Journal of Business Ethics
https://doi.org/10.1007/s10551-019-04143-6

REVIEW PAPER

Biometric Technology and Ethics: Beyond Security Applications

Andrea North-Samardzic[1]

Received: 14 July 2018 / Accepted: 4 March 2019

Abstract
Biometric technology was once the purview of security, with face recognition and fingerprint scans used for identification and law enforcement. This is no longer the case; biometrics is increasingly used for commercial and civil applications. Due to the widespread diffusion of biometrics, it is important to address the ethical issues inherent to the development and deployment of the technology. This article explores the burgeoning research on biometrics for non-security purposes and the ethical implications for organizations. This will be achieved by reviewing the literature on biometrics and business ethics and drawing from disciplines such as computer ethics to inform a more robust discussion of key themes. Although there are many ethical concerns, privacy is the key issue, with associated themes. These include definitions of privacy, the privacy paradox, informed consent, regulatory frameworks and guidelines, and discrimination. Despite the proliferation of biometric technology, there is little empirical research on applied biometrics and business ethics. As such, there are several avenues for research to improve understanding of the ethical implications of using this technology.

Keywords Biometric technology · Ethics · Privacy

Introduction

Biometric technology is widely used by a variety of organizations. Fingerprint scans and face recognition technology (FRT) are commonly used to assist with surveillance and border security. Recently, biometric technology has been used for commercial and civil applications, such as Facebook and iPhone, for identity management. With this evolution in application, questions arise about the ethical use of such technology within the broader field of technology ethics. It is its own field, distinct from other technological innovations such as artificial intelligence, three-dimensional printing, cloud technology, data analytics, nanotechnologies, and robotics (Schuelke-Leech 2018). Like these technologies, biometrics is disruptive, as it has the capacity to "restructure, reorganize, disrupt current social and institutional norms and standards, operations, production, trends, not limited to a particular market or industry" (Schuelke-Leech 2018, p. 270).

Unlike other technological innovations, biometrics leads to additional ethical concerns. Collecting biometric data have been described as "giving up a piece of yourself" (Alterman 2003), akin to extracting a biological sample (Milligan 1999), making it "intrusive" (Sprokkereef and de Hert 2012) and "invasive" (Jain and Kumar 2012) for data subjects. With the advent of second-generation behavioral biometrics, issues extend to covert data capture and lack of transparency and consent (Sprokkereef and de Hert 2012). This impinges on people's right to control their identity (Alterman 2003; Milligan 1999). This requires an examination and exploration of the ethical implications of the use of biometrics in and by organizations.

This article reviews the nascent literature on biometrics in applied organizational and business contexts, extending the themes and debates by drawing from the broader and more longstanding fields of technology and computer ethics. Although the literature on biometrics and business ethics is not substantial, it raises new and troubling questions that require debate and consideration from scholars to inform ethical business practices. While legislation covers many aspects of the ethical issues raised in the literature,

An earlier version of this paper was accepted for the 77th Academy of Management Meeting.

✉ Andrea North-Samardzic
andreans@deakin.edu.au

[1] Department of Management, Deakin Business School, Deakin University, 70 Elgar Road, Burwood, VIC 3125, Australia

Published online: 08 March 2019

regulatory frameworks alone are insufficient to ensure ethical probity in the use of biometric technology in organizations.

This article provides an overview of the nature of biometric technology and its applications. Attention is given to its evolution, from first to second generation and affordances. Next, the literature on biometric technology in applied organizational contexts, specifically business ethics, is reviewed. As most research does not consider ethical concerns for organizations, the extant literature on technology ethics informs a discussion of the themes that emerged from the review of the research on biometrics and business ethics, and ethics theories and frameworks. Building on this review, this article identifies areas for theoretical development, empirical advancement, and practical implications for the ethical use of biometrics. Although there is limited research on this topic, combined with broader research on biometrics and applied ethics, there are significant issues worth the attention of business ethics researchers and organizations.

Biometrics: An Overview of Application and Purpose

Biometric technology concerns the use of the physiological and behavioral characteristics of individuals. Biometric data are usually used for identity management or authentication (Jain et al. 2000). Biometric technology uses people's features and characteristics to capture data such as fingerprints, palm prints and geometry, hand vein patterns, finger knuckle prints, face, ear shape, tongue print, iris, retina, sclera, voice, keystroke dynamics, gait, signature (Unar et al. 2014), pulse and DNA (Sutrop and Laas-Mikko 2012). These can include static and moving images (Zhao et al. 2003). Jain et al. (2004, p. 2) identified the four most important qualities of biometric data:

1. universality: each person should possess the characteristic
2. collectability: the characteristic can quantitatively measured
3. distinctiveness: the characteristic should be different between people
4. permanence: the characteristic should be invariant over time.

The system must also be capable of accuracy and efficiency, acceptable to users, and non-susceptible to circumvention, such as hacking (Jain et al. 2004).

Biometrics can include medico-chemical technology such as magnetic resonance imaging and electrocardiogram machines (Unar et al. 2014). There is merit to recognizing such technology, given that personal fitness devices, such as Apple Watch and Fitbit, are considered biometric technology and incorporate health and medical data into their functions (Karkazis and Fishman 2017). Medico-chemical devices used in medicine are outside the scope of this review, as they were designed for different purposes, have separate regulatory frameworks, and are not used for civil applications outside healthcare. Thus, the ethical implications are different.

There are several notable shifts in biometric technology, from first to second generation. The latter has a greater focus on behaviors, as opposed to individual identifiers. Schumacher (2012) characterizes this shift as moving from "who you are" to "how you are." There has also been shifts in purpose and application, from security to safety (Norval and Prasopoulou 2017), specifically, civilian and private sector applications (Prabhakar et al. 2003).

A 2003 literature review of the applications of FRT (Zhao et al. 2003) identified four main uses of the technology: entertainment, smart cards, information security, and law enforcement. These activities specifically include (but are not limited to) border control, forensics, criminal identification, access control, computer logins, e-commerce, welfare disbursements, missing children identification, identification cards, passports, user authentication on mobile devices, and time and attendance monitoring systems (Bhattacharyya et al. 2009; Unar et al. 2014). With the shift to second-generation biometrics, the technology is extending beyond identity management to group analysis, in which generalizations about demographic categories can be made and behaviors can be analyzed (Schumacher 2012). It has afforded the rise of what McStay (2014, 2018) refers to as emotional surveillance or "empathic media … technologies that track bodies and react to emotions and intentions" (McStay 2016, p. 1). These differences are summarized in Table 1.

The diffusion of biometric technology has created new affordances outside traditional security and identity management. Biometrics has been used to assess student engagement. D'Mello et al. (D'Mello and Graesser 2010; D'Mello et al. 2009; McDaniel et al. 2007), among others (Whitehill et al. 2014), used FRT to evaluate the responses of students to classroom learning. This illustrated that facial movements predict outcomes of engagement, frustration, and learning (Grafsgaard et al. 2013). There is considerable research on audience evaluation in the form of laboratory studies that sought to gauge audience responses to arts, media, and entertainment (Hassib et al. 2017; Kirchberg and Tröndle 2012, 2015; Martella et al. 2015, 2017; Soleymani et al. 2014; Wang and Cesar 2014, 2017; Wang et al. 2014, 2016; Webb et al. 2016). Market research has used "methods such as eye tracking, measurements of brain activity through electroencephalography (EEG), and measurements of psychophysiological changes via electro-dermal activity" (Gregersen et al. 2017, p. 3). This is also known as galvanic skin response.

This research shows that the use of biometrics has significantly broadened beyond its initial applications. With

Table 1 Comparison of first- and second-generation biometrics

	First generation	Second generation
Purpose	Who are you?	How are you?
Application	Identity management and authentication	Safety and behavioral assessment
Context	Government and security	Civil and private sector
Level of analysis	Individual	Groups
Primary ethical concern	Privacy risks	Discrimination power
Example	Fingerprint or face recognition for law enforcement or consumer device identity management	Voice recognition to understand individual affect and face recognition to assess group demographic characteristics such as age, gender, and race

new affordances comes the potential for new or different ethical concerns (Schumacher 2012). The abovementioned studies are lab based. However, the question arises as to what happens when first- and second-generation technology is applied to organizations without ethical research guidelines. Given the widespread use of biometrics, the role of organizations as developers and users requires scrutiny. How business ethics addresses these concerns is worth examining.

Technology and Business Ethics

Before addressing biometrics and ethics in applied business and organizational settings, it is important to first address the existing literature on technology and business ethics so that the relevant research can be positioned in relation to existing debates and themes. A study of biometrics and ethics would be situated in the broader field of applied technology and ethics in organization technology (Buchholz and Rosenthal 2002; Loch et al. 1998; Martin and Freeman 2004). It would sit alongside research themes such as worker surveillance (Brown 1996; Loch et al. 1998; Martin and Freeman 2003; West and Bowman 2016), big data ethics (Herschel and Miori 2017; Nunan and Di Domenico 2017; Zwitter 2014), and the ethics of algorithms (Martin 2018). One of the main questions raised about technology, ethics, and organizations by business ethicists is “who should be accountable for the ethical implications of technologies? (Martin and Freeman 2004)” There is consensus that the organizations that deploy the technology should be accountable (Martin and Freeman 2003; West and Bowman 2016). Martin (2018) argues that developers of algorithms should be responsible for constructing software with ethical principles in mind. The nature of this accountability does not always align with ethical concepts, such as privacy as dynamic in practice (Brown 1996). In addition, the role of the software in the decision being made (either small or large) and the implications of the decision on society (ranging from minimal to pivotal, such as access to public goods) affect the nature of the responsibility (Martin 2018).

The ethics of technology and business have been well established by scholars, which begs the question of whether new ethical concerns arise when biometrics is used for non-security applications. Johnson (2001 in Martin and Freeman 2003) suggests that new technologies do not raise new ethical issues, simply new behaviors. For example, worker surveillance is common. Using biometric technology for this purpose may not change the nature of existing ethical concerns or create new ones. However, it is important to review the literature to ascertain if the use of biometric technology by businesses poses new or different ethical matters for researchers and organizations. Biometric scholars, such as Schumacher (2012), contend that it engenders new ethical considerations.

To advance this inquiry, an important step is to recognize one of the fundamental assumptions underpinning debates about technology and business ethics; that is, the relationship society has with technology. The traditional view considers the relationship either socially or technologically determined, representing two ends of a spectrum (Martin and Freeman 2004, p. 354). For Martin and Freeman (2004), this binary approach is limited, as people’s relationship with technology is neither fully technologically deterministic (i.e., people are controlled by technological artifacts) nor socially determined (i.e., technology is neutral and socially controlled). This approach perpetuates Martin and Freeman’s (2004) separation thesis of business and ethics, in which business is detached from ethics. Instead, they advocate a socio-technical systems approach, in which people’s relationship with technology is a natural social interaction and cannot be appropriately captured by binary opposites; people both shape and are shaped by technology (Martin and Freeman 2004). As such, it is simplistic to cast technology as either value-laden or morally neutral. In practice, people have constant and dynamic interactions with technology and, as such, ethics and technology, like ethics and business, are intertwined (Martin and Freeman 2003).

However, Martin and Freeman (2004) argue that a socio-technical systems approach alone is insufficient for a robust understanding of the situated nature of technology within organizations. They extend this view to account for business ethics concerns. Martin and Freeman (2004) take a pragmatic perspective and draw from their earlier work (Martin and Freeman 2003) that proposes a framework for ethical analysis. This is particularly useful for examining the ethical implications of technology within organizations, which appreciates the situated and relational nature of technology and business ethics. This includes an analysis of the traditional moral concepts of self, relationships with others, community, and property (Martin and Freeman 2003). Regarding the concepts of self, relationships with others, and community, they are surrounded by moral rights and duties such as freedom, privacy, respect, and responsibility. Similarly, property has associated concepts of responsibility, use and ownership, and voluntary agreement.

Whether the literature on biometrics and business ethics engages with these themes and frameworks is of interest to this article. Although this is not an in-depth review of the scholarship on technology and business ethics, this discussion provides an overview of themes and concerns to facilitate a comparison with the review of the biometrics and business ethics literature. The following section provides a review of the research into, and ethical concerns about, biometrics for non-security purposes.

Literature Review

Biometric technology has been in existence for over six decades (Royakkers et al. 2018), making for an expansive body of literature. This creates a challenge for determining the research to be considered to develop a cohesive and comprehensive—although not exhaustive—foundation for biometrics and business ethics scholarship. Three databases were searched (Business Source Complete, ProQuest Central, and ScienceDirect) using the terms “biometric” and “ethics.” Thousands of peer-reviewed journal articles were returned. A cursory examination revealed that a substantial number were irrelevant, as they were unrelated, consisted of book reviews, or were from business publications. To refine the fields, each database was considered separately.

Thirty articles were returned from Business Source Premier, with 15 from scholarly journals. These were scanned to determine if they discussed biometrics or ethics, or merely used the terms as examples. This resulted in six articles that addressed applied organizational, business or management contexts, or non-security applications such as consumer products, worker surveillance, or professional ethics. The search of ProQuest Central resulted in 13,365 peer-reviewed academic articles in scholarly journals. Given the significant number of articles returned, the search was refined to be limited to articles with biometrics and ethics in the abstract; this elicited 26 articles. As ProQuest Central is a multidisciplinary database, 11 medical research articles were returned and removed from the list, leaving 15 articles, with a subsequent article removed due to relevancy. Two were found in the search from Business Source Premier. A review of these articles resulted in an additional three identified as addressing biometrics and ethics in a business context.

It was concerning that the articles that were returned did not account for relevant technology and ethics journals such as *Surveillance and Society, Ethics and Information Technology, Science and Engineering Ethics, Journal of Information, Communication and Ethics in Society*, and *Journal of Business Ethics*. An additional search of these journals using the terms “biometric” and “ethics” returned 87 articles. To refine this search to those that were most relevant to business ethics scholarship, they were scanned to discover if they substantively addressed biometrics and ethics. If the words “biometric” or “ethics” were used only once or twice as illustrative examples of technology but were not actively discussed, the article was removed from the list. Business publications or book reviews were removed. This resulted in a list of 63 articles. These articles were scanned to ascertain if they discussed biometrics and ethics in an applied business or organizational context. This resulted in an additional six articles added to the list.

The search of ScienceDirect resulted in 2870 articles that mentioned “biometric” and “ethics.” Similar to the ProQuest Central database, this was refined by searching for articles with these terms in the title or abstract. Only two were returned, both of which were in public health. As such, none of the search returns from this database were included. The final list of 15 articles that address biometrics and ethics in an organizational or business context is included in Table 2.[1] These articles were reviewed to ascertain key elements such as whether the article was empirical or conceptual, the topic of the article, whether biometrics was the main technological focus, if it encompassed first or second biometric technology (see Table 1), the ethical theories included, the ethical issues raised, and the organizational context in which biometrics was applied.

As observed in Table 2, there are commonalities between the literature on applied biometrics and ethics in business. Most research is conceptual, rather than empirical, which means that evaluation of the applications of the technology and the ethical implications is necessary. First-generation biometrics for identity management is addressed, in addition to second-generation behavioral biometrics. The context in which the technology is applied is varied, with a number of articles exploring the ethical issues associated with biometrics related to customers, such as consumer products (Corcoran and Costache 2016; Park and Skoric 2017; Shi and Wu

[1] This review was updated in October 2018.

Table 2 Summary of articles on biometrics, organizations and business ethics

Authors	Type	Topic	Biometrics as focus technology	Biometric technology addressed	Ethical theories/conceptual frameworks included	Ethical issues raised	Applied organizational context
Ball (2005)	Conceptual	Organizational surveillance	Yes	First and second generation	Surveillance theory, Organizational Theory, Sociological Theory, Feminist Theory, post-structuralism	Surveillance: control, autonomy, privacy, discrimination	General
Corcoran and Costache (2016)	Conceptual	Smartphone identity management	Yes	First generation	None	Surveillance and privacy	Consumer products
Dixon (2008)	Conceptual	Library authentication	Yes	First generation	None	Privacy, confidentiality, fair information principles	Libraries
Evans et al. (2017)	Conceptual	Athlete as employee and wearable technology	Yes	First and second generation	None	Data ownership and privacy, data confidentiality, athlete welfare	Sports organizations
Lodge (2006)	Conceptual	Collaborative e-justice	Yes	First generation	None	Competency, accountability, rights of the individual, data reliability, informed consent, trust, risk, privacy	General
Malsch (2013)	Conceptual	Research governance	No	First and second generation	Theory of double effect, and Just War Theory, deontology, consequentialism	Just intent, proportionality, balance freedom-security, dual use risk/technology assessment, privacy	Technology development organizations
Mingers and Walsham (2010)	Conceptual	Ethical information systems	No	First generation	Habermas' discourse ethics and theory of communicative action	Universalization, legitimacy, efficacy, equity, fairness, justice, codes of ethics for IS practitioners, issues of privacy and security, combating of cybercrime, intellectual property disputes, free and open software, hacking, and the digital divide as a form of social exclusion	General
Odoherty et al. (2016)	Conceptual	Health data storage	Yes	First and second generation	None	Data security, human rights abuses and eugenics, risk, trust, privacy	General

Table 2 (continued)

Authors	Type	Topic	Biometrics as focus technology	Biometric technology addressed	Ethical theories/conceptual frameworks included	Ethical issues raised	Applied organizational context
Park and Skoric (2017)	Conceptual	Consumer products and wearable technology	Yes	First and second generation	None	Data surveillance, privacy, anti-trust, personal freedom	Consumer products
Royakkers et al. (2018)	Conceptual	Ethics of digitization	Yes	First and second generation	None	Privacy, autonomy, security, human dignity, justice, and balance of power	General
Shi and Wu (2017)	Conceptual	Genetic privacy	Yes	First and second generation	None	Privacy	Consumer health products
Sud and VanSandt (2015)	Conceptual	Identity rights, poverty and development	No	First generation	Sen's capability development and social choice research paradigm	Identity rights, inclusive growth, poverty alleviation, financial inclusion, property rights, necessity entrepreneurship	General
Trocchia and Ainscough (2006)	Empirical	Biometrics in retail	Yes	First and second generation	None	Personal safety, data security, identity theft, privacy, social control, surveillance, discrimination, dehumanization	Retail
Ulman et al. (2015)	Conceptual	Neuromarketing	Yes	First and second generation	Habermas' discourse ethics and theory of communicative action	Dignity, integrity, beneficence, non-maleficence, autonomy, informed consent, privacy, confidentiality, vulnerable groups	Marketing
Winter (2014)	Empirical	Consumer data	No	First and second generation	Nissenbaum's contextual integrity	Privacy, surveillance, lack of transparency, discrimination, autonomy and identity, public spaces and the public good, balance of power	Consumer experience

2017), retail (Trocchia and Ainscough 2006), and marketing (Ulman et al. 2015). These authors go beyond addressing biometrics for consumer identity management to address how the technology can be used to extract behavioral information. This issue was also explored in the context of performance data from athletes as employees and the associated ethical implications (Evans et al. 2017). Although biometrics for authentication in libraries (Dixon 2008) is acknowledged, the remaining articles discuss the ethical implications for business and organizations broadly, rather than in relation to specific applications or contexts. For example, Ball (2005) unpacks the ethical concerns if biometrics is used for organizational surveillance in general.

As evidenced in Table 2, less than half the articles used ethics theories or frameworks to inform their analyses, with little convergence; only Habermas' discursive approach was mentioned more than once. The absence of a theoretical or conceptual grounding in the literature is notable and will be discussed later. Many similar ethical themes were raised throughout the articles, indicating an opportunity for unifying theories, concepts, and frameworks to be employed in future research.

The themes identified from the articles in Table 2 are conceptualization of privacy, the privacy paradox, informed consent, legal frameworks, and discrimination. However, 15 articles are insufficient to constitute a meaningful discussion. Similar to the observation by Dierksmeir and Seele (2018) about Bitcoin scholarship, important research on biometrics and ethics is found in other disciplines that pertain to businesses and organizations. Such research was found in the database searches on biometrics. As they did not explicitly discuss business ethics and biometrics in applied organizational contexts, they were not included in Table 2 and the previous discussion. However, they discuss these themes in general terms and will be used to inform a more fulsome discussion of the themes from the articles in Table 2. Their criteria for inclusion were that the entry appeared as a result in the previous database searches and the book or article discussed the ethical implications for biometrics for non-security purposes, including research that considers biometrics for security topics. Border security and human trafficking would not be relevant. The themes were used as search terms to identify supporting literature that may not have been captured by the original search. These themes, combining the literature from the original search and the revised search, will now be discussed.

Conceptualizations of Privacy

As observed in Table 2, privacy was universally referred to, suggesting its primacy as an ethical issue. It is worth noting that, for Royakkers et al. (2018), privacy is more of a legal than ethical issue, given the existence of regulatory frameworks to protect individual privacy. The focus on privacy is unsurprising, as Evans et al. (2017) argue that biometric data are more sensitive than statistical data. Biometric technology is also argued to be an invasion of privacy, as it facilitates surveillance inside organizations toward their workers and outside organizations toward their customers and society (Ball 2005; Corcoran and Costache 2016; Royakkers et al. 2018). This contravenes the right to remain anonymous (Odoherty et al. 2016), which is especially the case for biometric technology embedded in wearable devices (Park and Skoric 2017).

Different authors make different distinctions between types of privacy. Ball (2005) points to corporal privacy and bodily integrity, and Shi and Wu (2017) refer to genetic privacy. Park and Skoric (2017) note the difference between institutional privacy, which is governed by legislation for data protection and social privacy, which is concerned with social norms such as interaction patterns. Royakkers et al. (2018) raise the concepts of spatial and mental privacy. Although these distinctions were acknowledged by the authors, they were not explored in detail.

The literature on biometrics and ethics positions privacy as an issue of autonomy (Karkazis and Fishman 2017; Sutrop and Laas-Mikko 2012) and the individual's control over how and when they are represented to others (Alterman 2003). Privacy has been conceptualized differently. The first notable framework is from Clarke (1997 in Campisi 2013), who distinguishes between four types of privacy regarding information technology and individual rights: decisional privacy is the right of the individual to make decisions regarding their life without undue interference, spatial privacy is the right to personal physical space that cannot be violated without explicit consent, intentional privacy is the right to forbid or prevent further communication of observable events (e.g., conversations held in public) or exposed features (e.g., publishing photos), and informational privacy refers to the right to limit access to personal information that represents information that could be used to identify an individual.

Technology has changed and now possesses the capacity to gather more physical and behavioral data than before. As such, people's understandings of privacy have evolved. Finn et al. (2013) updated the categories by Clarke (1997 in Campisi 2013) to include seven categories of privacy. They considered the framework by Clarke (1997 in Campisi 2013) insufficient to address the concerns raised by new technologies. These are

- privacy of the person, which encompasses the right to keep bodily functions and characteristics (such as genetic codes and biometrics) private
- privacy of behavior and action, which concerns activities that happen in both public and private space

- privacy of personal communication, which aims to avoid intercepting communications, including mail, the use of bugs, directional microphones, telephone, or wireless communication interception or recording, and access to e-mail messages
- privacy of data and images, which includes protecting an individual's data from being automatically available or accessible to others and ensuring that people can have control of their own data
- privacy of thoughts and feelings, which understands that individuals possess the right to independent thought
- privacy of location and space, which argues that individuals have the right to move in public or semi-public space without being identified, tracked, or monitored
- privacy of association (including group privacy), which is concerned with people's right to associate with whomever they wish without being monitored (Finn et al. 2013, pp. 8–9).

Finn et al. (2013) acknowledge that there may appear to be overlaps in these categories; however, each represents distinct forms of privacy that have emerged regarding people's changing relationships with technologies. For example, privacy of location and space may seem similar to privacy of behavior. However, privacy of location and space relates to the right to move throughout space without tracking; privacy of behavior is concerned with the right to behave how a person chooses without interference, as long as they are not harming others (Finn et al. 2013). Privacy of association is different to privacy of behavior, as the former is concerned with the right to associate with any group (e.g., unions or religion) and privacy of behavior is the right to behave within these groups as a person sees fit (Finn et al. 2013).

The main privacy concern with biometrics is informational privacy, as biometrics collects the personal data (Cavoukian et al. 2012; Smith et al. 2013; Sutrop and Laas-Mikko 2012; Van der Ploeg 2003) most closely aligned with the idea by Finn et al. (2013) of privacy of data and image. However, it can be argued that the evolution of second-generation biometrics and commercial and civil usage means that other types of privacy are equally relevant (Ball 2005; Royakkers et al. 2018). For example, FRT in public spaces that can measure emotional responses has the capacity to record interactions with social groups, impinging on the privacies of location and space, thoughts and feelings, behavior and action, and association.

The cumulative effect of different forms of biometric technology exponentially increases privacy concerns. Alterman (2003) argues that the greater the representations that identify people, the more systems are linked that house people's data, resulting in greater loss of privacy. In particular, second-generation biometrics is argued to threaten privacy on a large scale as a result of unprecedented convergence of technological developments (Jain et al. 2011). Conversely, if the technology is less concerned with unique identifiers and if systems are not linked, this suggests a lesser violation of privacy. For Corcoran and Costache (2016), the extent of privacy violations is contingent on who owns the data, what the proportional benefit to the parties are, and whether informed consent occurred. This illustrates that it is not the biometric technology that influences the extent of privacy concerns, but the nature of the application and the data collected.

Privacy Paradox

The literature also recognizes that people's relationships with privacy change as they adopt new technologies (Odoherty et al. 2016; Park and Skoric 2017). For example, in the study by Trocchia and Ainscough (2006), privacy was not the main concern for people using biometric technology as part of the customer experience. Convenience was more pressing, followed by identity theft (Trocchia and Ainscough 2006). This highlights the dynamic nature of the "privacy paradox" noted by Corcoran and Costache (2006), in which people seek to guard their privacy despite sharing a substantial amount of information online.

The "privacy paradox" concerns people's relationships with technology and privacy, specifically, freely exchanging personal images and information while simultaneously having increased concerns about privacy and security (Taddicken 2014). The review by Kokolakis (2017) of the "privacy paradox" demonstrates that attitudes toward privacy and associated behaviors are highly contextual and vary according to the technology and circumstances. The increasing use of social media and interconnected technology means that people are exercising free will and choosing to share more information about themselves, but does not mean they are less concerned about privacy (Maltseva and Lutz 2018; Naker and Greenbaum 2017). Research highlights that younger generations are more concerned about digital privacy, despite being digital natives (Hoofnagle et al. 2010). Although people have reasonable expectations of privacy (Milligan 1999), as social systems change and technologies evolve, so do expectations of privacy. For example, first-generation fingerprint biometrics is used for identity management and security. Second-generation behavioral biometrics can analyze an individual's emotions—tantamount to mind reading (Sprokkereef and de Hert 2012)—arguably a greater invasion of a person's privacy. This enables evaluation of people's inner conditions at scale, which is different to prior technologies and applications that are restricted to assessing external characteristics.

Informed Consent

A key factor that influences the ethical magnitude of biometric technology is whether data subjects have provided informed consent. Several authors in the review noted the importance of informed consent when deploying biometric technology (Corcoran and Costache 2016; Ulman et al. 2015), but do not assume it solves all ethical dilemmas related to privacy (Odoherty et al. 2016). Informed consent is an issue that varies with the application of the technology. If an individual consents to their biometric data being collected and used for legitimate use (e.g., for a research project), then it could be argued that these concerns are not equally significant (Alterman 2003). If individuals consent to their data being collected, such as athletes and wearable technology, then their sense of self is not as compromised and privacy concerns are lessened; their privacy is not being invaded. Arguably, it is willfully relinquished by the subject. Even personal data that are considered protected by law, such as race or sexual activity, can be collected if the subject has voluntarily consented (Sprokkereef and de Hert 2012).

Informed consent is a bigger issue for second-generation biometrics in which covert capture is possible. Subjects are unaware that their information is being collected and so are unable to provide informed consent (Norval and Prasopoulou 2017; Sutrop and Laas-Mikko 2012). This is often the case in situations of security and surveillance (Jain and Kumar 2012). According to Sprokkereef and de Hert (2012, p. 82), "the embedded systems, ambient intelligence, distant sensing and passive biometrics involved require no conscious cooperation from subjects and thus pose a challenge to the traditional concepts used in the fields of data protection and human rights."

As recognized by O'Doherty et al. (2016), even if informed consent is obtained, it does not nullify ethical concerns. For example, power disparities between parties make consent challenging. In the case of professional athletes, even if they consent to the collection of their biometric data and extract benefits from participation, the power relationships between athletes, their teams, and the league often mean that not consenting could have significant repercussions for their careers (Karkazis and Fishman 2017). Even if the relationships have equal power, if the benefits of participation are greater for one party than another, it would potentially violate the principles of fairness (Introna and Nissenbaum 2010). For Introna and Nissenbaum (2010), there may always be a power imbalance that is not in favor of the subject, as many individuals (perhaps none of whom the data subjects are aware of) may have access to, and view, their personal biometric information as part of the process of data storage, analysis, and dissemination.

There is also the challenge of whether data subjects are truly sufficiently informed to properly consent. Several scholars argue for education and training for data subjects on topics such as digital literacy, safety, information security, and privacy (Hoofnagle et al. 2010; Park 2013). Given the lack of data subjects exercising their ex ante rights to withdraw consent to biometric data collection (Introna and Nissenbaum 2010; Sprokkereef and de Hert 2012), this may be attributable to lack of awareness of their rights. The question of whether data subjects are truly sufficiently informed about biometrics to properly consent is worth exploring.

Regulatory Frameworks and Guidelines

Most authors identified in Table 2 argue that privacy and data protection legislation is a cornerstone of the appropriate use of biometrics (Dixon 2008; Evans et al. 2017; Lodge 2006; Malsch 2013; Odoherty et al. 2016; Sud and VanSandt 2015), protecting important issues such as "function creep" (Lodge 2006; Sud and VanSandt 2015) and establishing clear guidelines around data ownership (Corcoran and Costache 2016; Evans et al. 2017; Royakkers et al. 2018), proportionality (Corcoran and Costache 2016; Malsch 2013), benefit (Corcoran and Costache 2016), access (Evans et al. 2017), transparency (Royakkers et al. 2018), and purpose (Odoherty et al. 2016). The United States Fair Information Practices and OECD guidelines are cited by Dixon (2008) as key examples guiding the ethical use of biometrics and professional codes of ethics guiding organizational actions. The latter of which are noted by Mingers and Walsham (2010) as important ethical touchstones.

Although these articles elicited several legal frameworks and professional guidelines to regulate the appropriate use of biometrics and data, the extreme variance that can occur within and across national contexts was explicitly noted (Lodge 2006; Winter 2014). Winter (2014) argues that the privacy and data protection legislation in the European Union (EU) outstrips virtually non-existent frameworks in China. They state that the discourse around privacy versus security can vary substantially in a national context. For example, the EU focuses on migration, overseeing the asylum process, and visa fraud. In the US, the emphasis is on surveillance to facilitate activities in the "war on terror" (Lodge 2006). These separate purposes engender different applications to collect and store data with corresponding different ethical considerations. In the EU, the emphasis is on identity verification, which more closely relates to privacy and data protection. In the US, ethical concerns are more related to profiling and discrimination (Dixon 2008; Lodge 2006).

In addition to the articles identified in Table 2, the literature on data governance—which has existed since the advent of biometric technology—addresses ethical issues such as privacy by design (Norval and Prasopoulou 2017) and value sensitive design (Davis and Nathan 2015). Appropriate and rigorous data governance can mediate many of the risks and concerns about biometrics, particularly around privacy. Data governance specifically includes managing the availability, usability, integrity, and security of the data, and subsequent validity and interpretation (Karkazis and Fishman 2017). For example, access to privileged information can be readily tracked by secure and supportive information systems to ensure accountability for activities (Jain et al. 2011). It includes attention to the reliability and accuracy of the data, who has access to it, and ensures appropriate training of the individuals involved in the process of collection, analysis, and dissemination (Karkazis and Fishman 2017). Data governance is most effective when supported by privacy regulations (Lodge 2012; Schumacher 2012).

In the EU, it is established that all biometric data are classified as personal data under data protection legislation (Karkazis and Fishman 2017; Sprokkereef and de Hert 2012; Van der Ploeg 2003). Recently, the EU has updated the General Data Protection Regulation (GDPR), which came into effect in May 2018, and "regulates the processing by an individual, a company or an organization of personal data relating to individuals in the EU" (European Commission 2018a), thereby including all biometric data. It stipulates that all organizations must adhere to principles of data processing, including collecting data in a transparent and lawful manner, only collecting data for specific purposes, not transferring data from one purpose to another, storing data for no longer than necessary, and ensuring all organizations install technical safeguards to protect data (European Commission 2018b). Although these principles may already be in practice, the GDPR is a 'profound' (Zarsky 2017) piece of legislation, as breaches have potentially severe consequences, such as sanctions of up to four percent of an organization's annual global turnover, or up to €100 million (Albrecht 2016). To ensure compliance, approximately 75,000 privacy officers may be appointed across the globe (Custers et al. 2018). For those outside the EU, the OECD Privacy Guidelines are recommended for member states and cover key ethical principles such as purpose specification, openness, collection limitation, data quality, accountability, use limitation, individual participation, and security safeguards (Campisi 2013).

It is emphasized in the literature that legislation does not automatically lead to adherence (Evans et al. 2017; Lodge 2006; Naker and Greenbaum 2017; Winter 2014). The evolution and diffusion of technology often outpaces the law (Malsch 2013; Schumacher 2012) and allows room for function creep and data to be obtained outside the stated purpose (Lodge 2006, 2012). For example, Park and Skoric (2017) argue that there is limited legislation covering biometrics used for data marketing. Naker and Greenbaum (2017) acknowledge that, in the US, federal privacy law regulating the commercial uses of FRT has lagged and only covers health care and financial services. However, in the future, it is likely that there will be broader legislation. Even with the seemingly robust GDPR, there are significant differences in legal provisions and enforcement across nations. For example, only France has a legal obligation to undertake privacy impact assessments (Custers et al. 2018). Under US privacy law, professional athletes do not own their biometric data. In the EU and Canada, this would be unlawful (Karkazis and Fishman 2017). Thus, operating in a multinational business environment multiplies concerns (Lodge 2012). Further, in cases in which there is an absence of legal frameworks guarding privacy, such as China or some developing nations, the question arises as to which ethical principles will underpin organizations seeking to self-regulate.

Discrimination

Many of the articles in Table 2 address the issue of discrimination and profiling as a result of the biometric data generated (Ball 2005; Corcoran and Costache 2016; Lodge 2006; Mingers and Walsham 2010; Sud and VanSandt 2015). Both first- and second-generation biometrics can be used to demographically classify people based on age, ethnicity, gender, and sexual orientation (Cavoukian et al. 2012; Sprokkereef and de Hert 2012). The latter received significant public backlash when news was released of a study that used FRT to assess sexuality (The Economist 2017). These capabilities and events raise the question: if organizations have the right to discriminate against LGBTI + individuals, what would prevent them from using technology to identify people from this group and terminate employment or refuse service?

The consequences of categorization may be profiling with incomplete information and deindividualization, leading to unjustified and, in liberal societies, unjustifiable discrimination and stigmatization (Ball 2005; Sutrop and Laas-Mikko 2012). For organizations, when these data are used for hiring and firing decision-making, there are risks of exploitation, coercion, and employee discrimination (Campisi 2013; Naker and Greenbaum 2017). Given the history in the US of organizations using genetic testing to inform employment decisions (Murry et al. 2001) and health insurers using personal fitness data to influence pricing (Gurdus 2017), this is a legitimate concern.

For Van der Ploeg (2003), it is not the technology that is discriminatory, but the individuals using the data to inform decision-making. This means acknowledging the agency of the individuals involved in the development and deployment of biometrics. Discussions about negative effects often adopt a technologically deterministic view that deifies technology (Van der Ploeg 2003). Martin and Freeman (2004) note this as one end of a spectrum of the traditional view of technology. They advocate for abandoning this view for a more nuanced socio-technical systems approach. This would allow for greater appreciation of the "deeply politicized" (Norval and Prasopoulou 2017) nature of racial, gender, and sexual identities, particularly as individuals have the right to control the way they are presented to others and how their identities are projected, as subjective and self-defined (Alterman 2003). For example, it has been highlighted in the media that FRT is "racist" and the technology was developed by white coders who created algorithms that failed to account for physical nuances in other races, due to own race bias (Breland 2017), an argument that has empirical support (Klare et al. 2012). Thus, to be non-discriminatory, the use of biometrics capable of categorizing people should be used with an appreciation and critical awareness of the political nature of identity and the implications within. Given the widespread ethical concerns of the issue (see Dhanani et al. 2018 for a meta-analysis), biometrics could extend the technological capabilities of workplace discrimination.

What is discussed less but is important to a discussion of the discriminatory power of biometrics is social exclusion. This issue was raised by Sud and VanSandt (2015) in their research on a biometric identity card in India. One of the main arguments advocating for this is that social inclusion cannot occur without a legal identity, which the biometric identity card provides. They do not address the way biometric technology can be exclusionary, as not all individuals may be able to fulfill the criteria for physical attributes identified by Jain et al. (2004). Wickins (2007) argues that people with physical disabilities may not fit the criteria of physical universality (e.g., they may not have the digits for fingerprint identification or capacity for speech for voice recognition). Wickins (2007) contends that the elderly, or people with mental illness, may not be comfortable using biometrics, which impinges on the criterion of "acceptability" that Jain et al. (2004) consider a requirement for biometric systems. As such, already marginalized individuals may be subject to further social exclusion at the hands of biometrics.

The State of Biometrics and Business Ethics Research

This review of the literature indicates that, although there are overlapping themes in technology and business ethics, there must be greater engagement with the existing business ethics literature and stronger theoretical contributions. A critical starting point is for researchers in biometrics and business ethics to clarify their assumptions about technology and society. Are they adopting a technologically or socially deterministic view and why? A common assumption is that technology is ethically neutral (e.g., Brusoni and Vaccaro 2017), which is problematic, given that it does not provide a nuanced appreciation of people's relationships with technology (Van der Ploeg 2003) and does not account for the ethical issues of business and technology. This perpetuates the separation thesis that plagues business and ethics research (Martin and Freeman 2004). This issue must be addressed for future research to effectively build on existing traditions of business ethics literature.

An explicit recognition of the accountability of organizations was missing from the articles in Table 2, despite being a fundamental concern of technology and business ethics scholarship. It was implicit in debates about privacy and informed consent (i.e., organizations should be held accountable for ensuring informed consent from their subjects) but lacked an active interrogation of the ethical roles, responsibilities, and accountabilities of organizations. Martin's (2018) framework on the firm's responsibility for algorithms illustrates that the nature of the responsibility is not fixed but determined by two factors: the role of the decision in society and the role of the algorithm in the decision. This framework is most relevant when applied to the organizations responsible for creating the algorithms. However, some observations can be extended from this framework to explore the roles and responsibilities organizations should consider when deploying biometrics.

All biometric technology is governed by algorithms. Therefore, it can be stated that the role of the algorithm is significant and the role of the decision is less fixed. This review argues that this depends on the purpose of the data and, in the context of the application, the relationship between the organization and the subject, that is, an employee or consumer. This allows for a more full appreciation of the situated nature of technology and business ethics (Martin and Freeman 2003). It is crucial to understand the nature of the relationship and, drawing from stakeholder theory, examine the power dynamics between parties, particularly when considering the ethical implications of informed consent. For example, a customer has the power to deny their custom to an organization if they do not wish to consent to their biometric data being collected. However, an employee is less likely to quit their job.

In the context of the workplace, it can be stated that the role of the decision is pivotal. Using first-generation biometrics for identity management could physically bar someone from the workplace and prevent them from doing their job. This pales in comparison to second-generation behavioral biometrics. For example, in 2017, Westpac, an Australian bank, stated their intention to trial biometrics to measure the emotions and moods of their employees so that management could intervene to improve stress levels (Eyers 2017). This links to the literature about employee monitoring previously discussed (Brown 1996; Loch et al. 1998; Martin and Freeman 2003; West and Bowman 2016). There is little evidence of these examples in peer-reviewed research, as organizations are likely to be reluctant to expose these practices to external critical inquiry. However, the academic community must heed these trends so that the research community can understand and influence these technologies and ethical concerns.

Using the technology and business ethics literature, some conclusions can be drawn about how biometrics can be ethically used in, and by, organizations. The first is that organizations are accountable for the technology they deploy. Accountability does not stop with the firms designing the algorithms, as biometric technology is limited and organizations must be responsible for understanding the technology they are using. Further, biometrics has the capacity to exacerbate existing ethical concerns by facilitating unethical decision-making. In the example of Westpac what would prevent Westpac from using the data for performance management and discriminatory employment decisions?

Malsch (2013), drawing from consequentialist ethics and the theory of double effect, argues that organizations must account for the potential "evil" consequences of technologies that are intending to do "good." Consider the potential "evil" of the Westpac example. If an employee was consistently rated as having a low mood, they may be considered unmotivated. If they showed higher levels of stress, employers might feel they could not handle the pressure of their role. In both situations, the employee may be experiencing mental health problems such as depression or anxiety, which may register as low moods or high stress levels. To circumvent this, the data would have to be anonymized. However, if management were unaware of who they should target, they may be unable to apply the appropriate intervention. When reviewing the ethical implications of this scenario using a framework such as Martin and Freeman's (2003), significant implications for self, relationship with others, community, and property can be observed, given the infringements on freedom, privacy, and respect. Introducing behavioral biometrics into the workplace presents an ethical problem that has the potential to cause more harm than good. Numerous types of privacy are violated, in which anonymity cannot be preserved, consent is constrained by power imbalance, and the technologies possess in-built biases that facilitate discriminatory decision-making.

This example demonstrates that issues concerning biometrics and business ethics may not be new; however, they are more severe and complex. The evolution of biometric technology accounts for seven types of privacy, including privacy of thoughts and feelings (Finn et al. 2013). Previously, informational privacy was the main concern (Cavoukian et al. 2012; Smith et al. 2013; Sutrop and Laas-Mikko 2012; Van der Ploeg 2003). The use of multiple biometrics at any point has exponential ethical implications (Alterman 2003). The technology has become so advanced that informed consent becomes problematic, as the technology can capture data from subjects who are unaware (Norval and Prasopoulou 2017; Sutrop and Laas-Mikko 2012). One of the more significant problems is not only that biometrics can facilitate discriminatory decisions but also the use of technology provides the illusion of objectivity (Martin 2018). This seemingly enhances the veracity and validity of what may be unethical practices. To illuminate these issues, the following section provides a more detailed roadmap for theoretical and empirical directions to advance research and highlights the practical implications for organizations.

Future Research

Theoretical Perspectives

There are opportunities to extend the theoretical analyses proposed above. Table 2 illustrates that there has not been significant attention given to the relevant ethical frameworks in the literature on biometrics in organizational contexts. This is an important contextual approach to use in future research. The extensive review by Mingers and Walsham (2010) advocates Habermas' discourse ethics as a theoretical lens. This sets an important foundation, as it allows for an exploration of the nuance of people's relationships with technology, affording an appreciation of individual subjectivity, as demonstrated through communications. Habermas' discourse ethics for examinations of biometrics in organizational settings should be used, as it would capture the situated and dynamic nature of the relationship between technology and society. This was described by Martin and Freeman (2003, 2004) and is present in Nissenbaum's (2004, 2009, 2011) contextual integrity framework used by Winter (2014).

Attitudes toward privacy, and relationships with organizations deploying biometrics, are influenced by variations in the technology and its applications. In Winter's (2014) study of retail customers, cameras for surveillance were acceptable to ensure security in a retail environment. However, using biometric technologies for eye tracking and emotion recognition made customers feel uncomfortable and raised ethical concerns. As such, Nissenbaum's (2004, 2009, 2011) contextual integrity framework merits further attention, particularly in relation to privacy, as it facilitates an examination of what happens when ethical standards developed in the contexts of technological emergence migrate to new contexts with less-established norms.

Martin (2016) and Norval and Prasopoulou (2017) use Nissenbaum's (2004, 2009, 2011) framework of contextual integrity to reflect the multifaceted and ever-changing terrain of privacy concerns. Martin (2016) extended Nissenbaum's (2004, 2009, 2011) approach to develop social contract theory. They recognized that people develop micro-social contracts with each provider, technological artifact, and circumstances as they navigate the increasingly interconnected world. As an illustration, Martin (2016) argues that stakeholder complaints about privacy violations are often due to changes in social contracts without consultation and approval. Future research should consider this micro-social contract narrative. This requires an examination of expectations about privacy from a stakeholder perspective, what is considered when forming those norms (Martin 2016), and apply it to biometrics in organizational contexts. For example, Carpenter et al. (2018) surveyed attitudes on biometrics by employees and discovered that professional affiliations influenced an individual's trust in an organization. The study by Maltseva and Lutz (2018) of people using self-tracking products discovered that privacy concerns had a negative effect on trust and that self-tracking activities led to increased disclosure of personal information. However, they noted that the context in which the data were collected played a key role. These studies did not examine these phenomena from an ethics perspective. Thus, Martin's (2016) framework could be used as a theoretical lens to explain such findings.

Ball's (2005) unified approach to organizational surveillance merits further research. There is ongoing attention given to the ethical implications of workplace surveillance, with Ball (2010) providing a recent review of the literature and others making conceptual (Henschke 2017; Moore and Piwek 2017) and empirical (Carpenter et al. 2018; Holland et al. 2015) contributions. Using technology to monitor employees is not novel (Brown 1996; Fairweather 1999). Milligan (1999) raised the issue that biometric surveillance for security purposes could be extended to observation of employees to better understand behaviors, particularly related to performance. Organizational surveillance literature draws from a multitude of theories in addition to those utilized by Ball (2005), such as virtue ethics (West and Bowman 2016), psychological reactance, planned behavior, social identity theories (Martin et al. 2016), and routine activity theory (de Vries and van Gelder 2015). The explanatory power of these theories when examining biometric surveillance is a promising avenue for future research.

Recent work has extended Ball's (2005) theorizing on corporal surveillance and bodily integrity, which has consolidated into a body of literature on the "digitalisation of self." Deborah Lupton's ongoing work in critical digital data studies and critical digital health studies is particularly useful for theorizing the ethical effect of consumer product biometrics, particularly those designed for self-tracking, such as Fitbit and Apple Watch. Lupton examines key issues such as power relationships between data subjects and technology (Lupton 2016a), the complex sense-making processes people undergo to understand and accept data (Lupton 2016b, 2017), potential anxiety caused by biometric self-tracking (Lupton 2013), exposure to function creep, and potential exploitation (Lupton 2016a). Lupton (2016c) points to Beck's notion of the "risk society" as a useful theoretical perspective to examine the ethical dilemmas pertaining to risk associated with technological innovations. This view is supported by Sutrop and Laas-Mikko (2012). The theorizing by Lupton and others researchers (e.g., Henschke 2017) and empirical work by Maltseva and Lutz (2018) on the digitized self is valuable for investigating the effect of biometric data capture on employees and consumers.

There is also an opportunity to draw from the theoretical traditions of additional business ethics, such stakeholder theory and corporate social responsibility (CSR), to more squarely situate further research within business ethics scholarship. As discussed in the previous section, ethical implications are strongly related to the relationships between individuals, biometrics, and their contextual environment. As such, their position as data subject and stakeholder influence the nature of the ethical concern, making stakeholder theory a natural theoretical lens for such an analysis. For example, if FRT is used in a retail environment to gather data on shoppers and employees, how would the ethical implications differ for the separate groups? Stakeholder theory can illuminate the complicated social relationships between data subjects and organizations, enabling an exploration of ethical issues such as relational trust (Greenwood and Van Buren III 2010). Similarly, Sheehy's (2015, p. 635) conceptualization of CSR as "an international private business self-regulation" indicates that an examination of self-regulation practices of businesses using biometrics would benefit from drawing on the CSR literature, paying particular attention to the responsibility and accountability of organizations as they deploy biometric technology. Given that technology law is slow and inconsistently applied (Lodge 2012), the ethical use of biometric technology could be well positioned within CSR research. This could assist with providing a larger empirical foundation for much-needed data collection and position the ethical use of biometrics and other technologies as a key responsibility for socially responsible organizations.

Empirical Advancement and Practical Implications

There is limited empirical research on biometrics and ethics in applied business and organizational contexts. Therefore, there are many opportunities for empirical advancement. The contextual nature of ethical concerns means that data should be obtained from multiple settings and situated within the broader environment, for example, giving attention to the potential influence of the legal environment of ethical practice and contextual nuances, such as industry-level environmental factors. McStay's (2014, 2016, 2018) research on the affordances and concerns of biometrics that captures and analyzes people's emotions demonstrates that there is a strong business case for using the technology in retail organizations, marketing, and advertising. It would provide rich evaluative data on customers, translating into a better buying experience.

Attention to context also means attention to national culture. Different national legal environments allow for different degrees of privacy when collecting data, as observed in China's strict internet governance (Hou 2017) and India's biometric identity card (Sud and VanSandt 2015). Cultural values and attitudes also have an influence. As privacy is considered by some a "value" not a "right" (Mingers and Walsham 2010; Winter 2014), attitudes toward privacy could be influenced by national cultural values. This view has support (Li et al. 2017; Miltgen and Peyrat-Guillard 2014); however, not all research points to differences in cultural attitudes toward privacy (e.g., Pentina et al. 2016), which allows for empirical contributions.

Given the need for empirical data, such contributions can take many methodological forms. Due to the importance of a contextual understanding, qualitative and exploratory research is required to build empirical foundations. Mixed methods case studies allow for an appreciation of the situational factors that influence privacy and other ethical concerns. Although industry collaboration on case studies would be immensely valuable, due to the sensitive nature of the topic and privacy as the main ethical concern, finding industry partners willing to provide data about their activities, even ethical ones, is likely to be difficult. Quantitative surveys to assess broader themes, such as consumer attitudes or industry-level themes, would be worthwhile. For example, McStay's (2018) qualitative research into behavioral biometrics using 100 interview subjects can be scaled using quantitative methodologies, considering contexts beyond the UK, and gathering data to facilitate cross-cultural comparisons.

Based on the themes identified in the review of the articles, Table 3 illustrates areas for future research and implications for practice.

As stated, although informational privacy dominates the literature, other forms of privacy must be accounted for in research and practice. The distinctions between categories of privacy must be meaningfully addressed and debated. Because second-generation biometrics is arguably more invasive than first generation (Jain and Kumar 2012), exploring the different types of privacy and ethical implications associated with the different generations is a way forward for researchers. For practice, given the focus on informational privacy, other forms of privacy may not be recognized in professional guidelines, organizations policies, codes of ethics, and legislation. Organizations should assess the way they conceptualize and practice privacy for the various biometric technologies they use with a critical awareness of the categories of privacy described by Finn et al. (2013).

The privacy paradox is often cited in conceptual articles, but there is limited evidence of how it is practiced, particularly pertaining to applied biometrics. As attitudes

Table 3 Empirical advancement and implications for practice

Privacy theme	Future research	Implications for practice
Categories of privacy	Examination of the different definitions of privacy (beyond informational privacy) and the variable ethical implications across	Broad coverage of privacy types in professional guidelines, organizational policies and codes of ethics, not just informational privacy
Privacy paradox	Data on stakeholders' views of various biometric technologies. How the privacy paradox is practiced. How control and power influences the paradox	Policies and practices sensitive to the privacy paradox. Question assumptions of consistency in privacy expectations, particularly in relation to an individual's information disclosure
Informed consent	The nature of 'informed.' Investigations of contexts in which informed consent is used or not. Power disparities embedded in consenting relationships and proportionality	Informed consent should be standard. Providing technological explanations in lay terms for the general public. Attention to power disparities should be reflexive practice. Ensure avenues for withdrawal of consent and data deletion
Regulatory environment	Organizational responses to legislative changes. Ethical principles underpinning both positive and negative self-regulation	Codes of ethics in multinational environment, self-regulation practices, privacy officers, and ethical impact assessments
Discrimination	Ongoing accuracy testing and exploration of uses of biometrics and impact on decision-making in organizations for employees as well as customers	Assessment of use of biometrics, intent and purpose principle. How does it inform decision-making around employment decisions and is it used alongside other methods that promote equitable decision processes and outcomes? Awareness of inaccuracies inherent in the technology

toward privacy are contextual and informed by relationships between the technology and the organization, greater attention to the dynamic nature of the privacy paradox is required. For example, Maltseva and Lutz (2018) showed that trust is a key factor related to privacy concerns. They posited that privacy concerns are influenced by the context, purpose, and nature of the data-collection process. Drawing from stakeholder theory could inform a more holistic view of how the paradox may differ across organizational stakeholders and provide a more nuanced understanding of the way power disparities between parties influence ethical implications and translate into more effective organizational policies and practices.

Several themes about informed consent emerged. Future empirical research can contribute to questions such as whether people are sufficiently informed and able to understand complex biometric technology to be able to properly consent (Hoofnagle et al. 2010; Park 2013), and in what contexts covert data occur to prevent the opportunity for informed consent (Norval and Prasopoulou 2017; Sprokkereef and de Hert 2012). An additional concern is proportionality, that is, whether there is a proportional increase in gains for data subjects and the organizations (Alterman 2003), particularly if it is being used to gather data from employees (Karkazis and Fishman 2017). These themes are also important for ethical practice. Organizations must ensure that subjects are informed about the nature of the technology and the processes governing the resultant data. Further, they must guarantee that the study is beneficial to the subjects.

Legislation and regulatory frameworks standardize and enforce ethical practice; however, there are limitations. For example, only healthcare and financial institutions are covered by existing US legislation on biometric data capture (Naker and Greenbaum 2017). Even the European GDPR does not ensure consistency in practices (Custers et al. 2018). Further evidence is required about how organizations comply or evade legislation, how they seek to engage in ethical technology practices, and the ethical principles used to justify behaviors. The study by Winter et al. (2004) about the ethical attitudes of IT professionals found that Machiavellianism and ethical relativism influenced acceptance of intellectual property and privacy rights violations, which varied across professional groups and workplace experiences. Given that this research illustrates the ease with which individuals violate legal and ethical principles, more empirical evidence of such phenomena is required, particularly across cultural contexts and legal environments. Because working in multinational contexts provides additional concerns, a multinational organization's code of ethics on the use of biometric technology must also be global in its orientation. As legal changes are outpaced by technological innovations, rendering them insufficient, organizations must attend to their ethical obligations first.

As highlighted in the previous section, the final theme of "discrimination" has significant ethical implications. Discrimination is prevalent in first- and second-generation behavioral biometrics (Schumacher 2012). Therefore, commercial use of biometrics should only be deployed with a deep respect for the purpose principle, only using it when it is the most effective way to gather data about the individual without harming their rights (Lodge 2006, 2012). The research community must also be engaged in this topic to gather the necessary data to support the ethical use of biometrics to prevent discrimination. This includes research about which organizations are collecting these data and why, and how it is being used to inform decision-making. A multidisciplinary approach is advocated, as biometrics ethics traverses the confines of one discipline. For example, although it is not the explicit domain of business ethics, attention to the findings of the accuracy tests performed by the National Institute of Standards and Technology (NIST 2018) would allow an appreciation of the accuracy of biometric technology and how technology accuracy influences discriminatory practices.

Conclusion

Biometrics has become part of the landscape of business and organizations, as developers, users, and deployers of technology. While the disciplines of computer and technology ethics extensively explore the implications of biometrics, the ethical implications with which organizations must contend have gained comparatively little attention. The aim of this article was to review the smaller body of research about biometrics and business ethics and draw from the larger research areas to establish an empirical and conceptual foundation for further research.

One limitation of this article is that there are relatively few articles about biometrics and business ethics. This was offset by incorporating the broader literature on biometrics and ethics into a discussion about the main themes and theories. Given that the current and potential scope of the literature on biometrics and ethics is vast, it is likely that there are additional ethical concerns worth the attention of business ethics researchers that were not examined here.

Many of these were identified as areas for future research, with a need for ongoing attention given to theoretically and empirically bridging the gap between biometrics research and business ethics. Future research must acknowledge the contextual and complex nature of people's relationships with technology and consider the particularities of the ethical concerns of biometrics, not technology in general. Because second-generation biometrics has greater capacity to be used without informed consent, even a generalized understanding of biometrics and ethics would not capture the subtleties of an individual's relationship with the technology and the organization.

As the law is not guaranteed to ensure that privacy is upheld, business ethics research becomes increasingly important to ensure individual rights and civil liberties are not compromised. Computer and technology ethics researchers have made valuable contributions; however, the business and organizational implications of biometrics is not their primary ethical concern. As organizations are the site of the development and deployment of biometric technology, and biometrics has the capacity to incite unique ethical concerns, it would be beneficial to the community to give this topic greater attention.

Acknowledgements Feedback from the anonymous reviewers informed this updated version; I greatly appreciate their efforts and useful suggestions in improving the manuscript. I would also like to acknowledge the research assistance of Ishan Senarathna. I would also like to thank Nicholas Patterson and Matthew Warren for their feedback and guidance in the early stages.

Funding Funding for this research was provided by the Deakin Business School, Centre for Sustainable and Responsible Organisations (CSaRO).

Compliance with Ethical Standards

Conflict of interest I declare that I have no conflict of interest.

References

Albrecht, J. P. (2016). How the GDPR will change the world. *European Data Protection Law Review, 2*, 287–289.

Alterman, A. (2003). "A piece of yourself": Ethical issues in biometric identification. *Ethics and Information Technology, 5*(3), 139–150.

Ball, K. (2005). Organization, surveillance and the body: Towards a politics of resistance. *Organization, 12*(1), 89–108.

Bhattacharyya, D., Ranjan, R., Alisherov, F., & Choi, M. (2009). Biometric authentication: A review. *International Journal of u-and e-Service, Science and Technology, 2*(3), 13–28.

Breland, A. (2017). How white engineers built racist code—and why it's dangerous for black people. https://www.theguardian.com/technology/2017/dec/04/racist-facial-recognition-white-coders-black-people-police. Accessed 1 Nov 2018.

Brown, W. S. (1996). Technology, workplace privacy and personhood. *Journal of Business Ethics, 15*(11), 1237–1248.

Brusoni, S., & Vaccaro, A. (2017). Ethics, technology and organizational innovation. *Journal of Business Ethics, 143*(2), 223–226.

Buchholz, R. A., & Rosenthal, S. B. (2002). Technology and business: Rethinking the moral dilemma. *Journal of Business Ethics, 41*(1–2), 45–50.

Campisi, P. (2013). *Security and privacy in biometrics* (Vol. 24). New York: Springer.

Carpenter, D., McLeod, A., Hicks, C., & Maasberg, M. (2018). Privacy and biometrics: An empirical examination of employee concerns. *Information Systems Frontiers, 20*(1), 91–110.

Cavoukian, A., Chibba, M., & Stoianov, A. (2012). Advances in biometric encryption: Taking privacy by design from academic research to deployment. *Review of Policy Research, 29*(1), 37–61.

Corcoran, P., & Costache, C. (2016). Smartphones, biometrics, and a brave new world. *IEEE Technology and Society Magazine, 35*(3), 59–66.

Custers, B., Dechesne, F., Sears, A. M., Tani, T., & van der Hof, S. (2018). A comparison of data protection legislation and policies across the EU. *Computer Law and Security Review, 34*(2), 234–243.

D'Mello, S. K., Craig, S. D., & Graesser, A. C. (2009). Multimethod assessment of affective experience and expression during deep learning. *International Journal of Learning Technology, 4*(3–4), 165–187.

D'Mello, S. K., & Graesser, A. (2010). Multimodal semi-automated affect detection from conversational cues, gross body language, and facial features. *User Modeling and User-Adapted Interaction, 20*(2), 147–187.

Davis, J., & Nathan, L. P. (2015). Value sensitive design: Applications, adaptations, and critiques. In Handbook of ethics, values, and technological design (pp. 11–40). New York: Springer.

de Vries, R. E., & van Gelder, J.-L. (2015). Explaining workplace delinquency: The role of Honesty–Humility, ethical culture, and employee surveillance. *Personality and Individual Differences, 86*, 112–116.

Dhanani, L. Y., Beus, J. M., & Joseph, D. L. (2018). Workplace discrimination: A meta-analytic extension, critique, and future research agenda. *Personnel Psychology, 71*(2), 147–179.

Dierksmeier, C., & Seele, P. (2018). Cryptocurrencies and business ethics. *Journal of Business Ethics, 152*(1), 1–14.

Dixon, P. (2008). Ethical issues implicit in library authentication and access management: Risks and best practices. *Journal of Library Administration, 47*(3–4), 141–162.

Economist, T. (2017). Advances in AI are used to spot signs of sexuality. https://www.economist.com/news/science-and-technology/21728614-machines-read-faces-are-coming-advances-ai-are-used-spot-signs. Accessed 1 Nov 2018.

European Commission. (2018a). What does the General Data Protection Regulation (GDPR) govern? https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-does-general-data-protection-regulation-gdpr-govern_en. Accessed 28 Dec.

European Commission. (2018b). What data can we process and under what conditions? https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/what-data-can-we-process-and-under-which-conditions_en. Accessed 29 Dec.

Evans, R., McNamee, M., & Owen, G. (2017). Ethics, nanobiosensors and elite sport: The need for a new governance framework. *Science and Engineering Ethics, 23*(6), 1487–1505.

Eyers, J. (2017). Westpac testing AI to monitor staff and customers. Australian Financial Review. November 14. https://www.afr.com/technology/westpac-testing-ai-to-monitor-staff-and-customers-20171114-gzks7h. Accessed 29 Dec 2018.

Fairweather, N. B. (1999). Surveillance in employment: The case of teleworking. *Journal of Business Ethics, 22*(1), 39–49.

Grafsgaard, J., Wiggins, J. B., Boyer, K. E., Wiebe, E. N., & Lester, J. (2013). Automatically recognizing facial expression: Predicting engagement and frustration. In *Proceedings of the 6th International Conference on Educational Data Mining* (pp. 43–50).

Greenwood, M., & Van Buren, I. I. I., H. J (2010). Trust and stakeholder theory: Trustworthiness in the organisation–stakeholder relationship. *Journal of Business Ethics, 95*(3), 425–438.

Gregersen, A., Langkjær, B., Heiselberg, L., & Wieland, J. L. (2017). Following the viewers: Investigating television drama engagement through skin conductance measurements. *Poetics, 64*, 1–13.

Gurdus, E. (2017). UnitedHealthcare and Fitbit to pay users up to $1,500 to use devices, Fitbit co-founder says. https://www.cnbc.com/2017/01/05/unitedhealthcare-and-fitbit-to-pay-users-up-to-1500-to-use-devices.html. Accessed 4 Nov 2018.

Hassib, M., Schneegass, S., Eiglsperger, P., Henze, N., Schmidt, A., & Alt, F., EngageMeter: A system for implicit audience engagement sensing using electroencephalography. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems, 2017* (pp. 5114–5119): ACM.

Henschke, A. (2017). *Ethics in an age of surveillance: Personal information and virtual identities*. Cambridge: Cambridge University Press.

Herschel, R., & Miori, V. M. (2017). Ethics and big data. *Technology in Society, 49*, 31–36.

Holland, P. J., Cooper, B., & Hecker, R. (2015). Electronic monitoring and surveillance in the workplace: The effects on trust in management, and the moderating role of occupational type. *Personnel Review, 44*(1), 161–175.

Hoofnagle, C. J., King, Jennifer, Li, Su, & Turow, J. (2010). How different are young adults from older adults when it comes to information privacy attitudes and policies?. Available at https://doi.org/10.2139/ssrn.1589864.

Hou, R. (2017). Neoliberal governance or digitalized autocracy? The rising market for online opinion surveillance in China. *Surveillance and Society, 15*(3/4), 418–424.

Introna, L., & Nissenbaum, H. (2010). Facial recognition technology a survey of policy and implementation issues. Lancaster University Management School Working Paper (Vol. 2010/030): Lancaster University.

Jain, A. K., Hong, L., & Pankanti, S. (2000). Biometric identification. *Communications of the ACM, 43*(2), 90–98.

Jain, A. K., & Kumar, A. (2012). Biometric recognition: an overview. In Second generation biometrics: The ethical, legal and social context (pp. 49–79). New York: Springer.

Jain, A. K., Ross, A. A., & Nandakumar, K. (2011). Introduction. In *Introduction to biometrics* (pp. 1–49). New York: Springer.

Karkazis, K., & Fishman, J. R. (2017). Tracking US professional athletes: The ethics of biometric technologies. *The American Journal of Bioethics, 17*(1), 45–60.

Kirchberg, V., & Tröndle, M. (2012). Experiencing exhibitions: A review of studies on visitor experiences in museums. *Curator, 55*(4), 435–452.

Kirchberg, V., & Tröndle, M. (2015). The museum experience: Mapping the experience of fine art. *Curator, 58*(2), 169–193.

Klare, B. F., Burge, M. J., Klontz, J. C., Bruegge, R. W. V., & Jain, A. K. (2012). Face recognition performance: Role of demographic information. *IEEE Transactions on Information Forensics and Security, 7*(6), 1789–1801.

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers and Security, 64*, 122–134.

Li, Y., Kobsa, A., Knijnenburg, B. P., & Nguyen, M. C. (2017). Cross-cultural privacy prediction. *Proceedings on Privacy Enhancing Technologies*, 2017(2), 113–132.

Loch, K. D., Conger, S., & Oz, E. (1998). Ownership, privacy and monitoring in the workplace: A debate on technology and ethics. *Journal of Business Ethics, 17*(6), 653–663.

Lodge, J. (2006). Ethical EU eJustice: Elusive or illusionary? *Journal of Information, Communication and Ethics in Society, 4*(3), 131–144.

Lodge, J. (2012). The dark side of the moon: Accountability, ethics and new biometrics. In Second generation biometrics: The ethical, legal and social context (pp. 305–328). New York: Springer.

Lupton, D. (2013). Quantifying the body: Monitoring and measuring health in the age of mHealth technologies. *Critical Public Health, 23*(4), 393–403.

Lupton, D. (2016a). The diverse domains of quantified selves: Self-tracking modes and dataveillance. *Economy and Society, 45*(1), 101–122.

Lupton, D. (2016b). Personal data practices in the age of lively data. Digital sociologies, 335–350.

Lupton, D. (2016c). You are your data: Self-tracking practices and concepts of data. In *Lifelogging* (pp. 61–79): Springer.

Lupton, D. (2017). Feeling your data: Touch and making sense of personal digital data. *New Media and Society, 19*(10), 1599–1614.

Malsch, I. (2013). The just war theory and the ethical governance of research. *Science and Engineering Ethics, 19*(2), 461–486.

Maltseva, K., & Lutz, C. (2018). A quantum of self: A study of self-quantification and self-disclosure. *Computers in Human Behavior, 81*, 102–114.

Martella, C., Gedik, E., Cabrera-Quiros, L., Englebienne, G., & Hung, H. (2015). How was it?: Exploiting smartphone sensing to measure implicit audience responses to live performances. In *Proceedings of the 23rd ACM International conference on Multimedia* (pp. 201–210). Brisbane Australia.

Martella, C., Miraglia, A., Frost, J., Cattani, M., & van Steen, M. (2017). Visualizing, clustering, and predicting the behavior of museum visitors. *Pervasive and Mobile Computing, 38*, 430–443.

Martin, A. J., Wellen, J. M., & Grimmer, M. R. (2016). An eye on your work: How empowerment affects the relationship between electronic surveillance and counterproductive work behaviours. *The International Journal of Human Resource Management, 27*(21), 2635–2651.

Martin, K. (2016). Understanding privacy online: Development of a social contract approach to privacy. *Journal of Business Ethics, 137*(3), 551–569.

Martin, K. (2018). Ethical implications and accountability of algorithms. *Journal of Business Ethics*, 1–16.

Martin, K., & Freeman, R. E. (2003). Some problems with employee monitoring. *Journal of Business Ethics, 43*(4), 353–361.

Martin, K. E., & Freeman, R. E. (2004). The separation of technology and ethics in business ethics. *Journal of Business Ethics, 53*(4), 353–364.

McDaniel, B., D'Mello, S., King, B., Chipman, P., Tapp, K., & Graesser, A. (2007). Facial features for affective state detection in learning environments. In D.S. McNamara and J.G. Trafton (Eds.) *Proceedings of the 29th Annual Cognitive Science Society*, (pp. 467–472), Austin.

McStay, A. (2014). *Privacy and philosophy: New media and affective protocol*. New York, Peter Lang.

McStay, A. (2016). Empathic media and advertising: Industry, policy, legal and citizen perspectives (the case for intimacy). *Big Data and Society, 3*(2), 1–11.

McStay, A. (2018). *Emotional AI: The rise of empathic media*. Bangor: Sage.

Milligan, C. S. (1999). Facial recognition technology, video surveillance, and privacy. *Southern California Interdisciplinary Law Journal, 9*, 295.

Miltgen, C. L., & Peyrat-Guillard, D. (2014). Cultural and generational influences on privacy concerns: A qualitative study in seven European countries. *European Journal of Information Systems, 23*(2), 103–125.

Mingers, J., & Walsham, G. (2010). Toward ethical information systems: The contribution of discourse ethics. *MIS Quarterly, 34*(4), 833.

Moore, P., & Piwek, L. (2017). Regulating wellbeing in the brave new quantified workplace. *Employee Relations, 39*(3), 308–316.

Murry, W. D., Wimbush, J. C., & Dalton, D. R. (2001). Genetic screening in the workplace: Legislative and ethical implications. *Journal of Business Ethics, 29*(4), 365–378.

Naker, S., & Greenbaum, D. (2017). Now you see me: Now you still do: Facial recognition technology and the growing lack of privacy. *Boston University Journal of Science & Technology Law, 23*, 88.

Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review, 79*, 119–158.

Nissenbaum, H. (2009). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford: Stanford University Press.

Nissenbaum, H. (2011). A contextual approach to privacy online. *Daedalus, 140*(4), 32–48.

NIST (2018). National Institute of Standards and Technology Face Recognition Vendor Test. https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt. Accessed 4 Nov.

Norval, A., & Prasopoulou, E. (2017). Public faces? A critical exploration of the diffusion of face recognition technologies in online social networks. *New Media and Society, 19*(4), 637–654.

Nunan, D., & Di Domenico, M. (2017). Big data: A normal accident waiting to happen? *Journal of Business Ethics, 145*(3), 481–491.

Odoherty, K. C., Christofides, E., Yen, J., Bentzen, H. B., Burke, W., Koenig, N. H. A., et al. (2016). If you build it, they will come: Unintended future uses of organised health data collections. *BMC Medical Ethics, 17*(54), 1–16.

Park, Y. J. (2013). Digital literacy and privacy behavior online. *Communication Research, 40*(2), 215–236.

Park, Y. J., & Skoric, M. (2017). Personalized ad in your Google Glass? Wearable technology, hands-off data collection, and new policy imperative. *Journal of Business Ethics, 142*(1), 71–82.

Pentina, I., Zhang, L., Bata, H., & Chen, Y. (2016). Exploring privacy paradox in information-sensitive mobile app adoption: A cross-cultural comparison. *Computers in Human Behavior, 65*, 409–419.

Prabhakar, S., Pankanti, S., & Jain, A. K. (2003). Biometric recognition: Security and privacy concerns. *IEEE Security and Privacy, 99*(2), 33–42.

Royakkers, L., Timmer, J., Kool, L., & Rinie van, E. (2018). Societal and ethical issues of digitization. *Ethics and Information Technology, 20*(2), 127–142.

Schuelke-Leech, B. A. (2018). A model for understanding the orders of magnitude of disruptive technologies. *Technological Forecasting and Social Change, 129*, 261–274.

Schumacher, G. (2012). Behavioural biometrics: Emerging trends and ethical risks. In *Second Generation Biometrics: The Ethical, Legal and Social Context* (pp. 215–227). New York: Springer.

Sheehy, B. (2015). Defining CSR: Problems and solutions. *Journal of Business Ethics, 131*(3), 625–648.

Shi, X., & Wu, X. (2017). An overview of human genetic privacy. *Annals of the New York Academy of Sciences, 1387*(1), 61–72.

Smith, G. J. D., San Roque, M., Westcott, H., & Marks, P. (2013). Surveillance texts and textualism: Truthtelling and trustmaking in an uncertain world. *Surveillance and Society, 11*(3), 215–221.

Soleymani, M., Asghari-Esfeden, S., Pantic, M., & Fu, Y. Continuous emotion detection using EEG signals and facial expressions. In Multimedia and Expo (ICME), 2014 IEEE International Conference on, 2014 (pp. 1–6): IEEE**.

Sprokkereef, A., and de Hert, P. (2012). Biometrics, privacy and agency. In Second generation biometrics: The ethical, legal and social context (pp. 81–101). New York: Springer.

Sud, M., & VanSandt, C. (2015). Identity rights: A structural void in inclusive growth. *Journal of Business Ethics, 132*(3), 589–601.

Sutrop, M., & Laas-Mikko, K. (2012). From identity verification to behavior prediction: Ethical implications of second generation biometrics. *Review of Policy Research, 29*(1), 21–36.

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.

Trocchia, P. J., & Ainscough, T. L. (2006). Characterizing consumer concerns about identification technology. *International Journal of Retail and Distribution Management, 34*(8), 609–620.

Ulman, Y. I., Cakar, T., & Yildiz, G. (2015). Ethical issues in neuromarketing: “I Consume, Therefore I am!”. *Science and Engineering Ethics, 21*(5), 1271–1284.

Unar, J., Seng, W. C., & Abbasi, A. (2014). A review of biometric technology along with trends and prospects. *Pattern Recognition, 47*(8), 2673–2688.

Van der Ploeg, I. (2003). Biometrics and privacy: A note on the politics of theorizing technology. *Information, Communication and Society, 6*(1), 85–104.

Wang, C., & Cesar, P. Do we react in the same manner?: Comparing GSR patterns across scenarios. In *Proceedings of the 8th Nordic Conference on Human-Computer Interaction: Fun, Fast, Foundational*, 2014 (pp. 501–510): ACM.

Wang, C., & Cesar, P. The play is a hit: But how can you tell? In *Proceedings of the 2017 ACM SIGCHI Conference on Creativity and Cognition*, 2017 (pp. 336–347): ACM.

Wang, C., Geelhoed, E. N., Stenton, P. P., & Cesar, P. Sensing a live audience. In *Proceedings of the 32nd annual ACM conference on Human factors in computing systems*, 2014 (pp. 1909–1912): ACM.

Wang, C., Wong, J., Zhu, X., Röggla, T., Jansen, J., & Cesar, P. Quantifying audience experience in the wild: Heuristics for developing and deploying a biosensor infrastructure in theaters. In *Quality of Multimedia Experience (QoMEX), 2016 Eighth International Conference on IEEE*, 2016 (pp. 1–6).

Webb, A. M., Wang, C., Kerne, A., & Cesar, P. Distributed liveness: Understanding how new technologies transform performance experiences. In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work and Social Computing*, 2016 (pp. 432–437): ACM.

West, J. P., & Bowman, J. S. (2016). Electronic surveillance at work: An ethical analysis. *Administration and Society, 48*(5), 628–651.

Whitehill, J., Serpell, Z., Lin, Y.-C., Foster, A., & Movellan, J. R. (2014). The faces of engagement: Automatic recognition of student engagementfrom facial expressions. *IEEE Transactions on Affective Computing, 5*(1), 86–98.

Winter, J. S. (2014). Surveillance in ubiquitous network societies: Normative conflicts related to the consumer in-store supermarket experience in the context of the Internet of Things. *Ethics and Information Technology, 16*(1), 27–41.

Winter, S. J., Stylianou, A. C., & Giacalone, R. A. (2004). Individual differences in the acceptability of unethical information technology practices: The case of Machiavellianism and ethical ideology. *Journal of Business Ethics, 54*(3), 273–301.

Zarsky, T. Z. (2017). Incompatible: The GDPR in the age of big data. *Seton Hall Law Review, 47*(4), 995–1020.

Zhao, W., Chellappa, R., Phillips, P. J., & Rosenfeld, A. (2003). Face recognition: A literature survey. *ACM Computing Surveys, 35*(4), 399–458.

Zwitter, A. (2014). Big data ethics. *Big Data and Society, 1*(2), 1–6.

Wickins, J. (2007). The ethics of biometrics: the risk of social exclusion from the widespread use of electronic identification. *Science and Engineering Ethics, 13*(1), 45–54.

Finn, R. L., Wright, D., & Friedewald, M. (2013). Seven types of privacy. In *European data protection: coming of age* (pp. 3–32). Dordrecht: Springer.

Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. *IEEE Transactions on circuits and systems for video technology, 14*(1), 1–29.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.