Horizon Scanning Series

The Internet of Things

Monitoring and Surveillance in the Contemporary Workplace

This input paper was prepared by Peter Holland

Suggested Citation

Holland, P (2019). Monitoring and Surveillance in the Contemporary Workplace. Input paper for the Horizon Scanning Project "The Internet of Things" on behalf of the Australian Council of Learned Academies, www.acola.org.

Monitoring and Surveillance in the Contemporary Workplace

Professor Peter Holland

Swinburne Business School

Swinburne University of Technology

John Street

Hawthorn VIC 3122 Australia

pjholland@swin.edu.au

Examining the Evidence

It is clear with the advent of the internet of things (IoT), it has and will continue to enable more organisations to gather information on customers clients and especially employees. We are therefore at an interesting point in time with the emergence of the IoT as part of the 4th industrial revolution. In 2016 I co-authored a special issue of the International Journal of Human Resources Management on the use of technology at work and identified it as being potentially 'smart' in a sense of increasingly productivity or 'dark' in that it was used to increase surveillance and control over employees at the detriment of the employment relationship which should be underpinned by trust (Holland & Bardoel, 2016). If the recent passed is anything to go by the use of technology to increase (electronical) monitoring and surveillance (EMS) of employees has raised significant concerns resulting in court cases and an emphasis on the 'dark' side of technological use in the workplace. Before exploring these issues it is worth briefly considering how the dimensions of privacy have changed with the IoT to frame these issues.

Employee Privacy in the Digital Age

Whilst the concept of privacy can be elusive as it is a multi-dimensional construct, and too complex for this brief, I provide a contemporary frameworks of privacy in terms of how the boundaries through the IoT can and will change workplace relationships. Westin (1967) and Altman (1975) identified that privacy operates through individual, group, organisational and institutional levels with the belief that the individual can proactively manages their privacy, with the key intrusive force being technology. Although developed in the pre-internet era this point is arguably more relevant today than ever. However, with the IoT as the key intrusive

force this imbalance leaves employees significantly less protected in terms of their privacy and potentially their data than ever before against employer intrusion, with potentially little recourse to protection or managing these boundaries. Individuals have a need and expectation for privacy and in the workplace clear boundaries are required on how much of oneself is revealed to the employer (Fairweather, 1999; Petronio et al, 1998), especially in this era of intense and relentless EMS both inside and outside the workplace. Our on-going research and that of others in Australia (Holland, Hecker & Copper, 2016; Martin, Wellon & Grimmer, 2016), highlight that the more EMS employees perceive in the workplace the greater the decrease in trust between them and management. In modern management speak, these practices are unlikely to enhance the relationship, or increase engagement, commitment or moral, key factors in a productive and harmonious workplace. As recent cases highlight, which I have co-researched, there is every right for employees to be concerned about what information their employer is collecting and how it is used.

The Case of Starr (Barnes, Balnave & Holland, 2018)

Mr Daniel Starr a Public Servant was dismissed for posting information under an alias what his management considered inappropriate messages about the Department of Human Services (DHS). Whilst there were derogatory comment about clients of the DHS in these posts, the focus of DHS management appeared to be on:

- Criticism of the Federal Government and its policies;
- Encouraging members of the public to address their complaints to their local member of parliament;
- Disclosed problem with delays in the system.

Whilst Starr was subsequently re-instated on appeal, there are several key issues in this case that emerged, including the on-line activity occurred outside work as a member of the public which raised issues of the freedom of public servants to be able to have an opinion as a member of the public. However, in the context of the 'dark' side of this investigation what become apparent was the level and intensity of the investigation undertaken by the DHS. Evidence tabled in court indicated that the Business Integrity Office (BIO) had trawled through thousands of posts stretching back over a decade using comments about local landmarks and time of holiday breaks to seek and identify Starr. The extent of this search indicated how far the DHS was prepared to go in using advanced technology to arguably stifle debate and criticism and

use tax payer funds to in effect suppress information that was arguably in the public interest, and send a warning to other staff.

Concerning trends

The Starr case is not an isolated incident, with the issues associated with the federal governments' so-called Robo-Debt which highlighted similar strategies with attempts to silence public servants through the threat of disciplinary procedures or criminal prosecutions for those commenting on the system (Towell, 2017). Finally the case of Banerji where public servant Michaela Banerji posted under an alias critical comments of Australia's refugee policy in her own time and did not indicated she was a public servant. She also was tracked down and dismissed – a decision that was subsequently upheld.

The Case of Jeremy Lee (Holland & Tham, 2019)

In the private sector the case of Jeremy Lee highlights the use and misuse and level (or lack) of knowledge in managing advances in biometrics. Biometrics refers to technologies that measure and analyse unique characteristics of an individual which are generally considered innate and distinctive to identify employees (Moradoff, 2010). In the case of Lee this was a fingerprint scanner for clocking on and off work. Lee was sacked for not being prepared to hand over his biometric data to the company. His appeal for wrongful dismissal was rejected but was sent to the full bench of the Fair Work Commission for consideration due the significance of the case. Lee was successful in having his dismissal overturned. However, in the context of this brief the following issues came to light. In each hearing, the lack of knowledge and (legal) protocols by management to protect this data was variously considered concerning and disturbing, with several breaches of the *Privacy Act*. The issue of punitive sanctions for protecting one's own privacy and sovereignty of personal data is of equal concern. Noting this was simply for the change of the payroll system. Whilst in this case the outcome has helped to highlight, identify and clarify the need to protect individual privacy from arbitrary or unlawful interference in the workplace, without such people standing up to these arbitrary management decision underpinned by coercive threats of discipline and termination, they will likely to continue to erode employee privacy in and outside of work.

Conclusions

In dealing with issues of managerial prerogative and employee privacy rights, these cases highlighted indicate the emerging contested terrain in the employment relationship associated

with IoT. It also suggests a darker side, with the increasing integration of technology into the workplace. The depth and invasiveness of this technology is only now being understood and as the cases above highlight there are what might be described as some disturbing trends emerging. There is a fundamental question underpinning these issues which is *why* organisations have decided to implement these aggressive policies underpinned by the power of this new technology. In my discussion with managers the often simple reply is that we can. The key therefore in this may be to educate both managers and employees on the right, implications and impact of this new era of the Internet of Things.

References

Altman, I. (1975). *The Environment and Social Behavior: Privacy, Personal Space, Territory, Crowding*. Brooks/Cole, Monterey.

Comcare v Banerji [2019] HCA 23, C12/2018 (7 August 2019)

Barnes, A., Balnave, N., & Holland, P. (2018). 'Utterly disgraceful': social media and the workplace. *Australian Journal of Public Administration*, *77*(3), 492-499. https://doi.org/10.1111/1467-8500.12314

Fairweather, N. (1999). Surveillance in employment – the case of teleworking. *Journal of Business Ethics*, 22(2):39-49.

Holland, P., Cooper, B. & Hecker, R. (2016). Social Media: The New Employee Voice? *International Journal of Human Resource Management*, 27(21): 2621-2634.

Holland, P. & Tham, T.L. (2019). Workplace Biometric: Protecting Workplace Privacy One Fingerprint at a Time (*Unpublished*)

Holland, P. & Bardoel, A. (2016). Exploring the Smart and Dark side of Work in an Electronic Era. *International Journal of Human Resource Management*, 27(21): 2579-2581.

Lee, J. v Superior Wood Pty Ltd T/A Superior Wood, (FWC 4762), November 2018.

Lee, J. v Superior Wood Pty Ltd t./a Superior Wood, (FWC 95), January 2019.

Lee, J. v Superior Wood Pty Ltd, (FWCFB 2946), May 2019.

Martin, A., Wellon, J. & Grimmer, M. (2016).Eye on Your Work. *International Journal of Human Resource Management*, 27(21): 2579-2581.

Moradoff, N. (2010). Biometrics: Proliferation and constraints to emerging and new technologies. *Security Journal*, *23*(4): 276-298.

Petronio, S. (2002). *Boundary of Privacy: Dialectics of Disclosure*, SUNY Press, New York: NY.

The *Privacy Act 1988* (Privacy Act) Cth. Canberra. Australia: OAIC.

Towell, N. (2017). 'Robo-Debt' Centrelink Workers Threatened with Prosecution as Bosses Try to Stem the Leaks. *The Canberra Times* (January 18).

Westin. A. F, (1967) *Privacy and Freedom*. New York: Athenaeum Press.