McParland, Cliona; Connolly, Regina

Conference Paper

Employee Monitoring in the Digital Era: Managing the Impact of Innovation

Provided in Cooperation with:
IRENET - Society for Advancing Innovation and Research in Economy, Zagreb

Suggested Citation: McParland, Cliona; Connolly, Regina (2019) : Employee Monitoring in the Digital Era: Managing the Impact of Innovation, In: Proceedings of the ENTRENOVA - ENTerprise REsearch InNOVAtion Conference, Rovinj, Croatia, 12-14 September 2019, IRENET - Society for Advancing Innovation and Research in Economy, Zagreb, pp. 548-557

This Version is available at:
https://hdl.handle.net/10419/207717

Employee Monitoring in the Digital Era: Managing the Impact of Innovation

Cliona McParland
Dublin City University, Ireland
Regina Connolly
Dublin City University, Ireland

Abstract

The many obvious benefits that accompany digital technology have been matched by some less welcome and more contentious impacts. One of these is the steady erosion of privacy. For example monitoring and surveillance has become a fundamental part of the workplace environment, with employee performance often the main object of scrutiny. With companies now competing within a rapidly changing global economy, managers are forced to satisfy market trends that are driven by productivity and efficiency. Attempts to satisfy these imperatives have resulted in a relentless drive to improve performance and increase efficiency. In fact, the increasing number of organisations that monitor employees through advanced digital technologies has added a dystopian edge to existing employee privacy concerns, particularly as many employees are unable to exercise choice in relation to use of these technologies. If unaddressed, their concerns have potential to impact the psychological contract between employee and employer, resulting in loss of employee trust, negative attitudes and counterproductive work behaviours. This paper outlines some of the emerging issues relating to use of employee monitoring technologies. It summarises both management rationale for monitoring as well as employee privacy concerns in an effort to balance the perspectives of both parties.

Keywords: privacy, monitoring, trust, surveillance, empowerment, workplace, behaviours
JEL classification: O33

Introduction

Organisations and employees exist within a rapidly changing business context – an environment which over time has forced many employers to push for greater productivity and efficiency in order to satisfy market trends and remain competitive in the market. Technological advancements have facilitated the achievement of those efficiencies and in particular have enabled employers to gain more detailed insights into employee performance, including insights as to the use of technology both during and after work hours. Understandably however, these developments have generated significant privacy concerns for employees – particularly as they are often unsure of how management will use the information gathered on them. This in part stems from the fact that the volume and frequency of the data collection and the ways in which the collated information will be used, stored and managed is rarely disclosed to the employee. Consequently, this type of surveillance can significantly impact the relationship between the employee and employer, as for the employee, knowing that their performance is being monitored and that it may be used against them as part of a performance assessment for example, can negatively impact their productivity,

performance, motivation as well as reduce their trust in their employers and organisation. Moreover, it can send a message to the employee that they are under-performing, that they lack commitment or they are untrustworthy, which in turn can lead them to engage in deviant or counterproductive behaviours.

As profit driven organizations strive to manage their business in an efficient and productive manner, it is perhaps unrealistic to expect that organizations would not avail of the obvious empowering benefits that digital technologies, including communication, location and activity tracking applications afford them. Furthermore, it can be argued that they may in fact have legitimate reasons to monitor employee actions in the first place. However, for an employee, knowing that their performance is being monitored and that there is increased potential for that information to be used against them as part of performance assessment or promotion evaluation exercises inevitably changes their perspective of the parameters of the employment relationship. In fact these concerns and the associated power imbalance can fracture and severely damage the employee-employer social contract. Moreover, this opacity between how the information is collated and ultimately used by management creates an asymmetric power balance that can negatively impact the employee, reducing their productivity, motivation, trust in their employers and consequent commitment to the organisation.

This unequal balance of power resulting from workplace surveillance raises a number of questions, in particular those relating to the ethical nature of managements' ability to monitor employees' technology-enabled interactions. The aim of this paper therefore is to outline some of the major issues relating to workplace surveillance. It starts by discussing dataveillance and related privacy concerns from the employee perspective. The potential impact of workplace surveillance on employee trust and how this may manifest is described. The motivation behind managements' decision to employ monitoring technologies in the workplace is also outlined. Following this, the effort to balance the interests of both parties is addressed and discussed in detail.

Surveillance: An Employee Perspective and Concerns

In a drive to reduce costs and improve efficiency, companies are employing an increasing array of tracking and monitoring technology to allow them to view what their employees are doing at all times. In fact, a 2017 study of 1627 firms completed by the American Management Association found that 78% of major companies monitor the Internet usage, phone and email of their employees. This represents a steep increase over the past 20 years (from a figure of 35% in 1997). The figure is even higher for companies within the financial sector with over 92.1% of firms within that category participating in some form of surveillance. However, while such metrics may increase compliance and productivity, they come at a cost to employees. As Connolly (2013) (in Semuels, 2013) notes, the technology is being used to satisfy the needs of the employer, but is being leveraged against the employee. It provides employers with an increasing array of data to use to justify changes in the workplace and tilts the playing field in favour of the industry against the employee. For example, the information extracted from that data can be used to justify pay cuts, to pay people piecemeal or to fire employees outright. In fact, a study conducted by AMA in 2017 found that 26% of employers had fired employees for misuse of the Internet, 25% had terminated employees for email misuse and 6% had fired employees for misuse of office phones.

Perhaps a more indirect and nuanced cost relates to actual the employee-employer relationship however. For example, employee/employer relationships are

typically perceived as being a two-way exchange, with the focus squarely upon the perceptions of reciprocal promises and obligations of both parties (Guest, 2004). In short, employers have implicit and sometimes unvoiced expectations regarding employee contributions, in terms of effort, loyalty and ability for organizational inducements such as pay, promotion and job security (Morrison and Robinson, 1997; Conway and Briner, 2002). However, the monitoring of performance presents a threat to that previously accepted contract and indeed can be perceived as a breach of expectations by the employer, which in turn can lead to feelings of injustice or betrayal of employees (Morrison and Robinson, 1997). Moreover, it may be met with resistance from employees as it accentuates their concerns over privacy rights and due process.

Therefore, it is apparent that what companies gain in productivity may be lost in engagement, empowerment and trust, particularly if there is a lack of transparency regarding the monitoring behaviour and how the collated data is used. In fact, recent research (Martin et al., 2016) conducted in Australia has shown that attitudes towards surveillance in the workplace play an important role in determining whether surveillance systems and practices result in counterproductive work behaviours. As trust and fairness are core aspects of any psychological contract (Guest, 2004), workplace surveillance presents a considerable threat to the previously perceived trustworthiness and fairness of employers who now have the potential to leverage performance information against employees. It is therefore unsurprising that there is a small but growing body of evidence which shows that surveillance in the workplace can negatively influence employee stress levels, work attitudes and trust in management (Holland et al., 2015) thus causing employees to manipulate the surveillance system (Taylor and Bain, 1999), avoid monitored areas (Nussbaum and DuRivage, 1986; Stanton, 2002; Stanton and Weiss, 2000) and deliberately falsify the amount of work they are completing (Taylor and Bain, 1999) in some instances. Moreover, such behaviours can be further conceptualised through absenteeism, lateness and lack of productivity (Martin et al., 2016) as well as other deliberate violations of company regulations (Robinson and Bennett, 1997). While it is apparent that employees often alter or modify their behaviour in response to management monitoring activities, it is important to note that the use of such techniques may result in other more worrying outcomes. For example, many workers experience high degrees of stress knowing that their activities and interactions can be monitored by their employers (Tavani, 2004). The obvious negative impact that such surveillance techniques impose on employee morale is a serious consideration.

A number of theories in the literature can help provide an understanding of how employees react or behave when they are aware, they are being monitored in the workplace however. Protection motivation theory for example, suggests that employees protect their sensitive information by analysing the threats to their privacy, the likelihood their information will be breached, the severity of an attack and their ability to cope should it occur (Rodgers, 1975; Li, 2012). In this way, protection motivation theory suggests that employees will adjust their behavioural response in order to cope with or avoid what they deem to be a threat to their privacy. Similarly, psychological reactance theory suggests that employees may engage in counterproductive behaviours if they believe their freedom or ability to control a situation is under threat (Jensen and Raver, 2012; Graupmann et al., 2012). Communication privacy management (CPM) theory is also an important focus in research on electronic surveillance and the subsequent workplace attitudes and behaviours. For example CPM suggests that individuals manage the boundaries around their personal information in order to determine what information they chose to disclose and what information they wish to protect (Petronio, 2002). When applied

to the computer-mediated workplace environment however, this theory posits that employees make the decision to disclose or conceal their personal information based on the expected use of the information and perhaps more significantly their relationship with the organisation (Stanton and Stam, 2003). In a similar vein, researchers Kim and Kankanhalli (2009) combined the theory of Status Quo Bias with theories of technology adoption to explore the psychological and decision-making mechanisms that cause a user to demonstrate resistance to system implementation in the workplace.

It is clear that trust is an important construct that further supports the link between employee attitudes and workplace surveillance. For example a growing body of research has suggested that trust is a critical component in the relationship between management and employees particularly within the computer-mediated or knowledge based organisations (Dietz and Fortin, 2007; Holland et al., 2015; Mayer et al., 1995; Boxall and Purcell, 2011; Searle et al., 2011). Moreover, trust is central to social exchange theory (SET) with many researchers (Holland et al., 2015; Gould-Williams, 2003; Stanton and Stam, 2003) arguing that a lack of trust within the relationship can negatively impact an employees' behaviours, actions or willingness to share or disclose their information in the workplace. Further research has linked trust in management to work performance (Ferrin and Dirks, 2003; Tyler, 2003; Innocenti et al., 2011), contributions to the organisation (Boxall and Purcell, 2011) and positive workplace behaviours (Rousseau et al., 1998; Dirks and Ferrin, 2002; Connell et al., 2003). Similarly, from a strategic or HR perspective it has been linked closely to employee commitment (Searle et al., 2011; Nichols et al., 2009; Kepes and Delery, 2007), employee wellbeing (Bijlsma and Koopman, 2003) and employee turnover (Connell et al., 2003) within the organisation.

Surveillance: Managements Perspective and Motivations

Workplace surveillance clearly raises many ethical and social issues. However, in order to adequately address many of these issues we must first consider the motivations behind management's decision to employ monitoring technologies in the first place. While many reports emphasis the risks faced by the employee, it is reasonable to assume that in some instances management may have legitimate reasons to monitor their employee's actions. For example, profit driven organisations aim to manage their business in an efficient and productive manner and as such it may be unreasonable to expect that such companies would not avail of methods or employ technologies to ensure that their employees are completing the job they are being paid to do. Furthermore and perhaps more notably, organisations continually face the risk of adverse publicity resulting from offensive or explicit material circulating within the company and as such many employ monitoring technologies to protect themselves from costly litigation claims (Laudon & Laudon, 2001). The Internet has increased the possible threat of hostile work environment claims by providing access to inappropriate jokes or images that can be transmitted internally or externally at the click of a button (Lane, 2003). Moreover, a study carried out by Forbes in 2012 found that 64% of employees visit non-work related sites on a daily basis.

Whilst the need to improve productivity is a common rationale for employee monitoring, other motivations such as minimising theft and preventing workplace litigation can be considered equally justifiable in the eyes of management seeking to protect the interests of the organisation. The former motivation is particularly understandable as research shows that employees stole over 15 billion dollars in inventory from their employers in the year 2001 alone (Lane, 2003). In addition, the seamless integration of technology into the workplace has increased the threat of

internal attacks with Lane (2003) noting the ease at which sensitive corporate data and trade secrets can be down- loaded, transmitted, copied or posted onto a Web page by an aggrieved employee. Internal attacks typically target specific exploitable information, causing significant amounts of damage to an organisation (IBM, 2006). It is important to note however not all insider attacks are malicious by nature. In fact careless, negligent or poorly trained employees unintentionally cause an equally high number of security breaches and data leaks each year. In fact, Crowd Research Partners (2017) currently estimate that companies now consider the equal likelihood that insider attacks are the direct result of accidental or unintentional breaches. The study suggests that 67% of accidental insider attacks are the direct result of a phishing attack, whereby employees are tricked into sharing sensitive information with someone they believe to be a trusted contact or a legitimate business partner. Other culprits include weak or reused passwords (56%), unlocked or unsecured devices (44%) and poor password sharing practice (44%). It is perhaps somewhat unsurprising to note that it is now estimated that as many as 86% of organisations have or are currently building an insider threat program in order to protect themselves from insider threats, both malicious and accidental in nature. Management need to ensure that their employees use their working time productively, to the best interests of the company and are therefore benefiting the organisation as a whole (Nord et al., 2006). It is apparent however, that tensions will remain constant between both parties unless some form of harmony or balance between the interests of both the employer and employee is achieved.

In order to balance this conflict of interests however it is vital that clearly defined rules and disciplinary offences are implemented into the workplace (Craver, 2006). The need for structure becomes all the more apparent when one considers the differing views and tolerance levels certain managers may hold (Selmi, 2006). For example, if an employee is hired to work, then technically they should refrain from sending personal emails or shopping online during working hours. However, as a general rule, most management will overlook these misdemeanours as good practice or in order to boost worker morale. The situation becomes more serious however when the abuse of Internet privileges threatens to affect the company itself, be it through loss of profits or adverse publicity for the company. Furthermore, the problem increases as boundaries in the modern workplace begin to blur and confusion between formal and informal working conditions arise (Evans, 2007). For example by allowing an employee to take a company laptop into the privacy of their own home, management could be sending out a message that the computer can be used for personal use which may lead to the employee storing personal data on management's property. Legally, the employer would have claims over all of the data stored on the computer and could use it to discipline or even terminate an employee. In fact, it is this apparent lack of natural limit in regards what is acceptable or indeed unacceptable relating to workplace privacy which makes the task of defining appropriate principles all the more difficult to comprehend (Godfrey, 2001).

The issue of workplace surveillance raises a number of questions, in particular those relating to the ethical nature of managements' ability to monitor employees' technology-enabled interactions. However, as workplace surveillance is unlikely to decrease and may in fact become a more widely embedded condition of employment, the question will move from asking whether it is acceptable, to how it can be more effectively managed so as to avoid counter productive work behaviours and negative organisational impacts.

Surveillance: The Zone of Acceptance

It is becoming increasingly apparent that the use of modern technologies in the workplace represents a double-edged sword for employers whereby the same tools that can be used to increase productivity and efficiency can be abused or misused by the employee. Moreover, there is a significant disparity between management and employee perspectives on the issue of workplace surveillance. The uncertainty and lack of control related to the use of these communication monitoring technologies in the workplace reflects the significant asymmetry that exists in terms of what they mean to management versus the employee. While it is apparent that technology has created better, faster and cheaper ways for individuals to satisfy their own needs, the capability to leverage this technology is far higher for companies than for the employee. Because unequal forces, leading to asymmetric information availability, tilt the playing field significantly in favour of industry, such technologies do not create market benefit to all parties in an equitable manner (Prakhaber, 2000). As such one of the major tasks facing the computer-mediated organisation is that of identifying the factors to improve employees' attitudes and behavioural reactions towards surveillance in the workplace. There is a distinct need for clear measures that govern the effective and fair use of communication technologies in the workplace allowing management to monitor their staff in a reasonable and rational manner. Management should consider the ethical and social impacts that surveillance techniques may have within the workplace and employ specific policies which may both minimise the negative implications associated with the use of such technology as well as helping to improve employee receptiveness overall.

Organisations looking for ways in which to balance this conflict of interest between management and employees are focusing towards the use of workplace policies, many of which are framed on established or predefined codes of ethics. For example, Marx and Sherizen (1991) argue that employees should be made aware in advance of any monitoring practices conducted in the workplace before it actually occurs. In this way the individual can electively decide whether or not he or she wishes to work for that particular organisation. Furthermore the authors suggest that the employee should have the right to both view information collated on them and challenge inaccurate information before it can be used against them. Similarly researchers Stanton and Stam (2006) argue that if an employee perceives some benefit to the surveillance they are likely to be more open to the surveillance, particularly if the reasons and benefits are communicated clearly to them. In fact, this idea of 'transparency' in relation to surveillance methods is commonly supported by many privacy advocates within the literature. Management need to have clearly defined sanctions in place within the organisation informing employees of the depth and detail of monitoring practices in the company whilst deterring them from abusing workplace systems.

Conclusion

The primary objective of this paper was to address the issue of electronic monitoring in the computer-mediated work environment. It explored the ethical impact of monitoring in the computer-mediated work environment, addressing whether management's ability to monitor employee actions in workplace represents good business practice or constitutes an invasion of privacy. While it is apparent that management may have legitimate reasons to monitor employees' actions in the workplace, the privacy rights of the employee cannot be ignored. In this way it is paramount that some form of harmony or balance between the interests of the

employer and the employee is achieved.

Technology-enabled surveillance and tracking of employees in increasing both in terms of pervasiveness and sophistication. However, whilst much colloquial discussion of workplace surveillance exists, empirical studies on this issue are in short supply. Moreover those studies that do exist are commonly beset by both conceptual and operational confusion. This in part stems from the fact that the lines regarding what are correct and moral forms of behaviour continually blur thus limiting our overall understanding of the main issues involved as well as the ways in which to target them. Furthermore, the use of Internet-based technologies in the workplace presents businesses and employees with opportunities to engage in behaviours for which comprehensive understandings or rules have not yet been established. As such it is imperative that future research aims to alleviate this confusion by addressing these issues from both a rigorous and relevant perspective. Moreover, a greater awareness of increased surveillance and the corresponding acuteness of information privacy concerns further point to the need for additional research on this issue.

The themes identified in this paper have implications for future academic work in the area of workplace surveillance. Thus in order to examine and understand the factors that inhibit and amplify workplace surveillance issues future researchers must begin by exploring these issues directly with those that face them, identifying legitimate employee concerns as well as establishing the types of technologies employed by management and perhaps most importantly why. Only then can we try to establish some form of balance or harmony between both parties in the computer-mediated workplace environment.

References

1. AMA (2017), "Workplace Monitoring and Surveillance", available at: http://www.amanet.org/research/ (31 January 2019).
2. Bijlsma, K., Koopman, P. (2003), "Introduction: trust within organisations", Personnel Review, Vol. 32, No. 5, pp. 543-555.
3. Boxall, P., Purcell, J. (2011), Strategy and Human Resource Management, 3rd edition, Palgrave Macmillan, Basingstoke.
4. Connell, J., Ferres, N., Travalione, T. (2003), "Engendering trust in manager-subordinate relationships", Personnel Review, Vol. 32, No. 5, pp. 569-587.
5. Conway, N., Briner, R. B. (2002), "A daily diary study of affective responses to contract breach and exceeded promises", Journal of Organizational Behaviour, Vol. 23, No. 3, pp. 287-302.
6. Craver, C. B. (2006), "Privacy issues affecting employers, employees and labour organizations", Louisiana Law Review, Vol. 66, pp. 1057-1078.
7. Crowd Research Partners (2017), "Insider Threat Report", Cyber-security Insiders, CA Technologies, available at: https://www.ca.com/content/dam/ca/us/files/ebook/insider-threat-report.pdf (16 August 2018).
8. Dietz, G., Fortin, M. (2007), "Trust and justice in the formation of joint consultation committees", Journal of International Human Resource Management, Vol. 18, No. 7, pp. 1159-1181.
9. Dirks, K., Ferrin, D. L. (2002), "Trust in leadership: meta-analytic findings and implications for research and practice", Journal of Applied Psychology, Vol. 87, No. 4, pp. 611-628.
10. Evans, L. (2007), "Monitoring technology in the American workplace: Would adopting English privacy standards better balance employee privacy and productivity?", California Law Review, Vol. 95, pp. 1115-1149.
11. Ferrin, D. L., Dirks, K. T. (2003), "The use of rewards to increase and decrease trust: mediating processes and differential effects", Organization Science, Vol. 1, No. 1, pp. 18-31.

12. Forbes (2012), "Employees really do waste time at work, available at: https://www.forbes.com/sites/cherylsnappconner/2012/07/17/employees-really-do-waste-time-at-work/#b0461805e6da (16 August 2018).
13. Godfrey, B. (2001), "Electronic work monitoring: An ethical model", in the Proceedings of the second Australian institute conference on computer ethics, Canberra, Australia, Academic Press, pp. 18-21.
14. Gould-Williams, J. (2003), "The importance of HR practices and workplace trust in achieving superior performance: a study of public-sector organizations", International Journal of Human Resource Management, Vol. 14, No. 1, pp. 28-54.
15. Graupmann, V., Jonas, E., Meier, E., Hawelka, S., Aichhorn, M. (2012), "Reactance, the self, and its group: When threats to freedom come from the ingroup versus the outgroup", European Journal of Social Psychology, Vol. 42, No. 2, pp. 164-173.
16. Guest, D. E. (2004). "The Psychology of the employment relationship: An analysis based on the psychological contract", Applied Psychology, Vol. 53, No. 4, pp. 541-555.
17. 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, Vol. 44, No. 1, pp.161-175.
18. IBM (2006), "Stopping insider attacks: How organizations can protect their sensitive information", available at: http://www-935.ibm.com/services/us/imc/pdf/gsw00316-usen-00-insider-threats-wp.pdf (16 August 2018).
19. Innocenti, L., Pilati, M., Peluso, A.M. (2011), "Trust as moderator in the relationship between HRM practices and employee attitudes", Human Resource Management Journal, Vol. 21, No. 3, pp. 303-317.
20. Jensen, J. M., Raver, J. L. (2012), "When self-management and surveillance collide: Consequences for employees' trust, autonomy, and discretionary behaviors", Group & Organization Management, Vol. 37, No. 3, pp. 308-346.
21. Kepes, S., Delery, J. E. (2007), "HRM systems and the problem of internal fit", in Boxall, P., Purcell, J., Wright, P. (Eds.), The Oxford Handbook of Human Resource Management, Oxford University Press, New York, NY, pp. 385-404.
22. Kim, H. W., Kankanhalli, A. (2009), "Investigating user resistance to information systems implementation: A status quo bias perspective", MIS Quarterly, Vol. 33, No. 3, pp. 567-582.
23. Lane, F. S. (2003), The naked employee: How technology is compromising workplace privacy, AMACOM, New York, NY.
24. Laudon, K. C., Laudon, J. P. (2001), Essentials of management information systems: Organisation and technology in the networked enterprise, 4th edition, Prentice Hall, Upper Saddle River, NJ.
25. Li, Y. (2012), "Theories in online information privacy research: A critical view and an integrated framework", Decision Support Systems, Vol. 54, No. 1, pp. 471-481.
26. Martin, A. J., Wellen, J. M., Grimmer, M. R. (2016), "An eye on your work: How empowerment affects the relationship between electronic surveillance and counterproductive work behaviours", The International Journal of Human Resource Management, Vol. 27, No. 21, pp. 2635-2651.
27. Marx, G., Sherizen, S. (1991), "Monitoring on the job: How to protect privacy as well as property", in Forester, T. (Ed.), Computers in the human context: Information technology, productivity, and people, MIT Press, Cambridge, MA, pp. 397-406.
28. Mayer, R. C., Davis, J. D., Schoorman, F. D. (1995), "An integrative model of organisational trust", Academy of Management Review, Vol. 20, No. 3, pp. 709-734.
29. Morrison, E. W., Robinson, S. L. (1997), "When employees feel betrayed: A model of how psychological contract violation develops", The Academy of Management Review, Vol. 22, No. 1, pp. 226-256.
30. Nord, G. D., McCubbins, T. F., Horn Nord, J. (2006), "E-monitoring in the workplace: Privacy, legislation, and surveillance software", Communications of the ACM, Vol. 49, No. 8, pp. 73-77.
31. Nichols, T., Danford, A., Tasiran, A. (2009), "Trust, employer exposure and the employment relations", Economic and Industrial Democracy, Vol. 30, No. 2, pp. 241-

265.
32. Nussbaum, K., DuRivage, V. (1986), "Computer monitoring: Mismanagement by remote control", Business and Society Review, Vol. 56, pp. 16-29.
33. Petronio, S. (2002), Boundaries of Privacy: Dialectics of Disclosure, State University of New York Press, Albany, NY.
34. Prakhaber, P. R. (2000), "Who owns the online consumer?", Journal of Consumer Marketing, Vol. 17, No. 2, pp. 158-171.
35. Robinson, S. L., Bennett, R. J. (1997), Workplace deviance: Its definition, its manifestations, and its causes, JAI Press, Greenwich, CT.
36. Rodgers, R. (1975). "A Protection Motivation Theory of Fear Appeals and Attitude Change", The Journal of Psychology – Interdisiplinary and Applied, Vol. 91, No. 1, pp. 93-114.
37. Rousseau, D., Sitkin, S., Burt, R., Camerer, C. (1998), "Not so different after all: a cross-discipline view of trust", Academy of Management Review, Vol. 23, No. 3, pp. 393-404.
38. Searle, R., Den Hartog, D.N., Weibel, A., Gillespie, N., Six, F., Hatzakis, T., Skinner, D. (2011), "Trust in the employer: the role of high-involvement work practices and procedural justice in European organizations", The International Journal of Human Resource Management, Vol. 22, No. 5, pp. 1069-1092.
39. Selmi, M. (2006). "Privacy for the working class: Public work and private lives", Louisiana Law Review, Vol. 66, pp. 1035-1056.
40. Semuels, A. (2013), "Monitoring up- ends balance of power at workplace some say", Los Angeles Times, available at: https://www.latimes.com/business/la-xpm-2013-apr-08-la-fi-mo-monitoring-upends-balance-of-power-at-workplace-20130408-story.html (04 April 2016).
41. Stanton, J. M. (2002), "Company profile of the frequent internet user: Web addict or happy employee?", Communications of the Association for Computing Machinery, Vol. 45, No. 1, pp. 55–59.
42. Stanton, J., Stam, K. (2003), "Information Technology, Privacy and Power within Organizations: A View from Boundary Theory and Social Exchange Perspectives", Surveillance and Society, Vol. 1, No. 2, pp. 152-190.
43. Stanton, J., Stam, K. (2006), The Visible Employee: Using Workplace Monitoring and Surveillance to Protect Information Assets without Compromising Employee Privacy or Trust, Information Today, Inc., Medford, New Jersey.
44. Stanton, J. M., Weiss, E. M. (2000), "Electronic monitoring in their own words: An exploratory study of employees' experiences with new types of surveillance", Computers in Human Behavior, Vol. 16, No. 4, pp. 423-440.
45. Tavani, H. T. (2004), Ethics and technology: Ethical issues in an age of information and communication technology, John Wiley & Sons, Chichester, UK.
46. Taylor, P., Bain, P. (1999), "'An assembly line in the head': Work and employee relations in the call centre", Industrial Relations Journal, Vol. 30, No. 2, pp. 101-117.
47. Tyler, T. (2003), "Trust within organisations", Personnel Review, Vol. 32, No. 5, pp. 556-568.

About the authors

Cliona McParland is a Ph.D research student in the area of Management Information Systems at Dublin City University Business School, under the supervision of Prof. Regina Connolly. Her Ph.D is in the area of technology related privacy concerns with a particular emphasis on dataveillance behavioural outcomes in the computer-mediated work environment. Other areas of interest include information privacy, trust, ethics, empowerment and e-commerce risk and security management. The author can be contacted at **cliona.mcparland@dcu.ie.**

Regina Connolly, Prof., specialises in Information Systems at Dublin City University, Ireland. Her research focuses on digital service transformation, investigating the contemporary issues and challenges that government and organizations face in navigating an environment of accelerating technological change. She specifically focuses on how they can create new forms of value through redesigning their digital service offerings and re-visioning relationships. The author can be contacted at **regina.connolly@dcu.ie.**