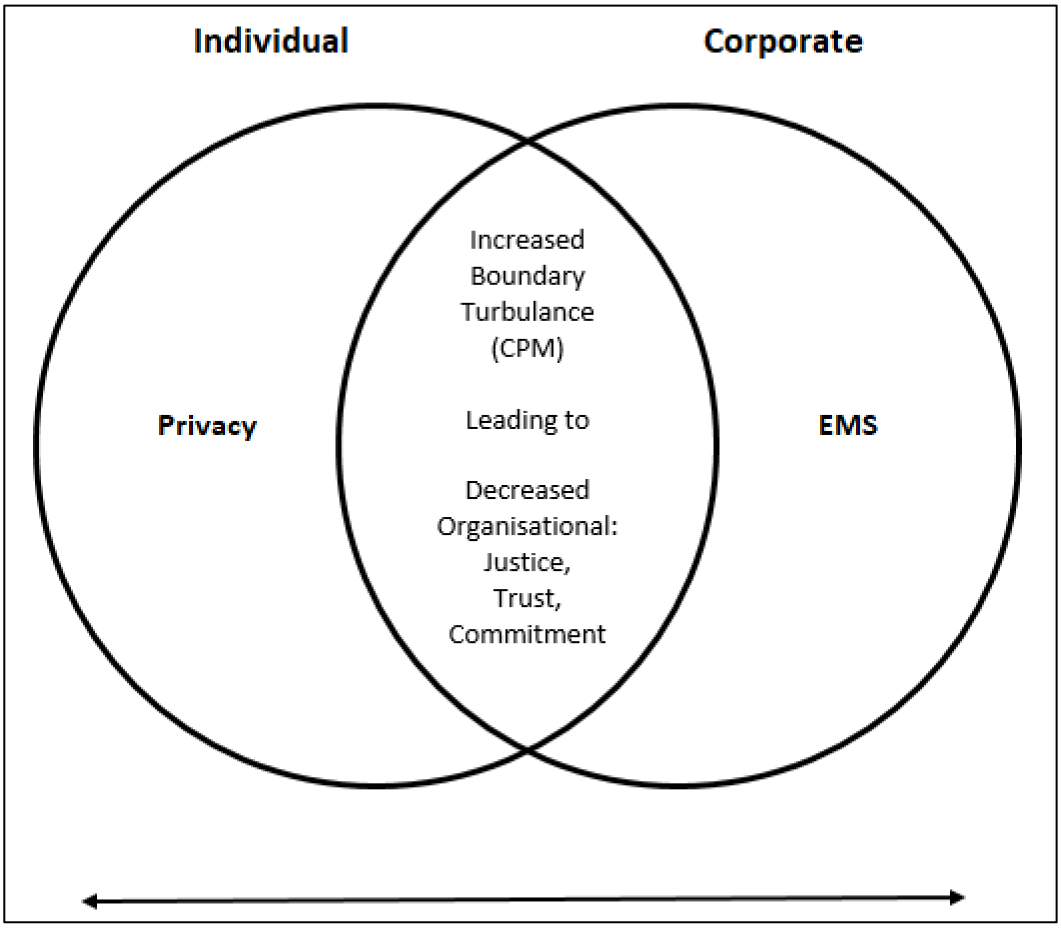

Figure 2: Privacy vs EMS

Figure 2 illustrates the possible results when an individual experiences boundary turbulence in the workplace due to increased EMS. Would the area of boundary turbulence and organisational privacy dimensions be reduced if regulatory requirements influence the acceptance of EMS technologies within the workplace?

3 Proposed Methodology

Section two positioned Petronio's communication privacy management theory as the best-suited theoretical approach to this study. Previous studies involving workplace e-mail monitoring and privacy recommend utilising case study as a methodological strategy in further exploring the impact of EMS on privacy (Holland et al., 2015).

Limitations from previous surveillance studies include self-reporting and sample sizes (Chang et al., 2015; Holland et al., 2015) and a recommendation to better understand the influence that legal regulations could have on workplace privacy expectations (Chang et al., 2015). This research will adopt an explanatory approach using the breadth of methods offered by case study research using the interpretive paradigm with the aim to provide a theoretical contribution by discovering the antecedents driving the outcomes of previous surveillance self-reporting research. Case study research lends itself to multiple data collection methods. While interviews are considered the corner-stone of case study research (Darke, Shanks, & Broadbent, 1998), interpretation of only interview material by the researcher may limit the validity of the research (Yin, 2017). This research will supplement participant interviews with questionnaires, documents and memoranda, unstructured interviews, and focus groups to provide for triangulation and the opportunity to present an objective view of events in relation to subjective interpretations of participants (Benbasat et al., 1987).

As interpretive methodologies attempt to understand a phenomenon from an individual's perspective by investigating interactions among individuals (Creswell, 2009) and the world around them – asking the 'why' and 'how' questions of human experience (Given, 2008) therefore provide both meaning and context of human behaviour. The components informing the interpretive paradigm align with both CPM and the research question:

- Personal information is different from person to person based on their individual engagements with the world around them.
- Privacy rules are developed by individuals based on their social environments, gender and cultural norms.
- CPM is contextualised as interpersonal or intrapersonal and is considered socio-cultural in tradition.
- The research will attempt to identify similarities in meaning of the privacy infringement phenomena within a defined social environment.

The research site selected for this study is based in South Africa and is actively engaging with the newly enacted Protection of Personal Information Act (POPIA) and its security requirements by implementing a next-generation EMS solution. This offers a unique opportunity to evaluate the effect POPIA has on workplace privacy expectations, and the reality of employee's perceptions of their privacy being infringed upon.

As per Chang et al.'s (2015) recommendation, reviewing the influence of POPIA on workplace privacy expectations offers a new area of research within South Africa. While the South African Information Regulator has proactively engaged with business about POPIA's requirements to promote the protection of personal information processed by public and private bodies, early indications show limited awareness of POPIA in the public domain (Netshakhuma, 2019).

4 Conclusion

While this research poses a primary and secondary research question, they are closely aligned. The President of South Africa proclaimed the commencement of POPIA on 1 July 2020, with all institutions having 12 months from this date to comply with the Act. The South African Information Regulator (Regulator) an independent body established in terms of section 39 of POPIA is empowered to monitor and enforce compliance by public and private bodies with the provisions therein. The Regulator has engaged with businesses over the past 2 years through various workshops and conferences outlining POPIA and its respective sections, requirements and controls.

The aim of this research is two-fold. At a theoretical level it aims to extend the understanding of privacy in the workplace, especially the potential acceptance (or not) of perceived privacy infringements through legislation-induced electronic monitoring and surveillance (Chang, Liu, & Lin, 2015). Practically, as this research will undertake a case study methodology, it will provide tangible insights and output from a "live" EMS implementation which could be beneficial to organisations undertaking similar implementations (Holland, Cooper, & Hecker, 2015)

5 Bibliography

Accenture, & Ponemon Institute. (2019). The Cost of Cybercrime - 9th Annual cost of Cybercrime Study. Retrieved from Accenture and Ponemon Institute website: https://www.accenture.com/t20190305T185301Z__w__/us-en/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf

Adler, G. (2001). Employee reactions to electronic performance monitoring: a consequence of organizational culture. Journal of High Technology Management Research, 12, 323–342.

Alge, B. J. (2001). Effects of computer surveillance on perceptions of privacy and procedural justice. Journal of Applied Psychology, (86), 797–804.

Allen, M., Coopman, S., Hart, J., & Walker, K. (2007). Workplace surveillance and managing privacy boundaries. Management Communication Quarterly, 21, 172–200.

Altman, I. (1977). Privacy Regulation: Culturally Universal or Culturally Specific? Journal of Social Issues, 33(3), 66–84. Retrieved from https://web-a-ebscohost-com.ezproxy.uct.ac.za/ehost/pdfviewer/pdfviewer?vid=1&sid=3df9b75b-3b6d-4839-9c62-f4990ba03a5f%40sessionmgr4006

Ball, K. (2002). Categorizing the workers: Electronic surveillance and social ordering in the call centre. In D. Lyon (Ed.), Surveillance as Social Sorting (pp. 201–225). London: Routledge.

Ball, K. (2010). Workplace surveillance: an overview. Labor History, 51(1), 87–106. https://doi.org/10.1080/00236561003654776

Ball, K., Daniel, E., & Stride, C. (2012). Dimensions of employee privacy: an empirical study. Information Technology & People, 25(4).

BBC. (2017). Chelsea Manning: Wikileaks source and her turbulent life - BBC News. Retrieved April 22, 2019, from bbc.com website: https://www.bbc.com/news/world-us-canada-11874276

Benbasat, I., Goldstein, D. K., & Mead, M. (1987). The Case Research Strategy in Studies of Information Systems. MIS Quarterly, 11(3), 369. https://doi.org/10.2307/248684

Botan, C. (1996). Communication work and electronic surveillance: A model for predicting panoptic effects. Communication Monographs, 63, 293–313.

Bridge, M. C., & Schrodt, P. (2013). Privacy Orientations as a Function of Family Communication Patterns. Communication Reports, 26(1), 1–12. https://doi.org/10.1080/08934215.2013.773054

Brown, W. S. (1996). Technology, Workplace Privacy and Personhood. Journal of Business Ethics, 15(11), 1237–1248. Retrieved from https://www-jstor-org.ezproxy.uct.ac.za/stable/25072848?seq=1#metadata_info_tab_contents

CA Technologies. (2018). Insider Threat - 2018 Report. Retrieved from CA Technologies website: https://www.ca.com/content/dam/ca/us/files/ebook/insider-threat-report.pdf

Caughlin, J. P., & Afifi, T. D. (2004). When is Topic Avoidance Unsatisfying? Examining Moderators of the Association Between Avoidance and Dissatisfaction. Human Communication Research, 30(4), 479–513. https://doi.org/10.1111/j.1468-2958.2004.tb00742.x

Chang, S. E., Liu, A. Y., & Lin, S. (2015). Exploring privacy and trust for employee monitoring. Industrial Management & Data Systems, 115(1), 88–106. https://doi.org/https://doi.org/10.1108/IMDS-07-2014-0197

Chory, R. M., Vela, L. E., & Avtgis, T. A. (2016). Organizational Surveillance of Computer-Mediated Workplace Communication: Employee Privacy Concerns and Responses. Employee Responsibilities and Rights Journal, 28(1), 23–43. https://doi.org/10.1007/s10672-015-9267-4

Creswell, J. (2009). Research Design: Qualitative, Quantitative, and Mixed Methods Approaches (3rd ed.). CAlifornia: SAGE Publications.

Cropanzano, R., & Greenberg, J. (1997). Progress in Organizational Justice: Tunneling Through the Maze. In C. L. Cooper & I. T. Robertson (Eds.), International Review of Industrial and Organizational Psychology (Volume 12, pp. 317–372). Retrieved from https://www.researchgate.net/publication/261286563_Progress_in_Organizational_Justice_Tunneling_Through_the_Maze

Cybersecurity Insiders. (2018). Insider Threat 2018 Report. Crowd Research Partners, 41. Retrieved from chrome-extension://oemmndcbldboiebfnladdacbdfmadadm/https://www.cybersecurity-insiders.com/wp-content/uploads/2016/09/Insider-Threat-Report-2018.pdf

D'Urso, S. C. (2006). Who's watching us at work? Toward a structural-perceptual model of electronic monitoring and surveillance in organizations. Communication Theory, 16, 281–303.

Darke, P., Shanks, G., & Broadbent, M. (1998). Successfully completing case study research: combining rigour, relevance and pragmatism. Information Systems Journal, 8(4), 273–289. https://doi.org/10.1046/j.1365-2575.1998.00040.x

Eastlick, M. A., Lotz, S. L., & Warrington, P. (2006). Understanding online B-to-C relationships: an integrated model of privacy concerns, trust, and commitment . Journal of Business Research, 59(8), 877–886.

Elifoglu, H., & Abel, I. (2018). Minimizing Insider Threat Risk with Behavioral Monitoring. Review of Business, 38(2), 61–74. Retrieved from https://www.stjohns.edu/academics/schools-and-colleges/peter-j-tobin-college-business/departments-and-faculty/tobin-faculty/review-business-interdisciplinary-journal-risk-and

Eminağaoğlu, M., Uçar, E., & Eren, Ş. (2009). The positive outcomes of information security awareness training in companies - A case study. Information Security Technical Report, 14(4), 223–229. https://doi.org/10.1016/j.istr.2010.05.002

Ernst & Young. (2016). Managing insider threat - A holistic approach to dealing with risk from within. Retrieved from Ernst & Young LLP website: https://www.ey.com/Publication/vwLUAssets/EY-managing-insider-threat-a-holistic-approach-to-dealing-with-risk-from-within/$FILE/EY-managing-insider-threat.pdf

Fairweather, N. B. (1999). Surveillance in Employment: The Case of Teleworking. Journal of Business Ethics, 22(1), 39–49. Retrieved from https://www-jstor-org.ezproxy.uct.ac.za/stable/25074188?seq=1#metadata_info_tab_contents

Fayol, H. (2016). General and Industrial Management. Ravenio Books.

Friedman, B. A., & Reed, L. J. (2007). Workplace Privacy: Employee Relations and Legal Implications of Monitoring Employee E-Mail Use. Employee Responsibilities and Rights Journal, 19(2), 75–83.

Given, L. (2008). The SAGE Encyclopedia of Qualitative Research Methods. https://doi.org/10.4135/9781412963909

Greenberg, A. (2018). The Untold Story of NotPetya, the Most Devastating Cyberattack in History | WIRED. Retrieved April 20, 2019, from wired.com website: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Hagen, J. M., Albrechtsen, E., & Hovden, J. (2008). Implementation and effectiveness of organizational information security measures. Information Management and Computer Security, 16(4), 377–397. https://doi.org/10.1108/09685220810908796

Holland, P. J., Cooper, B., & Hecker, R. (2015). Electronic monitoring and surveillance in the workplace: The effects on trust in management, and the moderating role of occupational type. Personnel Review, 44(1), 161–175. https://doi.org/https://doi.org/10.1108/PR-11-2013-0211

Jin, S. A. A. (2012). “To disclose or not to disclose, that is the question”: A structural equation modeling approach to communication privacy management in e-health. Computers in Human Behavior, 28(1), 69–77. https://doi.org/10.1016/j.chb.2011.08.012

Kim, K., & Kim, J. (2011). Third-party privacy certification as an online advertising strategy: an investigation of the factors affecting the relationship between third-party certification and initial trust. Journal of Interactive Marketing, 25(3), 145–158.

Kroll. (2018). Global Fraud & Risk Report. Retrieved from https://www.bentley.edu/files/2017/04/05/Kroll Global Fraud and Risk Report.pdf

Lee, S., & Kleiner, B. H. (2003). Electronic surveillance in the workplace. Management Research News, 26(2/3/4), 72–81. https://doi.org/10.1108/01409170310784014

Leskin, P. (2018). Biggest data breaches of 2018 - Business Insider. Retrieved April 20, 2019, from Businessinsider.com website: https://www.businessinsider.com/data-hacks-breaches-biggest-of-2018-2018-12?IR=T

Maconachy, V., Schou, C., Welch, D., & Ragsdale, D. J. (2001). A Model for Information Assurance: An Integrated Approach. Proceedings of the 2nd Annual IEEE Systems, Man, and Cybernetics Information Assurance Workshop, 306–310. West Point, NY.

Mattson, M., & Brann, M. (2002). Managed care and the paradox of patient confidentiality: A case study analysis from a communication boundary management perspective. Communication Studies, 53(4), 337–357. https://doi.org/10.1080/10510970209388597

Meyer, J. P., & Allen, N. J. (1991). A three-component conceptualization of organizational commitment. Human Resource Management Review, 1(1), 61–89. https://doi.org/10.1016/1053-4822(91)90011-Z

Miniwatts Marketing Group. (2019). Internet Growth Statistics 1995 to 2019 - the Global Village Online. Retrieved April 20, 2019, from https://www.internetworldstats.com/emarketing.htm

Mowday, R. T. (1998). Reflections on the study and relevance of organizational commitment. Human Resource Management Review, 8(4), 387–401.

Netshakhuma, N. S. (2019). Assessment of a South Africa national consultative workshop on the Protection of Personal Information Act (POPIA). Global Knowledge, Memory and Communication, ahead-of-print(ahead-of-print). https://doi.org/10.1108/gkmc-02-2019-0026

Nyhan, R. C. (2000). Changing the Paradigm: Trust and its Role in Public Sector Organizations. The American Review of Public Administration, 30(1), 87–109. https://doi.org/10.1177/02750740022064560

O'Reilly, C. A., & Chatman, J. (1986). Organizational commitment and psychological attachment: The effects of compliance, identification, and internalization on prosocial behavior. Journal of Applied Psychology, 71(3), 492–499. https://doi.org/10.1037/0021-9010.71.3.492

Oliver, H. (2002). Email and internet monitoring in the workplace: Information privacy and contracting-out. Industrial Law Journal, 31(4), 321–352. https://doi.org/10.1093/ilj/31.4.321

Petronio, S. (2002). Boundaries of privacy: Dialectics of disclosure. New York: Albany: State University of New York Press.

Petronio, S. (2004). Road to developing communication privacy management theory: Narrative in progress, please stand by. Journal of Family Communication, 4, 193–208.

Petronio, S., & Reierson, J. (2009). Regulating the Privacy of Confidentiality: Grasping the Complexities through Communication Privacy Management Theory. In T. Afifi & W. Afifi (Eds.), Uncertainty, Information Management, and Disclosure Decision: Theories and Application (pp. 365–383). New York, NY: Routledge.

Petronio, S., Sargent, J., Andea, L., Reganis, P., & Cichocki, D. (2004). Family and friends as healthcare advocates: Dilemmas of confidentiality and privacy. Journal of Social and Personal Relationships Copyright ©, 21(1), 33–52. https://doi.org/10.1177/0265407504039838

Raimondi, G., Nußberger, A., Trajkovska, M., Guerra, L., Bianku, L., Karakaş, I., … Prebensen, S. Barbulescu v. Romania. , (2017).

Romo, L. K., & Vangelisti, A. L. (2014). Money Matters: Children's Perceptions of Parent-Child Financial Disclosure. Communication Research Reports, 31(2), 197–209. https://doi.org/10.1080/08824096.2014.907147

Rosenberg, R. S. (1999). The Workplace on the Verge of the 21st Century. Journal of Business Ethics, 22(1), 3–14. Retrieved from https://www-jstor-org.ezproxy.uct.ac.za/stable/25074185?seq=1#metadata_info_tab_contents

Schou, C. D., & Trimmer, K. J. (2004). Information assurance and security . Journal of Organizational and End User Computing, 16(3), i–vii.

Scott, K. D. (1980). The causal relationship between trust and the assessed value of management by objectives. Journal of Management, 6, 157–175.

Sewell, G., & Barker, J. R. (2006). Coercion versus care: Using irony to make sense of organizational surveillance. Academy of Management Review, (31), 1–24.

Shaw, R. S., Chen, C. C., Harris, A. L., & Huang, H. J. (2009). The impact of information richness on information security awareness training effectiveness. Computers and Education, 52(1), 92–100. https://doi.org/10.1016/j.compedu.2008.06.011

Snyder, J. L. (2010). E-mail privacy in the workplace: a boundary regulation perspective. Journal of Business Communication, 47(3), 266–294.

Snyder, J. L., & Cistulli, M. D. (2011). The Relationship Between Workplace E-Mail Privacy and Psychological Contract Violation, and Their Influence on Trust in Top Management and Affective Commitment. Communication Research Reports, 28(2), 121–129. https://doi.org/10.1080/08824096.2011.565270

Stanton, J., & Stam, K. (2003). Information technology, privacy, and power within organizations: A view from boundary theory and social exchange perspectiv. Surveillance and Society, 1(2), 152–190.

Steers, R. M. (1977). Antecedents and Outcomes of Organizational Commitment. Administrative Science Quarterly, 22(1), 46–56. https://doi.org/10.2307/2391745

Stewart, J. M., Chapple, M., & Gibson, D. (n.d.). CISSP: certified information systems security professional study guide.

Tabak, F., & Smith, W. P. (2005). Privacy and Electronic Monitoring in the Workplace: A Model of Managerial Cognition and Relational Trust Development. Employee Responsibilities and Rights Journal, 17(3), 173–189. https://doi.org/10.1007/s10672-005-6940-z

Taddei, S., & Contena, B. (2013). Privacy, trust and control: which relationships with online self-disclosure? Computers in Human Behavior, 29(3), 821–826.

Townsend, A. M., & Bennett, J. T. (2003). Privacy, technology, and conflict: Emerging issues and action in workplace privacy. J Labor Res, 24, 195. https://doi.org/https://doi.org/10.1007/BF02701789

Turnley, W. H., & Feldman, D. C. (2000). Re-examining the effects of psychological contract violations: unmet expectations and job dissatisfaction as mediators. Journal of Organizational Behavior, 21(1), 25–42. https://doi.org/10.1002/(SICI)1099-1379(200002)21:1<25::AID-JOB2>3.0.CO;2-Z

Waters, S., & Ackerman, J. (2011). Exploring privacy management on facebook: Motivations and perceived consequences of voluntary disclosure. Journal of Computer-Mediated Communication, 17(1), 101–115. https://doi.org/10.1111/j.1083-6101.2011.01559.x

Wikipedia. (n.d.). Edward Snowden. Retrieved from https://en.wikipedia.org/wiki/Edward_Snowden

World Economic Forum. (2019). The Global Risks Report 2019. Retrieved from World Economic Forum website: http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf

Wu, K. W., Huang, S. Y., Yen, D. C., & Popova, I. (2012). The effect of online privacy policy on consumer privacy concern and trust. Computers in Human Behavior, 28(3), 889–897.

Yin, R. K. (2017). Case Study Research: Design and Methods (6th ed.). Thousand Oaks, California: SAGE Publications.