Editorial:

Workplace surveillance

Luke Tredinnick and Claire Laybats

Surveillance has become a persistent concern of the digital age. Technology provides new ways of connecting people, but at the same time the digital traces of our lives perpetually haunt us. Twenty years ago Cairncross observed that 'Paradoxically, the electronic media make it easier for pornographers, hackers, and swindlers to hide behind anonymity while at the same time representing a serious threat to privacy' (1997: 191–2). Almost a decade later the Office of the Information Commissioner published a report on the state of the surveillance society in the UK that declared:

> "We live in a surveillance society. It is pointless to talk about surveillance society in the future tense. In all the rich countries of the world everyday life is suffused with surveillance encounters, not merely from dawn to dusk but 24/7" (Wood, 2006)

The intensity and scope of social surveillance has only grown since then. Governments, public authorities and corporations routinely monitor the behaviour of individuals, sweeping the most innocuous traces of online and offline interactions into vast databases on which the statistical analysis of big data techniques can operate.

Many forms of digital surveillance are by themselves arguably relatively innocuous, such as for example the targeted advertising which supports much of the digital economy. Some are arguably for the general public good, such a health or crime profiling. A few are genuinely concerning as they undermine the functioning of an open society, such as for example the 2013 revelations about the scale of government monitoring of digital traffic. But whatever the motivations, risks and arguments behind contemporary surveillance practices, any surveillance situation brings the problem of function creep – the use of data in originally unintended ways. Combined they represent an unprecedented degree of insight into and manipulation of the opinions and behaviour of everyone.

Although digital surveillance has been of significant concern for many years, the recent past has seen greater awareness of the scope and scale of the practice. In 2010 Facebook founder and CEO Mark Zuckerberg stated in an interview:

> "People have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people […] That social norm is just something that has evolved over time." (Johnson, 2010)

In April 2019 he unveiled a product roadmap for the new "privacy focused social platform" at the corporation's developer conference in San Jose (Wong, 2019). The difference in emphasis over that time reflects not just a gradual evolution of Facebooks relationship with its userbase, but rather a response to a series of challenges the company has confronted. Not least of these were the 2018 revelations about the use of personal data harvested from the service by Cambridge Analytica and the use of that data in various political campaigns. This scandal has been called a watershed moment for the understanding of the uses and abuses of personal data and in a European context the timing alongside the implementation of the General Data Protection Regulations (GDPR) provided serendipitous reinforcement. Privacy and surveillance have never been more topical.

But while Facebook may be emphasising different aspects of its business model to meet these challenges, it does not change the fact that fundamentally it both reflects and relied on a more open attitude to privacy and personal data that has emerged in the digital age. It is sometimes suggested that if you cannot tell what product an online company is selling, then *you* are the product. This idea apparently originally derives from the business model of commercial television in the 1970s but has now become a commonplace. However it is not so much that users have become the product, but rather that their personal data has become the driving currency of the digital economy. Every time we use a social network, search engine, or similar advertising driven services, we are exchanging personal data about our identity, our likes, our beliefs, our friendships, our political opinions, our health status, our preoccupations and concerns, our religious identity, and countless other aspects of ourselves for access to those digital services. The overwhelming reluctance for consumers to pay for access to digital services has led directly to personal information becoming the medium of exchange.

This is not in principle an unfair exchange, although it may not always be as transparent as we might like. The question is therefore perhaps not one of privacy per se but whether the consent to surveillance that we all routinely provide is truly informed. The General Data Protection Regulations (GDPR) have strengthened the protections over both uses of personal data and the transparency of consent, but nevertheless not all users at all times attend to the details of the consent they provide. Consent may be forthcoming, but that consent is often not based on a well-informed understanding of the uses to which personal data may be put, and the processing to which it may be subjected.

One area in which questions of informed consent becomes particularly poised is in the workplace; it is perhaps tenable to argue that use of Facebook, Twitter or Google is a choice made freely by the consumer but it is harder to argue that the decisions about where to work are quite so freely made. Workplace surveillance of digital communications has of course often been commonplace for decades. Traditionally this has tended to focus on those channels through which employees come into contact with the outside world; monitoring of email, internet and telephone use is almost universal in the commercial sector. Often such workplace monitoring is there to protect the organisation from the consequences of improper behaviour, or from the threat of subsequent legal action. And while many employees may not particularly like it, there is a general acceptance that monitoring of such channels is reasonable providing the privacy of the individual is broadly respected in a reciprocal fashion.

More recently there have been a growing number of accounts of organisations and companies that have taken workplace surveillance to a new level, actively monitoring many aspects of employees' behaviour and performance both inside and outside the workplace. In 2019 the BBC reported that over half of companies with over US$750m in revenues had used non-traditional techniques to monitor staff, including tracking keystrokes, monitoring email conversations, and even monitoring conversations between staff (Belton, 2019). New workplace surveillance has included monitoring social media accounts, and even tracking exercise and sleep patterns. Increasingly workplace surveillance is not only used to deter or detect inappropriate behaviour but to boost productivity by monitoring employee performance and wellbeing with a view to identifying and acting on issues before they become problematic.

In 2018 the TUC published a report revealing that over half of employees in the UK think it is likely they are being routinely monitored at work (TUC, 2018). Two-thirds of employees worry about the discriminatory use of workplace surveillance, and seventy percent think that surveillance will increase in the future (TUC, 2018). What is perhaps more worrying is the ways in which this perception of surveillance appears to divide of demographic grounds. Younger employees for example express more concern about workplace surveillance than older employees. This may reflect differential awareness; it may reflect differential surveillance according to seniority. It may also reflect different practices of surveillance by industry, and it in in this respect that workplace surveillance becomes charged with social and political issues.

The TUC report also demonstrates that concern amongst employees is far greater in relation to techniques that monitor the individual rather than their communications; fewer than 40% of employees found email or telephone monitoring unacceptable, whereas nearly 70% objected to key-logging, monitoring employee's location, using webcams to monitor employees at their workstation, and monitoring social media usage outside work hours. Of greatest concern was the use of facial recognition software (TUC, 2018).

As technology develops the ways in which organisations can routinely monitor the performance and activity of their staff are likely to increase over time. Likewise the number of companies offering data-driven technologies to evaluate employee performance and engagement are likely to grow. But although there is a general feeling that workplace surveillance is likely to intensify in the coming years (cite), that does not necessarily mean it must necessarily become more intrusive. It is clear that people tolerate surveillance of work performance, and of workplace communications, but are mistrustful of surveillance that begins to blur the line between the occupational and private spheres. More than any other factor, clear communicating both of the kinds of monitoring that take place, and the reasons for that monitoring, is fundamental to building and maintaining trust in the workplace.

June Business Information Review

The first article in June's *Business Information Review* was written by editorial board member Denise Carter and former editor Sandra Ward. Exploring the implications of the Hawley Report originally published in 1995 but recently reappraised for its potential contribution to commercial information management strategy, the article reports on the updating and development of Hawleys original recommendation for a modern information context. Entitled *Information as an Asset - Today's Board Agenda: The value of Rediscovering Gold,* the paper traces the ways in which the information landscape has been transformed over the last twenty years, from connectivity, to the growth of artificial intelligence (AI), and the redevelopment of the Hawley report for contemporary contexts. The authors write of that: "our report is intended to be transformational and a wakeup call. It provides our view of the benefits from managing information with flair, a set of principles that Boards would do well to adhere to; and a checklist to enable boards to consider the extent to which they are delivering and promoting the effective management and use of information assets". The publication of *Information as an Asset: Today's Board Agenda* by the Chartered Institute of Library and Information Professionals (CILIP) in February 2019 is an important landmark in commercial information management, as out first paper makes clear.

Our second article was written by Paul H Cleverley and Simon Burnett from Robert Gordon University in the United Kingdom and addressed the topical and important subject of enterprise search solutions. Entitled *Enterprise Search: A State of the Art,* the paper reports on interview research conducted with eighteen participants from a range of backgrounds into challenges for enterprise search and future directions for development. The paper develops a four-level model for enterprise search use cases that "could be used to reframe how enterprise search is perceived, influencing strategies, deployments and conceptual models".

The third article for June 2019 is entitled *The Innovation Ecosystem and Knowledge Management: A Practitioners viewpoint. What does Innovation Mean?* Witten by Rosemary Nunn from I&K, the Information and Knowledge Agency, the paper explores the meaning of innovation in organisational contexts, and the link between innovation and Knowledge Management. The paper explains how to map the innovation ecosystem within the organisation, and uses case studies to map the impact of knowledge management on innovation.

Our fourth paper was written by Paul Corney, founder of knowledge et al, a UK-based KM consultancy and a Knowledge & Information Management Ambassador for CILIP. The paper illustrates the importance careful planning plays in creating the right environment for face-to-face collaboration and learning, and outlines ten virtual facilitation success factors.

Our final article for June was written by editorial board member Denise Carter, from DCision Consult, Geneva, Switzerland. Entitled *Real World Experience: Lessons Learnt From My Experience of Bringing a Fully Outsourced Library Service Back In-house,* the paper reflects on the ways in which early professional experiences can have a important and continued effect on our working lives. We are very grateful for Denise in contributing this paper.

Bibliography

Belton, P (2019), How Does it Feel to be Watched at Work All the Time? *BBC News,* 12th April 2019, available at: https://www.bbc.co.uk/news/business-47879798 [accessed: 09th May 2019]

Cairncross, F. (1997), *The Death of Distance: How the Communcations Revolution will Change our Lives,* Boston, Mass.: Harvard Business School Press.

Johnson, B. (2010), Privacy No Longer a Social Norm says Facebook Founder, *The Guardian,* 11th Jan 2010, available at: https://www.theguardian.com/technology/2010/jan/11/facebook-privacy [accessed: 09th May 2019]

TUC (2018), *I'll Be Watching You: a Report on Workplace Monitoring,* Trades Union Congress, available at: https://www.tuc.org.uk/research-analysis/reports/i%E2%80%99ll-be-watching-you [accessed: 09th May 2019]

Wood, D. M. (2006), *A Report on the Surveillance Society,* Information Commissioners Office.

Wong, J. C. (2019), Facebook’s Zuckerberg Announces Privacy Overhaul, *the Guardian,* 30th April 2019, available at: https://www.theguardian.com/technology/2019/apr/30/facebook-f8-conference-privacy-mark-zuckerberg [accessed: 09th May 2019]