Journal of Business Analytics

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/tjba20

Balancing privacy rights and surveillance analytics: a decision process guide

Daniel J. Power, Ciara Heavin & Yvonne O'Connor

To cite this article: Daniel J. Power, Ciara Heavin & Yvonne O'Connor (2021) Balancing privacy rights and surveillance analytics: a decision process guide, Journal of Business Analytics, 4:2, 155-170, DOI: 10.1080/2573234X.2021.1920856

To link to this article: https://doi.org/10.1080/2573234X.2021.1920856

© 2021 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group.

Published online: 06 May 2021.

Submit your article to this journal

Article views: 6180

View related articles

View Crossmark data

Full Terms & Conditions of access and use can be found at
https://www.tandfonline.com/action/journalInformation?journalCode=tjba20

JOURNAL OF BUSINESS ANALYTICS
2021, VOL. 4, NO. 2, 155–170
https://doi.org/10.1080/2573234X.2021.1920856

THE OPERATIONAL RESEARCH SOCIETY
Taylor & Francis
Taylor & Francis Group

ORIGINAL ARTICLE

OPEN ACCESS Check for updates

Balancing privacy rights and surveillance analytics: a decision process guide

Daniel J. Power [a], Ciara Heavin [b] and Yvonne O'Connor [b]

[a]College of Business Administration, University of Northern Iowa, Cedar Falls, USA; [b]Business Information Systems, Cork University Business School, University College Cork, Cork, Ireland

ABSTRACT

The right to privacy has been discussed by scholars in multiple disciplines, yet privacy issues are increasing due to technological advances and lower costs for organisations to adopt smart surveillance. Given the potential for misuse, it seems prudent for stakeholders to critically evaluate Surveillance Analytics (SA) innovations. To assist in balancing the issues arising from SA adoption and the implications for privacy, we review key terms and ethical frameworks. Further, we prescribe a two-by-two Surveillance, Privacy, and Ethical Decision (SPED) Process Guide. SPED recommends the use of one or more of three ethical frameworks, Consequence, Duty, and Virtue. The vertical axis in the SPED matrix is the sophistication of an organisation's SA and the horizontal axis is an assessment of the current privacy level and the rights afforded to the target(s) of surveillance. The proposed decision process guide can assist senior managers and technologists in making decisions about adopting SA.

ARTICLE HISTORY
Received 11 July 2020
Accepted 14 April 2021

KEYWORDS
Ethical decision making; privacy; surveillance analytics; big data; artificial intelligence; decision process

1. Introduction

For many people, surveillance has a negative connotation. Surveillance is about control and power (Foucault, 1991; Marx, 2005b; Ragnedda, 2011; Vagle, 2016), but it is not inherently about coercion, discipline, covert spying, and loss of freedom. Surveillance poses a threat to privacy. In recent years, computer-based surveillance systems have been enhanced with powerful capabilities. For example, if we compare the state of the art in 2005 for video surveillance systems (Valera & Velastin, 2005) with current distributed, high-definition video monitoring hardware, and sophisticated software for facial recognition and real-time analytics (Garvie & Moy, 2019), we see how much has changed. Also, since 2000, the Internet and rapid diffusion of personal computing devices has created large volumes of structured and unstructured data that managers want analysed (Syed et al., 2013).

To meet the need to analyse opportunistic and intentional surveillance data, organisations have been hiring data scientists, business analysts, data engineers, marketing data analysts, and intelligence analysts (Power & Heavin, 2017). These data professionals are trained in various disciplines including Business Analytics and Data Analytics. Surveillance analytics (SA) involves both expert use of analytics tools including algorithms and statistics, and creation and deployment of embedded, "smart" surveillance through automated object detection methods leveraging high-complexity image/data processing technologies and algorithms (Hu & Ni, 2017).

Analytics and surveillance innovations are not always beneficial nor always harmful (Degli Esposti, 2014); hence, stakeholders, including key decision-makers such as senior managers, technologists, and data professionals must balance outcomes and make value judgements about adopting innovative analytics and surveillance. Making expanded use of business analytics (BA) with data about people and adopting SA innovations creates challenging ethical questions associated with privacy, data ownership, and accuracy (Moor, 2005).

People fear surveillance because of scenarios like George Orwell's (1949) "Big Brother" (Power, 2016) and articles on the Chinese surveillance state (Campbell, 2019). "Technology's complexity and its potential to impact society have generated a certain ambiguity towards, sometimes even a fear of technology" (Palm & Ove Hansson, 2006, p. 547). Zuboff (2015) metaphorically labels surveillance capitalism as "Big Other". Many organisations are using SA including non-profits like hospitals and universities, and more traditional firms in banking, financial services, and professional services. Privacy problems are growing because of technological advances and lower costs for organisations to adopt smart surveillance.

This article explores issues associated with Surveillance Analytics (SA) in multiple settings and it attempts to provide guidance for professionals, especially those in business and data analytics, who want to ensure that a proposed surveillance innovation such as analytics will not unnecessarily infringe on privacy

CONTACT Ciara Heavin c.heavin@ucc.ie Business Information Systems, Cork University Business School, University College Cork, Cork, Ireland

© 2021 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group.
This is an Open Access article distributed under the terms of the Creative Commons Attribution-NonCommercial-NoDerivatives License (http://creativecommons.org/licenses/by-nc-nd/4.0/), which permits non-commercial re-use, distribution, and reproduction in any medium, provided the original work is properly cited, and is not altered, transformed, or built upon in any way.

rights. The primary focus is on innovative surveillance adoption decisions in private sector organisations. This focus on private surveillance narrows the scope and complexity of the analysis to fewer types of settings with decision processes that are more understandable, and yet the number of specific decisions is likely much larger than in the public sector.

The next section defines and explores the key concepts of privacy rights, surveillance analytics, ethical decision-making, and balance (Section 2). We then frame both the need for and the challenge of balancing privacy rights in the context of surveillance analytics (Section 3). Section 4 examines some surveillance analytics innovations. Section 5 summarises our findings by proposing a prescriptive decision process guide. The SPED Process Guide recommends ethical frameworks for assessing surveillance analytics innovations and for evaluating the associated privacy implications. Section 6 discusses the agency problem and other associated issues. The concluding section draws some conclusions about next steps for both academics and practitioners.

2. Defining key concepts

Developing a decision guide to help those obligated to evaluate innovative surveillance analytics begins with defining and analysing key concepts and terms. This section defines the four concepts of balance, privacy and privacy rights, surveillance analytics, and ethical decision-making.

2.1. Balance and balancing

The goal of balancing the value of privacy rights that might be lost with any benefits from designing and deploying innovative surveillance capabilities implies a goal of finding a win-win resolution of conflicting outcomes. A balanced analysis examines what privacy rights must be diminished or reduced to balance the perceived benefits from adopting a specific surveillance analytics solution. Striving for balance means that there are no absolute privacy rights and that some innovations in surveillance create significant social good that cannot be ignored. According to Sableman (2014), "Privacy policy, however, is inherently about balance. Almost every aspect of modern civilization interferes with personal privacy to some extent". In 2020, it seems especially important for stakeholders to find a balance prior to implementing tools like video surveillance (Wolfe & SDMmag.com, 2020).

The balance metaphor does not imply that attaining the benefits from an innovation in surveillance analytics must lead to a decrease in privacy or a loss of privacy rights. Surveillance analytics is not in direct conflict with privacy rights. Cultural factors, trust, and prior privacy violations impact the perceived balance and perceptions of those individuals who are the targets of surveillance (Luppicini & So, 2016). Moosavian (2016) does caution us that the balance metaphor can lead to misuse of confidential information. He notes benefits from a security analytics innovation are only subjectively commensurable with any harm from privacy infringement or reduction.

2.2. Privacy and privacy rights

The two related concepts of privacy and privacy rights are variously defined and are difficult to measure. Privacy rights especially depend upon laws in the jurisdiction where surveillance occurs. A common dictionary definition of privacy is "freedom from unauthorized intrusion and the quality or state of being apart from company or observation" (Merriam Webster, 2020). The International Association of Privacy Professionals (IAPP, 2020) define privacy as "the right to be let alone, or freedom from interference or intrusion. Information privacy is the right to have some control over how your personal information is collected and used". Others suggest that privacy is one's ability to control information about oneself (Bélanger et al., 2002; Stone et al., 1983). Clarke (1999) states that "privacy is often thought of as a moral right or a legal right" (p. 60). Privacy of an individual is multi-faceted and includes (i) privacy of the person; (ii) privacy of personal behaviour; (iii) privacy of personal communication; (iv) privacy of personal data; (v) privacy of location and space; and (vi) privacy of thoughts and feelings (Borton et al., 2013; Lee et al., 2013). Privacy also refers to being able to keep certain acts and information, especially personal matters, to oneself and avoid public attention (Derlega & Chaikin, 1977).

Privacy rights refers to the concept that one's personal information is protected from public scrutiny (P. M. Schwartz, 1994). In a foundational article, Warren et al. (1890) reviewed the common law, the U.S. Constitution, and statutes related to a right to privacy. Then and now, privacy rights are not fixed, and they vary among jurisdictions. For example, the majority in Olmstead v. United States (1928) ruled that incriminating evidence obtained in wiretapping by government officials did not violate constitutional rights. In his dissent to Olmstead, Justice Brandeis noted "time works changes, brings into existence new conditions and purposes". Olmstead was overturned 40 years later in Katz and United States (n. d.). Katz held that warrants were in fact required to wiretap pay phones. Also, Katz established a new test of whether there is an expectation of privacy in a situation upon which one may justifiably rely.

The United Nations Declaration of Human Rights Article 12 states that "No one shall be subjected to arbitrary interference with his privacy, family, home

or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks". Some of the terms and phrases in Article 12 like "arbitrary interference" and "attacks upon his honour" are vague and subject to various interpretations.

2.3. Surveillance analytics

Surveillance analytics refers to the use of software algorithms to detect, classify, monitor, and track objects or persons in real-time or after an event (Zalud, 2013). Surveillance analytics is a process that uses analytics techniques and tools like statistics and machine learning to identify patterns in data collected about people. Surveillance systems monitor behaviour, activities, or other changing things to manage, direct, or protect people (Zuboff, 2015). Surveillance also involves intercepting private emails or phone calls, passive or active video camera data gathering and analysis, clicking behaviour on Facebook or YouTube, or monitoring web surfing.

Heibutzki (2018) defines surveillance narrowly as "the covert observation of people, places and vehicles, which law enforcement agencies and private detectives use to investigate allegations of illegal behaviour. These techniques range from physical observation to the electronic monitoring of conversations". Surveillance equipment includes various devices including audio recorders, digital cameras, GPS tracking devices, and real-time listening devices. Surveillance analytics applies business analytics (BA) methods and tools to data about people. BA is about the discovery of meaningful patterns in data (Delen & Ram, 2018). Also, as Power et al. (2018) explain BA "applies qualitative, quantitative, and statistical computational tools and methods to analyze data, gain insights, inform, and support decision-making (p. 51)".

New forms of social surveillance apply "scrutiny through the use of technical means to extract or create personal or group data, whether from individuals or contexts" (Marx, 2005a). Marx (2005a) cites new tools like "computer matching, profiling and data mining; work, computer and electronic location monitoring; DNA analysis; drug tests; brain scans for lie detection; various self-administered tests and thermal and other forms of imaging to reveal what is behind walls and enclosures".

Technologies such as knowledge mining and deduction, pattern recognition and cloud computing are widely utilised in the next generation of video surveillance systems (Xu et al., 2016). Surveillance creates "Big Data" and proposes a framework for how to process, organise, manage, and store massive video data (Xu et al., 2016). The term "Big Data" is widely used in both the academic and popular literature (Power & Heavin, 2017) and video surveillance data are the largest source of "Big Data" (Gandomi & Haider, 2015). According to Constantiou and Kallinikos (2015), much of what comes under the "Big Data" umbrella is not collected deliberately and purposefully. Typically, "Big Data" is diverse, randomly collected and, not infrequently, trivial, messy, and agnostic (Anderson, 2008).

Big data is one outcome of surveillance analytics, as the use of video and other technologies results in the generation of large volumes of diverse data. These data may be used to monitor and track peoples' behaviour as well as provide new opportunities to generate new data-based insights (Xu et al., 2016). However, Tene et al. (2013) state "We live in an age of 'big data' (p. 239)", but they note "the extraordinary benefits of Big Data are tempered by concerns over privacy and data protection" (p. 241).

2.4. Privacy calculus, privacy paradox, and communication privacy management

To explain individual reactions to surveillance, Culnan and Armstrong (1999) propose the "privacy calculus" theory which seeks to explain how individuals rationally balance the benefits and costs of disclosing personal data (i.e., cost-benefit trade-off). Since then, the concept of privacy calculus has been extended (cf. Dienlin & Metzger, 2016; Dinev et al., 2008; Plangger & Montecchi, 2020). One of the reasons for this is reflected in the fact that individuals disclose personal information even when they consider that the risks are high (commonly referred to as "privacy paradox" (Barnes & State University of New York at Buffalo, 2020; Taddicken, 2014)).

Privacy paradox in the era of surveillance analytics is well documented (Doty, 2020; Rowe, 2020). In their work, Mourey and Waldman (2020) provide insights in "which one's subjective importance of privacy itself varies as a function of who is in control of managing privacy and the extent to which managing privacy is perceived to be easy or difficult" (p. 162). Another reason for extending the privacy calculus theory can be explained by individuals who have rule-based boundaries that they use to determine whether to conceal or disclose information from others due to the ubiquitous nature of technology and the level of its use by others (commonly referred to as 'Communication Privacy Management – (Petronio, 2020)). As a result, it is important to explore the perceived sophistication of surveillance technologies (complexity) and the privacy level of control (certainty) over personal information when focusing on surveillance analytics as a single perspective will only provide limited results.

Surveillance systems are not inherently evil nor good, but they produce big data. However, due to

a lack of transparency around the design, development, and use of surveillance data, citizens have privacy concerns. Across various cultures, privacy is considered a basic human right (Hartman, 2001). As a result, infringing on individual's privacy unnecessarily is considered unethical (Hagen et al., 2018).

2.5. Ethical decision making

Ethical decision-making (EDM) is a process of evaluating and choosing among alternatives in a manner consistent with ethical principles and ethical frameworks (M. S. Schwartz, 2016). Ethical decision-making should be broader than applying lexical rules. In decision-making, lexical rules give one type of consideration absolute priority over another, e.g., privacy rights have an absolute priority and surveillance and surveillance analytics should never infringe or violate privacy rights, cf., Baron (1986).

EDM is about "choosing the right thing to do", it is rarely about clear-cut right and wrong decisions (M. S. Schwartz, 2016). In many situations, EDM is about choosing the "lesser of two evils" and finding a balance between principles and frameworks. Some technology decisions require a prioritisation among competing ethical values and principles. In most situations, there is a tendency to rationalise. Just because everyone is doing it or it is legal and permissible, does it mean that a new surveillance innovation is ethical? Ethics refers to applying "moral rules, codes, or principles which provide guidelines for right and truthful behavior in specific situations" (Lewis, 1985, p. 382).

Marx (1998) argued that before implementing surveillance innovations, we should evaluate the proposed methods by asking 29 questions to help determine the ethics of a proposed surveillance innovation. For example, Marx suggests we ask, "Is the personal information used for the reasons offered for its collection and for which consent may have been given and does the data stay with the original collector, or does it migrate elsewhere?" Data professionals cannot be expected to memorise these questions, but checklists, processes, and frameworks can be an established component of EDM.

Table 1 highlights the various EDM approaches (consequence, duty, and virtue) which have been reported in the surveillance analytics literature. This table emphasises the siloed approach to exploring EDM in surveillance analytics, with limited studies focusing on using multiple philosophical frameworks for ethical analyses.

The next section frames the privacy and surveillance balance problem under investigation as part of this article.

3. Framing the privacy and surveillance balance problem

Surveillance and analytics are transforming nation-states and organisations into less personal environments (Zuboff, 2015) with greater centralised control. In many countries and organisations, people are directly and indirectly impacted by surveillance. Some uses of surveillance technologies and associated analytics have had significant benefits including creating new products, for example, in healthcare (Raghupathi & Raghupathi, 2014) and providing evidence about crimes whereas other uses like storing web cookies and gathering or harvesting Facebook users' personal data have caused privacy concerns (Sewell & Barker, 2006).

The central problem addressed in this article is how to help decision-makers make balanced, ethical decisions about adopting a specific surveillance innovation. This frame helps us understand, define, and prioritise a complex, situational problem. The privacy-surveillance problem, as we have noted, is increasingly important and is often a decentralised decision made in organisations with broader societal implications (Zuboff, 2015).

Privacy and surveillance are not new topics. In 1986, Mason noted "Our society is truly an information society, our time an information age. The question before us now is whether the kind of society being created is the one, we want. It is a question that should especially concern those of us in the MIS community for we are in the forefront of creating this new society". In his article, he focused on four ethical issues that pose a threat to human dignity: 1) privacy, 2) accuracy, 3) property, and 4) accessibility (Mason, 1986). All four of these issues remain relevant.

This analysis focuses primarily on adoptions of innovative surveillance technologies by organisations rather than political entities. Many organisations collect data for marketing purposes or data about employees. The hospital setting might focus on patient and employee data. A school or university may collect data on multiple groups including students, faculty, staff, donors, and alumni.

As technology and analytical capabilities evolve, we revisit topics. For example, the debate over monitoring Internet use and the email of employees in the workplace is ongoing. Alge (2001) noted electronic workplace surveillance is raising concerns about privacy and fairness. In 2002, Zimmerman summarised the issues regarding privacy and monitoring. Little has changed in the debate other than arguing about new technologies, including the implementation of Video Monitoring Surveillance capabilities (SHRM, 2019).

At the time, Zimmerman and Workforce.com (2002) was sceptical of IT involvement in surveillance decision-making. She quoted an IT consultant who

Table 1. Overview of EDM in surveillance analytics studies.

EDM approach	Definition	Example of surveillance analytics studies
Consequence/ Deontology	Considers the potential effect of a decision into the future, it helps us to consider who might be affected and what the outcome of an action might be (Sinnott-Armstrong, 2019).	(McKee, 2013; Bonilla, 2014; Charles et al., 2015; Palayoor & Mavoothu, 2017)
Duty/ Utilitarianism	The Duty framework focuses on a set of rules or principles to guide ethical decision-making (Alston, 1988; Alexander & Moore, 2016)	(McKee, 2013; Andrejevic, 2019; Bilal et al., 2020)
Virtue	Virtue ethics is a broad term for theories that emphasise the role of character and virtue in moral philosophy rather than either doing one's duty or acting to bring about good consequences (Hursthouse, 1999).	(Van Der Sloot 2014; Holt et al., 2017; La Fors et al., 2019; Gal et al., 2020; Morley, Floridi et al., 2020; Wigan, 2020)
Hybrid	Focuses on deontology, utilitarianism, and value ethics.	(Custers & Ranchordas, 2019)

equated IT staff to law enforcement. Supposedly he said, "you have the cops making the laws, and that's not good". Zimmerman and Workforce.com (2002) also identified a reoccurring problem "that companies often make a snap decision about how they are going to use monitoring software". Today there seems to be an understanding that both HR and IT experts should be part of an ethical decision-making process about when and how to monitor employees. As Dobrin (2012) explains "Ethical problems are often complicated and require more than a formula to solve. The proper resolution of ethical problems requires judgment and good decision-making".

For many years, researchers have discussed the growing surveillance threat. For example, Boyd and Crawford (2012) asserted that "There is a deep government and industrial drive toward gathering and extracting maximal value from data, be it information that will lead to more targeted advertising, product design, traffic planning, or criminal policing (p. 675)". The "Big Brother" metaphor mentioned in the introduction focuses our attention on data collection by government institutions in general and at all levels. Zuboff's (2015) "Big Other" metaphor expanded the threat to privacy from surveillance to larger corporations and other institutions. She asserts that any organisation that has sufficient resources to own and operate surveillance tools and maintain extensive data collections may invade privacy boundaries (Zuboff, 2015).

According to Richards and Harv. L. Rev (2013), some possible harms from surveillance associated with diminished privacy rights include: 1) reduced intellectual privacy, for example, a chilling effect on discussing union organising, criticising management, or an inclination to conformity, 2) surveillance poses harm by altering the power dynamic between the watcher (the boss) and the watched (the worker or customer), and 3) surveillance may lead to blackmail and other corrupt behaviours. Richards and Harv. L. Rev (2013) further notes if "we are watched while engaging in intellectual activities, broadly defined – thinking, reading, web surfing, or private communication – we are deterred from engaging in thoughts or deeds that others might find deviant. Surveillance thus menaces our society's foundational commitments to intellectual diversity and eccentric individuality".

Surveillance capabilities continue to expand with technological developments. Data professionals, including business analytics practitioners and data scientists are not trained as moral philosophers nor as lawyers and yet these experts increasingly need to make ethical decisions about new surveillance opportunities.

Some sources prescribe using Privacy by Design (Cavoukian, 2011; Hustinx, 2010) to protect privacy rights. Privacy by Design (PbD) is a system engineering approach initially intended for three application domains: 1) IT systems; 2) accountable business practices; and 3) physical design and networked infrastructure. PbD ideas can also be applied to business analytics and surveillance analytics. Ethical decision-making deliberations also help balance competing claims and concerns.

4. Surveillance analytics innovations

In a specific surveillance implementation, multiple analytics tools can be used to develop a system. For example, machine learning algorithms can be used for classification and prediction innovations like predicting feelings from facial recognition, cheating during test taking, and shoplifting (Gates, 2011). Real-time monitoring of millions of video and voice feeds is impossible without AI (Artificial Intelligence) technologies, especially Machine Learning. Cognitive computing, a term used by IBM to describe the current wave of AI, means software could even interact with people being monitored (Sommer, 2017). Both video and voice data could be archived, edited, and reviewed. Imagine organisations using Video Surveillance with facial recognition to monitor and track the actions of workers. Also, Video Surveillance has been widely used in schools to prevent bullying, deter vandalism, monitor visitors, and maintain a record of evidence in the event of a crime. Imagine new capabilities with alerts to school officials. One vendor advertises "Our HD Wi-Fi Nanny Camera Teddy Bear is the cuddliest guy around". California, USA, is one of the few jurisdictions that requires the

consent of all parties to a recorded conversation or video.

A broader, more ambiguous change that may threaten privacy involves the convergence of information and communication technologies. Surveillance analytics can exploit these advances by incorporating data sources from devices such as phones, video cameras, computer log files, specialised Internet of Things devices, and remote data capture devices (Zalud, 2013). Surveillance analytics algorithms and technologies leverage multiple data sources to provide descriptive, diagnostic, predictive, and prescriptive information. For example, Google provides cloud-computing services that include image identification, voice recognition, and machine learning technology.

Biometric technology like facial recognition systems can identify individuals without their knowledge. According to Sumner (2016), in "November 2013 supermarket giant Tesco announced that it would be installing screens positioned by payment tills which scan its customers faces, then display targeted advertising to them". One example of an innovative surveillance system is metaphorically called "Big Proctor". Flaherty's (2020) article in Inside Higher Ed has received many comments. She explains "Online proctoring has surged during the coronavirus pandemic, and so too have concerns about the practice, in which students take exams under the watchful eyes (human or automated) of third-party programs" (Flaherty, 2020). She notes "Chief among faculty and student concerns are student privacy and increasing test anxiety via a sense of being surveilled" (Flaherty, 2020). According to an April 2020, Educause poll, 54% of institutions were using online or remote proctoring services, while another 23% were considering or planning to use them. Even so, over half of the institutions polled said they were concerned about cost, as well as student privacy. From a student or teacher perspective, ask yourself how you would assess an innovation like this with monitoring of head movements as an indicator of cheating. What data would you use to train a machine learning algorithm? Should you tell students about the algorithm? If the algorithm indicated a student cheated on a test, what would you do?

Rapidly improving technologies and remote distributed data gathering coupled with decision automation alters what is possible and what is expected by managers. With the continued changes in the application of analytics to big data involving new and more data sources and more sophisticated analytics techniques, some long-standing beliefs about fair data/information practices and provisions of existing law and guidance raise significant challenges for organisations that want to apply analytics to big data (Center for Policy Leadership, 2013).

The United Nations Office of the High Commissioner for Human Rights (2020) website notes that "data-intensive technologies, such as artificial intelligence applications, contribute to creating a digital environment in which both States and business enterprises are increasingly able to track, analyse, predict, and even manipulate people's behaviour to an unprecedented degree. These technological developments carry significant risks for human dignity, autonomy and privacy and the exercise of human rights in general, if applied without effective safeguards".

In many political jurisdictions, people expect that surveillance data, especially any personal and behavioural information will be protected. In these jurisdictions, it is accepted that this information belongs to the person and does not belong to an organisation, the public, or government. Managers and stakeholders need to ensure that data that is collected and used does not infringe on the expected privacy rights of individuals (Power & Heavin, 2018). Regrettably, the exact extent of privacy rights for employees, customers, and other data providers is not always clearly defined.

Society is at an inflection point, and perhaps a turning point regarding the ethical use of surveillance analytics using advanced technologies. Identifying an ethical innovation in data collection and/or analytics applied to surveillance data requires answering a difficult and complex question.

5. A prescriptive decision guide

Adoption, appropriate use, and assessment of surveillance-related innovations should be made in the context of prevailing ethical standards (Breidbach & Maglio, 2020; McParland & Connolly, 2020). Surveillance and privacy perceptions provide a context for ethical decision-making about surveillance innovations (Darmody & Zwick, 2020). To assist in assessing and balancing surveillance data gathering and analysis proposals, we propose a two-by-two Surveillance, Privacy and Ethical Decision-Making (SPED) Process Guide that prescribes the most appropriate ethical decision-making process(s) given the decision context. According to Gregor (2006 p. 620), a prescriptive approach specifies "how people can accomplish something in practice (e.g., construct an artifact or develop a strategy)".

Using M. S. Schwartz's (2016) characterisation of types of EDM models, SPED is more interactional, i.e., person-situation focused, in nature. As a prescriptive framework, SPED "allows for the establishment of grounds (i.e., reasons) for imputation of a person with regard to her actions, of responsibility with regard to others, and of recognition with regard to unknown others" (Reijers & Coeckelbergh, 2020, p188). We argue that a single code of technology ethics cannot fit all contexts and situations.

The SPED framework draws upon principal-agent theory (Eisenhardt, 1989), also known as the agency dilemma, to provide an understanding of the forces that need to be examined in terms of balancing the privacy rights of individuals and the use of innovative surveillance innovations. Senior managers are the principals and employees or customers are agents. In a surveillance or monitoring situation, the principal, e.g., employer, assumes the role of the watcher and takes actions to protect the interests of various agents, e.g., employees who are watched. The implicit contract is often about creating a safe workplace for employees or providing customers with a good experience and value while maintaining their privacy rights. Agents may be concerned that the principal is acting from self-interest rather than their interest when implementing surveillance systems and using a data-driven approach in the form of surveillance analytics to predict behaviours.

The SPED framework (see Figure 1) can be viewed as a situation-specific extension of the macro-level contingency theory (Lawrence & Lorsch, 1967) to the micro-decision-making level. The two dimensions are framed specifically for privacy and surveillance analytics adoption decisions.

Taking Galbraith's (1974) information processing theory to the decision situation level, our guide prescribes that as uncertainty increases, the principal requires an increasing amount of information to make an ethical decision about the proposed surveillance analytics innovation. Duncan's (1972) complexity-dynamism hypothesis supports providing more information to the principal as complexity increases. In all four situations, one or more principal stakeholders act on behalf of a group of agents, e.g., employees or customers, who expect the principal to act in their best interests. SPED may shine a new light on the dilemmas, challenges, and information needs facing management decision-makers, data scientists, data and IT professionals, and government and organisation policy-makers.

The vertical axis in the SPED framework is a measure of the perceived sophistication of currently implemented surveillance analytics and technology. An organisation's level of sophistication in the use and management of IT is a multidimensional construct with four components: 1) technology use and utilisation, 2) applications portfolio, 3) centrality of the IS function, and 4) managerial governance and control of IT (cf., Cheney and Dickson 1982); Raymond and Pare 1992).

Technology sophistication reflects the extent of diverse and complex IT elements employed within society (adapted from Coetzee, 2017) ranging from low to high on a continuum of sophistication. Low technology sophistication reflects simpler and generic technological elements. Therefore, decisions about the adoption of surveillance innovations in low technology sophistication situations can be informed by simple lexical rules and the application of the virtue ethical decision-making framework. In a high surveillance technology sophistication, situation with surveillance analytics in an organisation and/or country of operation stakeholders should make use of multiple ethical decision-making frameworks. Several types of ethical theory exist and using only one may not be sufficient to address ethical implications (Broad, 2014).

The horizontal axis in the decision guide is a measure of privacy levels and existing privacy rights of individuals in a country and a specific organisation. Privacy level is a measure of how much perceived control an individual has over how personal information is collected and used (Smith et al., 1996). Since 1997, Privacy International[1] has calculated an Internet Privacy index for countries. The index is calculated based on mean scores on 14 criteria, including Constitutional protection, Visual surveillance, Communication interception, and Workplace

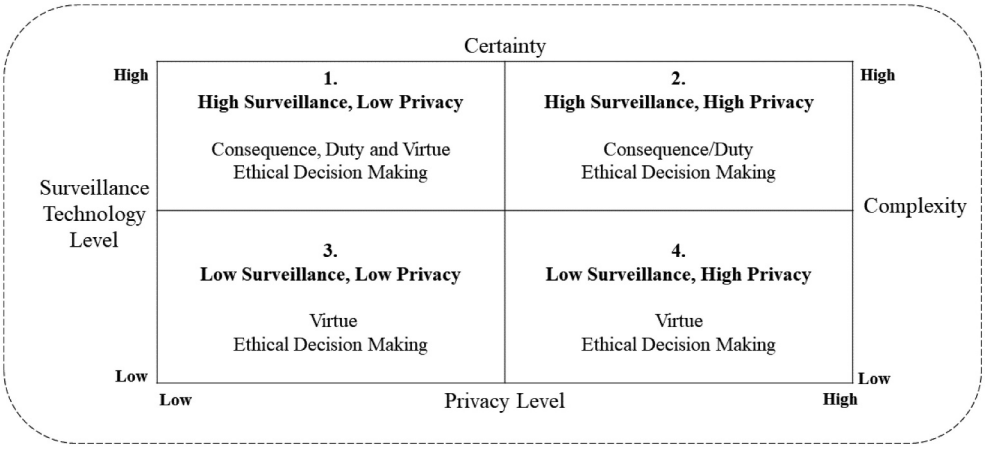

Figure 1. Surveillance, Privacy, and Ethical Decision-Making (SPED) Framework.

monitoring. When sophisticated surveillance already exists in a country or organisation, adopting more advanced surveillance analytics to process data creates a need for a more rigorous process for balancing the trade-offs of reduced privacy and additional benefits from surveillance (Anhalt-Depies et al., 2019; Pal et al., 2020).

Under conditions of low privacy, people have limited opportunities to identify which data, structured or unstructured, can be accessed, processed, and stored about them and thus, individuals are more vulnerable to unauthorised intrusion from surveillance. The opposite occurs in the high privacy situation as proposed by Tarkkanen and Harkke (2016) when investigating privacy concerns in designing social network sites.

In Figure 1, the concepts of surveillance sophistication and privacy level are identified as independent constructs, although the constructs are likely correlated with an inverse relationship where the lower the privacy level, the higher the surveillance sophistication. The relationship is most likely moderated by resource constraints and the availability of expertise due to the inequalities in digital proficiency experienced globally (Pearce & Rice, 2017). Also, small, and medium-sized organisations are much less likely to have sophisticated surveillance analytical systems. The constructs are represented as having only a high and a low value when the constructs are continuous variables, and the surveillance dimension is changing rapidly due to technological advances.

Both a current and ongoing assessment of surveillance technology sophistication and context factors are important in recommending an appropriate EDM decision process, as Morley et al. (2020) argue "what was ethically justifiable in one place yesterday might not be so tomorrow".

There are ethical implications for increasing surveillance of people in public places, but McParland and Connolly (2020) argue that there may be even more issues when introduced in a workplace or within a person's private domain. Hence, evaluating surveillance innovations is dependent upon context. There are three major components of the context that must be considered: 1) *Place* – where will the proposed surveillance occur? 2) *Purpose* – What is the purpose of the proposed surveillance? Perhaps a broad purpose like control or a more specific purpose like detecting changes in disease occurrence? and 3) *Expectations of Privacy Rights* – surveillance in one place may be ethical, but the same innovation may not be ethical in another place (Morley, Floridi et al., 2020). Likewise, surveillance for one purpose may be ethical but unethical for another (Koskela, 2006). Finally, in one political jurisdiction, privacy laws may permit or allow a specific type of surveillance, but the same surveillance may violate privacy rights in another jurisdiction (Gstrein, 2020).

Building from Table 1, the SPED framework contingently prescribes three normative approaches to ethical decision-making including *Consequence*, Teleological moral systems (Sinnott-Armstrong, 2019), *Duty*, Deontological moral systems (Alexander & Moore, 2016; Alston, 1988), and *Virtue*, Virtue-based ethical theories (Hursthouse, 1999) perspectives.

In the Consequence or Consequentialist framework, a stakeholder focuses on the future effects of the possible courses of action, considering the people who will be directly or indirectly affected. A decision-maker should ask what outcomes are desirable in each situation and consider ethical conduct to be whatever will achieve the best consequences (Howard-Snyder, 1996). A person using the Consequence framework desires to produce the greatest good (Driver, 2011). From this perspective, it is the consequences that make actions, good or bad, right, or wrong. The deliberative process should focus on outcomes and the likelihood they will be realised (Sinnott-Armstrong, 2019). The EDM process directs attention to the future effects of an action, for all people who will be directly or indirectly affected by the action. Ethical conduct is taking the action that will achieve the best consequences.

Alston (1988) argues that the *Duty* perspective is one which follows rules or duty regardless of outcome. This approach harnesses obligations or duties of individuals and organisation to "do the right thing". In the Duty framework, a stakeholder focuses on the duties and obligations the principal has in each situation and considers what ethical obligations exist and what one should never do (Larry & Moore, 2007). Ethical conduct is defined by doing one's duties and doing the right thing, and the goal is performing the correct action. The deliberative process involves defining obligations in the situation, and what a decision-maker should never do (Lazar, 2017).

The *Virtue* framework relies on "virtuous traits" to guide ethical decision-making. This approach relies on human traits and behaviours as a way of discerning what is ethical. Virtue ethics states that practising good habits such as honesty and generosity makes a moral and virtuous person (Crossan et al., 2013). It guides a person without specific rules for resolving the ethical complexity. Crossan et al. (2013) argues that the inclusion of a virtue ethical perspective into existing EDM frameworks is imperative for decision-making models. More recently, Drašček et al. (2020) argue that virtue ethics is not considered in research on ethical decision-making. Luppicini and So (2016) argue that ethical practices vary among individuals and communities. Hence, May (2013) purports that virtue ethics represents a middle ground between duty

and consequence ethics. Applying the virtue framework means a decision-maker focuses upon what a choice and my actions will show about my character. Ethical conduct is defined as what a virtuous (good) person would do in the circumstances.

Let us briefly examine the four quadrants in the SPED Framework in more detail:

Quadrant 1: Situations with high surveillance and analytics sophistication and with low levels of individual privacy create multiple ethical issues. To legitimise new surveillance projects proposed in Quadrant 1 situations, policy-makers, developers, and adopters of surveillance analytics tools and technologies and purchasers of surveillance-related data should use all three normative approaches to ethical decision-making, *Consequence, Duty*, and *Virtue*. Using these three perspectives together provides a more comprehensive and holistic view of the legitimacy issues associated with a surveillance proposal.

The three frameworks/perspectives are not mutually exclusive. The nature of ethics and ethical decision-making is so complex that these frameworks together may enable achieving a positive outcome.

Each of the three ethical decision-making approaches in this quadrant have potential weaknesses. From a *Consequence* perspective, successfully predicting outcomes is difficult to achieve, particularly when unexpected variables arise. There are also limitations associated with the *Duty* perspective, treating everyone the same may be ethical in principle but may result in a negative outcome for some individuals. Furthermore, with the *Virtue* perspective, it is difficult to define and agree upon what constitutes the term virtue and how it manifests in human behaviour as there are different virtue traits.

Quadrant 1 represents decision situations that currently have high surveillance and analytics sophistication and with low levels of individual privacy. In this situation, there is high complexity and low certainty so more information is easy to obtain.

Quadrant 2: Another scenario occurs when surveillance analytics tools and technologies have the capacity to capture a large volume of high velocity, and high variety structured and unstructured data about a specific person, but they have the option of identifying what data can be accessed, processed, and stored. The ethical decision-making process underpinning Quadrant 2 builds on Quadrant 1 but extends the decision-making scope to engage more individuals in the process and directs attention to the future effects of an action and to our duties. The legitimacy of surveillance is based on motivation to produce the best outcomes and to perform the right action. This decision-making approach, however, would be difficult to operationalise in real-time and is further complicated by the absence of approaches for identifying aberrant behaviour by adopters of surveillance analytics.

Quadrant 2 represents decision situations that currently have high surveillance and analytics sophistication with high levels of individual privacy. There is high complexity and high certainty, so more information is desirable.

Quadrant 3: Low amounts of surveillance and rudimentary surveillance analytics with low levels (limited) of individual privacy rights are perhaps the focus for the evolution of a "Big Brother" society. This quadrant attempts to discern character traits motivating people in the situation (i.e., Focus of Virtue Ethical Decision Perspective). Here, policy-makers, developers, and adopters of surveillance technologies and purchasers of surveillance-related data identify and examine a person's initial impressions surrounding the capture, use and storage of personal data vis-à-vis surveillance technologies.

Quadrant 3 represents decision situations that currently have low surveillance and analytics sophistication and low levels (limited) of individual privacy rights. In this quadrant, there is low complexity and low certainty.

Quadrant 4: Surveillance technologies are limited in terms of data collection abilities and yet people have opportunities to identify what personal data can be accessed, analysed, and stored about them and thus people have a lower threat of unauthorised intrusion. This quadrant in the SPED Framework has the fewest ethical concerns because each person is in control of identifying and monitoring the capture, analytical processing, and storage of their personal data. Here the sole ethical responsibility is placed upon the individual (Virtue Ethical Decision-Making). As such, people will be faced with answering questions such as "What will my actions show about my character?" and/or "What would a virtuous person do in the circumstances?" Where people have high privacy rights, policymakers, and developers of surveillance technologies should provide an approach or system that enables a person to take control of their personal data and to determine how it is captured, processed, and stored.

Quadrant 4 represents decision situations that currently have low surveillance and analytics sophistication and high levels (limited) of individual privacy rights so people have a lower threat of unauthorised intrusion. Here, there is low complexity and high certainty.

Surveillance and analytics sophistication are positively associated with complexity. Privacy level is positively associated with the certainty of an individual about their privacy rights.

In a classic review article of ethical decision-making research, Ford and Richardson (1994) examined variables associated with the individual decision-maker and variables which form and define the situation in which the individual makes

decisions. They found some evidence of differences in behaviour based upon job responsibilities, but they concluded that "Industry ethical standards were not related to an individual's ethical beliefs and decision-making behavior". Prior research identified two situational factors, a positive organisational ethical climate, and the existence of corporate codes of conduct that positively increase an individual's ethical beliefs and decision behaviour. They did note the type of ethical decision did influence decision-making behaviour. O'Fallon and Butterfield (2005) and Craft (2013) reported similar findings.

6. Discussion and reflections

Leveraging the premise of several theories, we propose the prescriptive Surveillance, Privacy, and Ethical Decision-Making (SPED) Process Guide to better support senior managers' understanding of the forces that need to be examined to achieve "balance" when considering the privacy rights of individuals and the implementation and use of innovative surveillance systems. Technological advances have increased the possibilities for more sophisticated surveillance which can impact privacy, raising significant ethical questions. Our proposed framework acts to guide decision processes with the overarching goal of protecting the privacy rights of citizens. As a result, five recommendations are proposed to support people to develop a strategy which focuses on balancing Privacy Rights and Surveillance Analytics:

Recommendation 1 (based on ***Q1*** *SPED Framework*): As this quadrant reflects high levels of complexity (high surveillance) and low certainty (low privacy), individuals will feel a loss of autonomy. *Decision-makers should consider a range of ethical viewpoints to ensure that what, why, when, and how data is collected*. Decision makers must consider the potential effect of a decision into the future, ensuring rules are adhered to but equally, to understand and appreciate rights and wrongs based on the consequences of these rules which are underpinned by reason and truth. Decision makers must build a reputation for consistently acting out their virtues over time. Herschel and Miori (2017 p. 31) argue that a multiple philosophical ethical approach "affords insight into the context and the logic of the moral arguments being presented, thereby providing us with a rational mechanism by which to better evaluate whether an intended action or actual outcome is morally right or wrong".

In doing so, this will provide insights for individuals to make more informed decisions about revealing and concealing private information (i.e., Communication Privacy Management). This theory states that individuals have rule-based boundaries that they use to determine whether to conceal or disclose information from others (Petronio, 2020).

In many ways, people, and especially information technologists and researchers, are caught in a paradoxical situation. Big Data and surveillance analytics algorithms and technologies have many positives for individuals, organisations, and society. For example, surveillance analytics are being used to understand individual citizen behaviour particularly in terms of compliance with "Stay at Home" guidelines and to track contacts in the event of a positive COVID-19 diagnosis. These technologies are being leveraged for the "greater good" of society, this strategy may be placed in Quadrant 1 of the SPED Framework where surveillance and analytics sophistication is high, and privacy rights are low resulting in serious ethical dilemmas.

Recommendation 2 (based on ***Q2*** *SPED Framework*): As this quadrant reflects high levels of complexity (high surveillance) but high certainty (high privacy), the cost-benefit trade-off of disclosing personal data (Privacy calculus) will be observed by more individuals. To maximise this, *decision-makers should embed a set of rules or principles which give full autonomy to individuals in managing how data is accessed, processed, and stored about them*. Any future changes in the way surveillance analytics are employed by decision-makers should consider who might be affected and what the outcome of an action might be. Such an approach can be achieved through citizen-engagement activities and providing individuals with a dynamic informed consent process which enables them to opt in or out of certain surveillance data acquisition, use, and analysis. In this scenario, principal-agent theory may come into play where incentives or rewards are used to motivate the agent to provide consent. Arthur and Owen (2019) present an example of this in financial services where customers can choose to opt into a scheme and consent to allowing their personal transaction data to be used in exchange for rewards provided under a merchant-funded rewards programme.

Surveillance analytics and privacy rights are local and organisational as well as personal and societal issues. The dynamics differ in each setting, but the ethical issues and the possibilities are similar. Ethical and responsible use of algorithms and surveillance data can have benefits (Stahl & Wright, 2018). With an increase in new types of data analysis techniques, there is a concern about a growing indifference to the specifics of persons, places, and events (Amoore, 2011, p. 30). Context matters in assessing the surveillance data so the place, time of day, and weather conditions where the data is originating among many factors must be considered in processing data, especially streaming data. This reality reinforces the need to ensure that surveillance technologies are developed,

managed, and evaluated in a fair, transparent, explainable, and intentional manner (European Parliamentary Research Service, 2020).

Recommendation 3 (based on ***Q3*** *SPED Framework*): This quadrant reflects low levels of complexity (low surveillance) and low certainty (low privacy). Since surveillance analytics is not human and privacy is commonly seen as an instrumental value in relation to personal autonomy, *decision-makers who employ surveillance analytics should reflect upon their actions and assess if they are adhering to or ignoring the rights of others by their actions*. One of the most important things to do at the beginning of an ethical deliberation is to identify ethical aspects of the proposed innovation and determine who may be affected by those making decisions. Van Der Sloot (2014) argue that the virtue ethics embraced by decision-makers will enhance the background, value, and scope of the right to individual privacy, which he argues is "not only of theoretical importance; it has practical significance for privacy protection in the age of Big Data".

In a human surveillance system, in the past managers watched employee and customer behaviours and drew conclusions based upon limited data and in many cases anecdotal experiences. Managers now can get better data and have experts and algorithms analyse the data for patterns and correlations. Decision-making can be informed and potentially more systematic. Managers and other data and privacy experts in an organisation must find the appropriate balance between the benefits of proposed surveillance innovations and the surveillance target's expectations for privacy. For example, emails sent or received through an organisation email account are generally not private. Once a valid business purpose exists for the surveillance, employers are free to monitor and capture these communications using a proxy server. If the communications are analysed, the data analyst should assess the need to protect the identities of sender and receiver(s). An algorithm automatically assures anonymity and de-identification during analysis. A policy of de-identification can increase trust with those who provide personal information. Such a policy stated in the Terms of Service might be appropriate for data associated with store affinity cards, buyer rebate software, and discount or bank cards. Garfinkel and Department of Commerce, NISTIR 8053 (2015) asserts "De-identification can reduce the privacy risk associated with collecting, processing, archiving, distributing, or publishing information. De-identification thus attempts to balance the contradictory goals of using and sharing personal information while protecting privacy, p. iii".

Recommendation based on ***Q4*** *SPED Framework*: As this quadrant reflects low levels of complexity (low surveillance) and high certainty (high privacy), *the decision-maker should always place the privacy control in the hands of the individual being monitored*. The aim is to find a balance between monitoring and trust by building trust around the use of emerging technologies such as surveillance analytics (Bilal et al., 2020). It is argued that virtue ethics could be one solution to the privacy paradox (Bilal et al., 2020).

However, in this scenario, principal-agent problems may arise when information asymmetry exists. In the context of the pandemic where working from home or remote working has become essential, employers have had less oversight of employees' daily activities. Some organisations have adopted a virtue lens for monitoring employee productivity with minimal surveillance. Holt et al. (2017) outlines an alternative approach with organisations using monitoring systems to improve performance measurement, increase productivity, and reduce costs. In his Guardian article, Walker (2021) outlines how one organisation plans to address information asymmetry with the implementation of home webcams connected to AI-based scanning systems to monitor the activity of 380,000 call centre staff working from home across 34 countries. The organisation has since refuted this claim stating that they trust their employees and that the innovative technology is being implemented to promote employee collaboration and to monitor customer data security. Trade unions and the UK government have communicated their concerns about the implementation of these surveillance technologies in the home.

Holt et al. (2017) purport that the ethical implications of monitoring have been largely ignored as well as the impact on employees' morale and their views of the organisation. There is an opportunity to place emphasis on virtues, or moral character, rather than duties, rules, or the consequences of actions (Bilal et al., 2020).

Recommendation 5 (Entire SPED Framework): Decision makers should be proactive in supporting the development and implementation of regulations that govern the use of analytics and AI in society, organisations, homes, and in devices. Using AI is a large scale "real world" experiment. We, as scientists, have an obligation to ensure that people are not harmed by algorithms and AI. All of us are becoming subjects in uncontrolled surveillance analytics experiments (Anderson & Rainie, 2018).

Some nations are moving, perhaps unknowingly, closer to the "Big Brother" society described by Orwell. Also, large multinational organisations often determine the balance of data control and economic power (Nemitz, 2018). On the one hand, individuals, national public health systems, and governments prioritise heath and access to the right healthcare above everything else. On the other hand, some privacy experts are beginning to flag the need for

governments to implement appropriate data privacy and security measures now, advocating for "Responsible Surveillance" (Minevich, M. & Beridze, I., 2020).

7. Conclusions

This article explores issues associated with surveillance in diverse settings and it attempts to provide guidance for professionals in multiple disciplines, especially business and data analytics, who want to ensure that a proposed surveillance innovation such as analytics will not unnecessarily infringe on privacy rights. This article contributes to both theory and practice.

In terms of practical contributions, we propose a prescriptive two-by-two Surveillance, Privacy, and Ethical Decision-Making (SPED) Process Guide that can be used to guide the decision process in assessing ethical dilemmas arising from the use of surveillance analytics and their implications for privacy. The vertical axis in the SPED framework is a measure of the perceived sophistication of currently implemented surveillance analytics and technology. The horizontal axis is a measure of privacy levels and existing privacy rights of individuals in a country and a specific organisation. Stakeholders must want to make ethical decision for the framework to have value. Surveillance analytics and privacy rights seem to come into focus when new use cases or technologies become "visible" and highlight a potential problem.

It is problematic to justify actions as ethical simply because the data are accessible (Boyd & Crawford, 2012, p. 672). Business and data analysts and data scientists should critically review proposed uses of surveillance analytics for behavioural prediction. These specialist IT professionals should be the first line of defence in maintaining privacy rights that might be lost to surveillance innovation. Organisations should conduct ethics training for their IT professionals and have ethics committees in place to review the use of analytics with biometric data (cf., Forbes Insights, 2018).

From a theoretical perspective, we argue that a single code of technology ethics cannot fit all contexts and situations, leveraging a range of existing ethics and IS theories we present in the SPED Process Guide. This framework offers a theoretical lens for researchers to explore privacy rights through Consequence, Duty, and Virtue ethics against a landscape of increasingly sophisticated surveillance analytics. Future studies should include empirical research to evaluate the SPED framework and the proposed recommendations. Future research could consider how to leverage the SPED framework, 1) as a tool to support decision makers in their adoption and use of smart surveillance systems, and 2) as a tool to explore existing situations where surveillance technologies and big datasets have raised ethical concerns.

In her work on Big Other and Surveillance Capitalism, Zuboff (2015) calls scholars and citizens to action "The trajectory of this narrative depends in no small measure on the scholars drawn to this frontier project and the citizens who act in the knowledge that deception-induced ignorance is no social contract, and freedom from uncertainty is no freedom (p86)". Building on this, we assert that there is a real need to offer theoretical and practical guidance to academics and decision makers to enable and support the balancing of surveillance and privacy rights. This may prompt organisations to invest in and promote awareness of new training opportunities, guidelines, and policies to promote greater "balance". The SPED Process Guide for decision-making is likely to apply in a variety of settings and levels (i.e., individual, organisational, governmental, and societal) where balancing the value of privacy rights and the use of innovative surveillance capabilities should be examined prior to the design and deployment of these solutions.

Note

1. https://privacyinternational.org

Acknowledgement

This article is dedicated to the memory of Prof. Daniel J. Power.

Disclosure statement

No potential conflict of interest was reported by the authors.

ORCID

Daniel J. Power http://orcid.org/0000-0001-8226-8737
Ciara Heavin http://orcid.org/0000-0001-8237-3350
Yvonne O'Connor http://orcid.org/0000-0002-3745-0342

References

Alexander, L., & Moore, M. (2016). Deontological ethics. In E. N. Zalta (Ed.), *The Stanford encyclopedia of philosophy* https://plato.stanford.edu/archives/win2016/entries/ethics-deontological/

Alge, B. J. (2001). Effects of computer surveillance on perceptions of privacy and procedural justice. *Journal of Applied Psychology*, *86*(4), 797–804. https://doi.org/10.1037/0021-9010.86.4.797

Alston, W. (1988). The Deontological Conception of Epistemic Justification. *Philosophical Perspectives*, *2*, 257–299. https://doi.org/10.2307/2214077

Amoore, L. (2011). Data derivatives: On the emergence of a security risk calculus for our times. theory. *Theory*,

Culture & Society, *28*(6), 24–43. https://doi.org/10.1177/0263276411417430

Anderson, C. (2008). The end of theory: The data deluge makes the scientific method obsolete. Wired Magazine. July, http://www.wired.com/science/discoveries/magazine/16-07/pb_theory

Anderson, J., & Rainie, L. (2018). The future of Well-Being in a Tech-Saturated world. Pew Research Center. April, https://www.pewresearch.org/internet/2018/04/17/the-future-of-well-being-in-a-tech-saturated-world

Andrejevic, M. (2019). Automating surveillance. *Surveillance & Society*, *17*(1/2), 7–13. https://doi.org/10.24908/ss.v17i1/2.12930

Anhalt-Depies, C., Stenglein, J. L., Zuckerberg, B., Townsend, P. A., & Rissman, A. R. (2019). Tradeoffs and tools for data quality, privacy, transparency, and trust in citizen science. *Biological Conservation*, *238*, 108195. https://doi.org/10.1016/j.biocon.2019.108195

Arthur, K. N. A., & Owen, R. (2019). A Micro-ethnographic study of big Data-Based Innovation in the financial services sector: Governance, ethics and organisational practices. *Journal of Business Ethics*, *160*(2), 363–375. https://doi.org/10.1007/s10551-019-04203-x

Barnes, E. A. (2020). Negotiating the boundaries of our right to privacy: The landscape of privacy behaviors, Surveillance Capitalism, and Public Policy in the United States, State University of New York at Buffalo.

Baron, J. (1986). Tradeoffs among reasons for action. *Journal for the Theory of Social Behaviour*, *16*(2), 173–195. https://doi.org/10.1111/j.1468-5914.1986.tb00074.x

Bélanger, F., Hiller, J., & Smith, W. J. (2002). Trustworthiness in electronic commerce: The role of privacy, security, and site attributes. *Journal of Strategic Information Systems*, *11*(3/4), 245–270. https://doi.org/10.1016/S0963-8687(02)00018-5

Bilal, A., Wingreen, S., & Sharma, R. (2020). Virtue ethics as a solution to the privacy paradox and trust in emerging technologies. *Proceedings of the 2020 the 3rd international conference on information science and system*, 224–228. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/3388176.3388196

Bonilla, D. N. (2014). Information management professionals working for intelligence organizations: Ethics and deontology implications. *Security and Human Rights*, *24*(3–4), 264–279. https://doi.org/10.1163/18750230-02404005

Borton, D. A., Yin, M., Aceros, J., & Nurmikko, A. (2013). An implantable wireless neural interface for recording cortical circuit dynamics in moving primates. *Journal of Neural Engineering*, *10*(2), 026010. https://doi.org/10.1088/1741-2560/10/2/026010

Boyd, D., & Crawford, K. (2012). Critical questions for big data. *Information, Communication & Society*, *15*(5), 662–679. https://doi.org/10.1080/1369118X.2012.678878

Breidbach, C. F., & Maglio, P. (2020). Accountable algorithms? The ethical implications of data-driven business models. *Journal of Service Management*, *31*(2), 163–185. https://doi.org/10.1108/JOSM-03-2019-0073

Broad, C. D. (2014). *Five types of ethical theory*. Routledge.

Campbell, C. (2019). "'The entire system is designed to suppress us.' What the Chinese surveillance state means for the rest of the world," Time. https://time.com/5735411/CHINA-SURVEILLANCE-PRIVACY-ISSUES .

Cavoukian, A. (2011). "Privacy by design: The 7 foundational principles. International Association of Privacy Professionals. https://www.iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf

Center for Policy Leadership (2013). Big data and analytics: seeking foundations for effective privacy guidance. Hunton and Williams LLP. http://www.hunton.com/files/Uploads/Documents/News_files/Big_Data_and_Analytics_February_2013

Charles, V., Tavana, M., & Gherman, T. (2015). The right to be forgotten-is privacy sold out in the big data age? *International Journal of Society Systems Science*, *7*(4), 283–298. https://doi.org/10.1504/IJSSS.2015.073225

Cheney, P. H., & Dickson, G. W. (1982). Organizational characteristics and information systems: An exploratory investigation. *Academy of Management Journal*, *25*(1), 170–184. https://doi.org/10.2307/256032

Clarke, R. (1999). Internet privacy concerns confirm the case for intervention. *Communications of the ACM*, *42*(2), 60–67. https://doi.org/10.1145/293411.293475

Coetzee, F. (2017).The impact of information technology sophistication on the work alienation of knowledge workers. PhD diss., University of Pretoria.

Constantiou, I. D., & Kallinikos, J. (2015). New games, new rules: Big data and the changing context of strategy. *Journal of Information Technology*, *30*(1), 44–57. https://doi.org/10.1057/jit.2014.170268-3962

Craft, J. L. (2013). A review of the empirical ethical Decision-Making literature: 2004–2011. *Journal of Business Ethics*, *117*(2), 221–259. https://doi.org/10.1007/s10551-012-1518-9

Crossan, M., Mazutis, D., & Seijts, G. (2013). In search of virtue: The role of virtues, values and character strengths in ethical decision making. *Journal of Business Ethics*, *113*(4), 567–581. https://doi.org/10.1007/s10551-013-1680-8

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science*, *10*(1), 104–115. https://doi.org/10.1287/orsc.10.1.104

Custers, B. H. M., & Ranchordas, S. (2019). In Reuse of data in smart cities: Legal and ethical frameworks for big data in the public arena. F. Feldberg et al.Eds., *Appropriate use of data in public space: Essay collection* NL Digitaal. SSRN Electronic Journal , Elsevier BV. pp.9–35

Darmody, A., & Zwick, D. (2020). Manipulate to empower: Hyper-relevance and the contradictions of marketing in the age of surveillance capitalism. *Big Data & Society*. https://doi.org/10.1177/2053951720904112

Degli Esposti, S. (2014). When big data meets dataveillance: The hidden side of analytics. *Surveillance & Society*, *12*(2), 209–225. https://doi.org/10.24908/ss.v12i2.5113

Delen, D., & Ram, S. (2018). Research challenges and opportunities in business analytics. *Journal of Business Analytics*, *1*(1), 2–12. https://doi.org/10.1080/2573234X.2018.1507324

Derlega, V. J., & Chaikin, A. L. (1977). Privacy and Self-Disclosure in social relationships. *Journal of Social Issues*, *33*(3), 102–115. https://doi.org/10.1111/j.1540-4560.1977.tb01885.x

Dienlin, T., & Metzger, M. J. (2016). An extended privacy calculus model for SNSs: Analyzing self-disclosure and self-withdrawal in a representative US sample. *Journal of Computer-Mediated Communication*, *21*(5), 368–383. https://doi.org/10.1111/jcc4.12163

Dinev, T., Hart, P., & Mullen, M. (2008). Internet privacy concerns and beliefs about government surveillance–An empirical investigation. *Journal of Strategic Information Systems*, *17*(3), 214–233. https://doi.org/10.1016/j.jsis.2007.09.002

Dobrin, A. (2012, February 05).Why Ethics Is Hard: Some say, Don't bother me with all this thinking. Psychology

Today. February 05 https://www.psychologytoday.com/us/blog/am-i-right/201202/why-ethics-is-hard
Doty, P. (2020). Oxymorons of privacy and surveillance in "smart homes". *Proceedings of the Association for Information Science and Technology*, *57*(1), e222. https://doi.org/10.1002/pra2.222
Drašček, M., Rejc Buhovac, A., & Mesner Andolšek, D. (2020). Moral pragmatism as a bridge between duty, utility, and virtue in managers' ethical Decision-Making. *Journal of Business Ethics*. https://doi.org/10.1007/s10551-020-04489-2
Driver, J. (2011). *Consequentialism*. ISBN 9780415772587. Routledge.
Duncan, R. B. (1972). Characteristics of organizational environments and perceived environmental uncertainty. *Administrative science quarterly* 17(3): 313–327.
Eisenhardt, K. M. (1989, January). Agency theory: An assessment and review. *The Academy of Management Review*, *14* (1), 57–74. JSTOR 258191 https://doi.org/10.5465/amr.1989.4279003
European Parliamentary Research Service. (2020). The ethics of artificial intelligence: Issues and initiatives. European Parliament Think Tank . https://www.europarl.europa.eu/RegData/etudes/STUD/2020/634452/EPRS_STU(2020)634452_EN.pdf
Flaherty, C. (2020). Big proctor. Inside Higher Ed. https://www.insidehighered.com/news/2020/05/11/online-proctoring-surging-during-covid-19
Ford, R. C., & Richardson, W. D. (1994). Ethical decision making: A review of the empirical literature. *Journal of Business Ethics*, *13*(3), 205–221. https://doi.org/10.1007/BF02074820
Foucault, M. (1991). Discipline and punish: The birth of the prison. Translated from the French by Alan Sheridan, translation copyright 1977, Second Vintage Books Edition.
Gal, U., Jensen, T. B., & Stein, M. K. (2020). Breaking the vicious cycle of algorithmic management: A virtue ethics approach to people analytics. *Information and Organization*, *30*(2), 100301. https://doi.org/10.1016/j.infoandorg.2020.100301
Galbraith, J. R. (1974). Organization design: An information processing view. *Interfaces*, *4*(3), 28–36. https://doi.org/10.1287/inte.4.3.28
Gandomi, A., & Haider, M. (2015). Beyond the hype: Big data concepts, methods, and analytics. *International Journal of Information Management*, *35*(2), 137–144. https://doi.org/10.1016/j.ijinfomgt.2014.10.007
Garfinkel, S. L. (2015). De-identification of personal information. National Institute of Standards, U.S. Department of Commerce, NISTIR 8053, October http://dx.doi.org/10.6028/NIST.IR.8053
Garvie, C., & Moy, L. M. (2019).America under watch: Face surveillance in the United States. Georgetown Law: Center on Privacy & Technology, May 16. https://www.law.georgetown.edu/privacy-technology-center/publications/america-under-watch-face-surveillance-in-the-united-states/
Gates, K. A. (2011). *Our biometric future: Facial recognition technology and the culture of surveillance* (Vol. 2). NYU Press.
Gregor, S. (2006). The nature of theory in information systems. *MIS Quarterly*, *30*(3), 611–642. https://doi.org/10.2307/25148742
Gstrein, O. J. (2020). Mapping power and jurisdiction on the internet through the lens of government-led surveillance. *Internet Policy Review*, *9*(3), 1–17. doi: 10.14763/2020.3.1497
Hagen, C. S., Bighash, L., Hollingshead, A. B., Shaikh, S. J., & Alexander, K. S. (2018). Why are you watching? Video surveillance in organizations. *Corporate Communications: An International Journal*, *23*(2), 274–291. https://doi.org/10.1108/CCIJ-04-2017-0043
Hartman, L. P. (2001). Technology and ethics: Privacy in the workplace. *Business and Society Review*, *106*(1), 1–27. https://doi.org/10.1111/0045-3609.00099
Heibutzki, R. (July 1, 2018).Types of surveillance in criminal investigations. Hearst Newspapers Ltd. . https://work.chron.com/types-surveillance-criminal-investigations-9434.html
Herschel, R., & Miori, V. M. (2017). Ethics & big data. *Technology in Society*, *49*, 31–36. https://doi.org/10.1016/j.techsoc.2017.03.003
Holt, M., Lang, B., & Sutton, S. G. (2017). Potential employees' ethical perceptions of active monitoring: The dark side of data analytics. *Journal of Information Systems*, *31* (2), 107–124. https://doi.org/10.2308/isys-51580
Howard-Snyder, F. (1996). A new argument for consequentialism? A reply to Sinnott-Armstrong. *Analysis*, *56*(2), 111–115. https://doi.org/10.1093/analys/56.2.111
Hu, L., & Ni, Q. (2017). IoT-driven automated object detection algorithm for urban surveillance systems in smart cities. *IEEE Internet of Things Journal*, *5*(2), 747–754. https://doi.org/10.1109/JIOT.2017.2705560
Hursthouse, R. (1999). *On virtue ethics*. OUP Oxford.
Hustinx, P. (2010). Privacy by design: Delivering the promises. *Identity in the Information Society*, *3*(2), 253–255. https://doi.org/10.1007/s12394-010-0061-z
International Association of Privacy Professionals (IAPP) (2020). What does privacy mean?. The International Association of Privacy Professionals. https://iapp.org/about/what-is-privacy/
Insights, F. (2018). Organizations are gearing up for more ethical and responsible use of artificial intelligence. SAS Institute Inc. SAS Press Release. (pp. 1–31). http://dssresources.com/news/5035.php .
Katz, V. United States. (n.d.). Oyez. January 19, 2021 https://www.oyez.org/cases/1967/35
Koskela, H. (2006). The other side of surveillance: Webcams, power and agency. In *Theorizing surveillance: The panopticon and beyond. Willan Publishing cop.* (pp. 163–181).
La Fors, K., Custers, B., & Keymolen, E. (2019). Reassessing values for emerging big data technologies: Integrating design-based and application-based approaches. *Ethics and Information Technology*, *21*(3), 209–226. https://doi.org/10.1007/s10676-019-09503–4
Larry, A., & Moore, M. (2007). Deontological ethics. In E. N. ZaltaEd., *the Stanford encyclopedia of philosophy*. Center for the Study of Language and Information, Stanford
Lawrence, P. R., & Lorsch, J. W. (1967). Differentiation and integration in complex organizations. *Administrative Science Quarterly*, *12*(1), 1–47. https://doi.org/10.2307/2391211
Lazar, S. (2017). Deontological decision theory and agent-centered options. *Ethics*, *127*(3), 579–609. https://doi.org/10.1086/690069
Lee, S., Shin, Y., Woo, S., Kim, K.,& Lee, H.N. (2013). Review of Wireless Brain-Computer Interface Systems, Brain-Computer Interface Systems - Recent Progress and Future Prospects, Reza Fazel-Rezai, IntechOpen, doi:10.5772/56436. Available from: https://www.intechopen.com/books/brain-computer-interface-systems-recent-progress-and-future-prospects/review-of-wireless-brain-computer-interface-system s

Lewis, P. V. (1985). Defining 'business ethics': Like nailing jello to a wall. *Journal of Business ethics*, 4(5), 377–383.

Luppicini, R., & So, A. (2016). A technoethical review of commercial drone use in the context of governance, ethics, and privacy. *Technology in Society*, *46*, 109–119. https://doi.org/10.1016/j.techsoc.2016.03.003

Marx, G. T. (1998). An ethics for the new surveillance. *The Information Society*, *14* (3), 171–185. https://doi.org/10.1080/019722498128809 .

Marx, G. T. (2005a). Surveillance and Society. Encyclopedia of Social Theory. MIT. https://web.mit.edu/gtmarx/www/surandsoc.html

Marx, G. T. (2005b). Seeing Hazily (But Not Darkly) through the lens: Some recent empirical studies of surveillance technologies. *Law & Social Inquiry*, *30*(2), 339–399. https://onlinelibrary.wiley.com/doi/pdf/10.1111/j.1747-4469.2005.tb01016.x? .

Mason, R. O. (1986). Four ethical issues of the information age. *MIS Quarterly*, *10*(1), 5–12. https://doi.org/10.2307/248873

May, S. (2013). Introduction: Ethical perspectives and practices. Case studies in organizational communication: Ethical perspectives and practices, 1–33.

McKee, R. (2013). Ethical issues in using social media for health and health care research. *Health Policy*, *110*(2–3), 298–301. https://doi.org/10.1016/j.healthpol.2013.02.006

McParland, C., & Connolly, R. (2020). Dataveillance in the workplace: Managing the Impact of Innovation. *Business Systems Research Journal*, *11*(1), 106–124. https://doi.org/10.2478/bsrj-2020-0008

Merriam Webster (2020). Definition: Privacy. Merriam Webster Inc. https://www.merriam-webster.com/dictionary/privacy

Minevich, M., & Beridze, I. (2020). Using AI responsibly to fight the coronavirus pandemic. Techcrunch, Verizon Media. https://techcrunch.com/2020/04/02/using-ai-responsibly-to-fight-the-coronavirus-pandemic .

Moor, J. H. (2005). Why we need better ethics for emerging technologies. *Ethics and Information Technology*, *7*(3), 111–119. https://doi.org/10.1007/s10676-006-0008-0

Moosavian, R. (2016). A just balance or just imbalance? The role of metaphor in misuse of private information. *Journal of Media Law*, *7*(2), 196–224. https://doi.org/10.1080/17577632.2015.1108587

Morley, J., Cowls, J., Taddeo, M., & Floridi, L. (2020). Ethical guidelines for COVID-19 tracing apps. *Nature*, *582*(7810), 29–31. https://doi.org/10.1038/d41586-020-01578-0

Morley, J., Floridi, L., Kinsey, L., & Elhalal, A. (2020). From what to how: An initial review of publicly available AI ethics tools, methods and research to translate principles into practices. *Science and Engineering Ethics*, *26*(4), 2141–2168. https://doi.org/10.1007/s11948-019-00165-5

Mourey, J. A., & Waldman, A. E. (2020). Past the privacy paradox: The importance of privacy changes as a function of control and complexity. *Journal of the Association for Consumer Research*, *5*(2), 162–180. https://doi.org/10.1086/708034

Nemitz, P. (2018). Constitutional democracy and technology in the age of artificial intelligence. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, *376*(2133). http://doi.org/10.1098/rsta.2018.0089

O'Fallon, M. J., & Butterfield, K. D. (2005). A review of the empirical ethical Decision-Making literature: 1996-2003. *Journal of Business Ethics*, *59*(4), 375–413. OHCHR 1996-2021. https://doi.org/10.1007/s10551-005-2929-7

Olmstead, V. United States, 277 U.S. 438 (1928). Olmstead v. Justia. https://supreme.justia.com/cases/federal/us/277/438

Orwell, G. (1949). *Nineteen Eighty-Four. A novel*. London: Secker & Warburg.

Pal, R., Li, J., Crowcroft, J., Li, Y., Liu, M., & Sastry, N. (2020). Privacy Risk is a Function of Information Type: Learnings for the Surveillance Capitalism Age. *IEEE Transactions on Network and Service Management.*

Palayoor, A. J., & Mavoothu, D. (2017). Ethical orientation: a solution for workplace monitoring and privacy issues. *Seventeenth AIMS international conference on management*.

Palm, E., & Ove Hansson, S. The case for ethical technology assessment (eTA). (2006). *Technological Forecasting and Social Change*, *73*(5), 543–558. 0040-1625. https://doi.org/10.1016/j.techfore.2005.06.002

Pearce, K. E., & Rice, R. E. (2017). Somewhat separate and unequal: Digital divides, social networking sites, and capital-enhancing activities. *Social Media+ Society*, *3*(2), 2056305117716272. https://doi.org/10.1177/2056305117733224

Petronio, S., & Child, J. T. (2020). Conceptualization and operationalization: Utility of communication privacy management theory. *Current Opinion in Psychology, 31*, 76–82. https://doi.org/10.1016/j.copsyc.2019.08.009

Plangger, K., & Montecchi, M. (2020). Thinking beyond privacy calculus: Investigating reactions to customer surveillance. *Journal of Interactive Marketing*, *50*, 32–44. https://doi.org/10.1016/j.intmar.2019.10.004

Power, D. J. (2016). "Big Brother" can watch us. *Journal of Decision Systems*, *25*(2), 578–588. https://doi.org/10.1080/12460125.2016.1187420 sup1

Power, D. J., & Heavin, C. (2017). *Decision support, analytics, and business intelligence* (Third Edition ed.). Business Expert Press.

Power, D. J., & Heavin, C. (2018). *Data-based decision making and digital transformation*. Business Expert Press.

Power, D. J., Heavin, C., McDermott, J., & Daly, M. (2018). Defining business analytics: An empirical approach. *Journal of Business Analytics*, *1*(1), 40–53. https://doi.org/10.1080/2573234X.2018.1507605

Raghupathi, W., & Raghupathi, V. (2014). Big data analytics in healthcare: Promise and potential. *Health Information Science and Systems*, *2*(1), 3. https://doi.org/10.1186/2047-2501-2–3

Ragnedda, M. (2011). Social control and surveillance in the society of consumers. *International Journal of Sociology and Anthropology*, *3*(6), 80–188. https://academicjournals.org/article/article1379500884_Regnedda.pdf

Ranjan, P., Li, J., Crowcroft, J., Li, Y., Liu, M., & Sastry, N. (2020). Privacy risk is a function of information type: learnings for the surveillance capitalism age, in IEEE transactions on network and service management. https://doi.org/10.1109/TNSM.2020.3046704

Raymond, L., & Pare, G. (1992, July). Measurement of IT sophistication in small manufacturing businesses. *Information Resources Management Journal*, *5*(2): 4–16. https://doi.org/10.4018/irmj.1992040101

Reijers, W., & Coeckelbergh, M. (2020). Praxis and Contemporary Philosophy of Technology. *In Narrative and Technology Ethics* (pp. 25–48). Palgrave Macmillan, Cham.

Richards, N. (2013). The dangers of surveillance. Harvard Law Review. May 20, 126 Harv. L. Rev. 1934, https://harvardlawreview.org/2013/05/the-dangers-of-surveillance

Rowe, F. (2020). Contact tracing apps and values dilemmas: A privacy paradox in a neo-liberal world. *International Journal of Information Management*, *55*, 102178. https://doi.org/10.1016/j.ijinfomgt.2020.102178

Sableman, M. (2014). Balancing the data privacy debate: The benefits of big (and little) data. Thompson Coburn LLP Blog post, April 11 https://www.thompsoncoburn.com/insights/blogs/internet-law-twists-turns/post/2014-04-11/balancing-the-data-privacy-debate-the-benefits-of-big-(and-little)-data

Schwartz, M. S. (2016). Ethical decision-making theory: An integrated approach. *Journal of Business Ethics*, *139*(4), 755–776. https://doi.org/10.1007/s10551-015-2886-8

Schwartz, P. M. (1994). Privacy and participation: Personal information and public sector regulation in the United States. *Iowa L. Rev*, *80*, 553. https://heinonline.org/HOL/Page?handle=hein.journals/ilr80&div=29&g_sent=1&casa_token=1YVamnYvZCAAAAAA:KpeEudQyz6gBF2d_xkfHQI8dPKfrjlR0IQy6XxYbjGY_dV88PAL9uXlMITPyuV1AmZWFgpE&collection=journals

Sewell, G., & Barker, J. R. (2006). Coercion versus care: Using irony to make sense of organizational surveillance. *Academy of Management Review*, *31*(4), 934–961. https://doi.org/10.5465/amr.2006.22527466

SHRM. (2019)."Managing workplace monitoring and surveillance. SHRM.org, March 13 https://yourbusiness.azcentral.com/employers-rights-monitor-employees-email-internet-use-8477.html

Sinnott-Armstrong, W. (2019). In Consequentialism, the stanford encyclopedia of philosophy (summer edition). E. N. ZaltaEd. Stanford University. Library of Congress Catalog. https://plato.stanfod.edu/archives/sum2019/entries/consequentialism

Smith, H., Milberg, S., & Burke, S. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly*, *20*(2), 167–196. https://doi.org/10.2307/249477

Sommer, P. (2017). Artificial intelligence, machine learning and cognitive computing.IBM. https://www.ibm.com/blogs/nordic-msp/artificial-intelligence-machine-learning-cognitive-computing

Stahl, B. C., & Wright, D. (2018). Ethics and privacy in AI and big data: Implementing responsible research and innovation. *IEEE Security & Privacy*, *16*(3), 26–33. https://doi.org/10.1109/MSP.2018.2701164

Stone, E. F., Gueutal, G. H., Gardner, D. G., & Mcclure, S. A. (1983). Field experiment comparing information-privacy values beliefs and attitudes across several types of organizations. *Journal of Applied Psychology*, *68*(3), 459–468. https://doi.org/10.1037/0021-9010.68.3.459

Sumner, S. (2016). *You: For sale: Protecting your personal data and privacy online*. ISBN 978-0-12-803405-7. Elsevier Inc.

Syed, A., Gillela, K., & Venugopal, C. (2013). The future revolution on big data. *Future*, *2*(6), 2446–2451. https://www.ics.uci.edu/~ddenenbe/248/Selected%20readings/Networking%20Part%20I/TheFutureRevolutionOnBigData.pdf

Taddicken, M. (2014). The 'privacy paradox' in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure. *Journal of Computer-Mediated Communication*, *19*(2), 248–273. https://doi.org/10.1111/jcc4.12052

Tarkkanen, K., & Harkke, V. (2016). Manifestations of users' privacy concerns in a formative usability test of social networking site. In D. Kreps, G. Fletcher, & M. Griffiths (Eds.), *Technology and intimacy: Choice or Coercion. HCC 2016. IFIP advances in information and communication technology* (Vol. 474), pp.215-228. Springer. https://doi.org/10.1007 .

Tene, O., & Polonetsky, J. (2013). "Big data for all: Privacy and user control in the age of analytics," 11 Nw. J. Tech. & Intell. Prop. 239. Northwestern Journal of Technology and Intellectual Property, Northwestern University . https://scholarlycommons.law.northwestern.edu/njtip/vol11/iss5/1

United Nations Declaration of Human Rights Article 12, Universal declaration of human rights. United Nations . https://www.un.org/en/universal-declaration-human-rights

Vagle, J. (2016). Surveillance is still about power. JustSecurity blog, February 9. https://www.justsecurity.org/29240/surveillance-power/Web-basedresourceJustsecurity

Valera, M., & Velastin, S. A. (2005). Intelligent distributed surveillance systems: A review, in IEE Proceedings - Vision. *IEE Proceedings - Vision, Image, and Signal Processing*, *152*(2), 192–204. https://doi.org/10.1049/ip-vis:20041147

Van Der Sloot,B.,(2014). Privacy as human flourishing: Could a shift towards virtue ethics strengthen privacy protection in the age of big data. *J. Intell. Prop. Info. Tech. & Elec. Com*, *5*, 230. https://www.jipitec.eu/issues/jipitec-5-3-2014/4097

Walker, P. (2021). Call centre staff to be monitored via webcam for home-working 'infractions. The Guardian. https://www.theguardian.com/business/2021/mar/26/teleperformance-call-centre-staff-monitored-via-webcam-home-working-infractions

Warren, L., & Brandeis, S. D. (1890). The right to privacy. *Harvard Law Review*, *IV*December15(5)5 https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html

Wigan, M. (2020). Rethinking IT professional ethics. *Australasian Journal of Information Systems*, *24*. https://doi.org/10.3127/ajis.v24i0.2851

Wolfe, C. (2020). Balancing privacy concerns with video monitoring capabilities. SDMmag.com, July. BNP Media. https://www.sdmmag.com/articles/98278-balancing-privacy-concerns-with-video-monitoring-capabilities

Xu, Z., Mei, L., Hu, C., & Liu, Y. (2016). The big data analytics and applications of the surveillance system using video structured description technology. *Cluster Computing*, 19. Kluwer Academic Publishers. https://doi.org/10.1007/s10586-016-0581-x .

Zalud, B. (2013). 9 ongoing trends for surveillance analytics. BNP Media. https://www.securitymagazine.com/articles/83984-ongoing-trends-for-surveillance-analytics

Zimmerman, E. (2002, June 20).HR must know when employee surveillance crosses the line. Workforce.com, https://www.workforce.com/news/hr-must-know-when-employee-surveillance-crosses-the-line

Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, *30*(1), 75–89. https://doi.org/10.1057/jit.2015.5