Journal of Business Research 136 (2021) 52–62

Contents lists available at ScienceDirect

Journal of Business Research

journal homepage: www.elsevier.com/locate/jbusres

Opportunities and challenges of using biometrics for business: Developing a research agenda

Arne De Keyser [a,*], Yakov Bart [b], Xian Gu [c], Stephanie Q. Liu [d], Stacey G. Robinson [e], P. K. Kannan [f]

[a] Department of Marketing, EDHEC Business School, France, 24 Avenue Gustave Delory, CS 50411, 59057 Roubaix Cedex 1, France
[b] D'Amore-McKim School of Business, Northeastern University, 360 Huntington Avenue, Boston, MA 02115, USA
[c] Kelley School of Business, Indiana University, HH2100, 1309 E. 10th St, Bloomington, IN 47405, USA
[d] Consumer Sciences Program, The Ohio State University, 265C Campbell Hall, 1787 Neil Avenue, Columbus, OH 43210, United States
[e] University of Alabama, 132 Alston Hall, Box 870225, Tuscaloosa, AL 35487, USA
[f] Department of Marketing, Robert H. Smith School of Business, University of Maryland, 3445 Van Munching Hall, College Park, MD 20742-1815, USA

ARTICLE INFO

Keywords:
Biometrics
Technology
Ethics
Privacy
Security
AI
Bias

ABSTRACT

Recently, biometric data generated by fingerprints, hand geometry, heart rate, voice patterns, facial characteristics and expressions, brain activity and body movement has increased in both volume and prominence. Surprisingly, academic business literature has remained relatively silent on the immense potential of biometric data, as well as on the various dangers that come with its collection and usage. This article sets out to (1) detail what biometric data entails and how it may be used, (2) describe opportunities associated with using biometric data in various business applications, (3) discuss challenges related to biometric data collection and usage, privacy and security, storage and safety, and potential for reduced inclusiveness and enhanced biases, and (4) outline related directions for future research.

1. Introduction

Practitioners and researchers are increasingly focused on exploring and evaluating biometric data for business purposes. Specifically, the Marketing Science Institute (MSI) lists understanding advances in biometric data, knowing when to employ biometric data, and investigating the ethical implications of such data as a key priority at present and in the immediate future (MSI 2020). The use of biometric data like fingerprints, hand geometry, heart rate, voice patterns, facial characteristics and expressions, brain activity and body movement has exploded in the last few years (eMarketer 2019). The number of devices collecting and processing biometric data is growing rapidly, and includes smart phones capturing fingerprints and face images, voice assistants making use of voice patterns, smart watches processing heartbeat rates, and digital signage systems analyzing face and full body images (Du et al. 2021).

Multiple industries are at the forefront of this rapid adoption of biometric data collection and usage. The transportation industry, for instance, has long used biometric data for airport security, with many airlines now utilizing biometric-based boarding systems. Hotels are adopting facial recognition and fingerprint scanning to optimize check-in procedures and provide room access. In the financial services industry, biometrics have become a vital element of security platforms through biometric checks via the face, fingerprints and finger veins. In a healthcare setting, smart bracelets are used to track heart rate and oxygen levels on a continuous basis; while automotive players use facial and voice analytics to sense driver and passengers' physical state and emotions to adjust vehicle settings (e.g., music, lighting, temperature). In a retail setting, facial analytics and behavioral tracking are implemented to learn about shoppers' preferences, but also for crime prevention (e.g., shoplifting) through detecting and flagging suspicious behavior. In short, the recent collection and use of biometric data across industries signals its increasing importance (see Table 1 for specific use-cases).

With an estimated $35.5 billion global market in 2020 (eMarketer 2019) and widespread adoption of biometric systems across industries, Sheth & Kellstadt (2021) call biometric data one of the next frontiers of research in business and marketing[1]. Despite all this, academic business

* Corresponding author.
E-mail addresses: arne.dekeyser@edhec.edu (A. De Keyser), y.bart@northeastern.edu (Y. Bart), xiangu@iu.edu (X. Gu), liu.6225@osu.edu (S.Q. Liu), sgrobinson@cba.ua.edu (S.G. Robinson), pkannan@umd.edu (P.K. Kannan).

[1] For an overview of non-business biometrics research and the challenges this domain is facing, we refer the reader to Jain et al. (2016).

https://doi.org/10.1016/j.jbusres.2021.07.028
Received 17 December 2020; Received in revised form 9 July 2021; Accepted 11 July 2021
Available online 23 July 2021

Table 1
Selected biometric use cases.

	Organization/*specific software* solution	Description	Biometric data used
Hospitality/Travel	Marriott International	partnership with Alibaba to use facial recognition for guest check-in, room fee charging, automatic deposits to Alipay accounts and room key provision.	facial characteristics
	AlmaHotels	the Alma Barcelona hotel allows room access through fingerprint scanners.	fingerprints
	JetBlue	partnership with U.S. Customs and Border Protection to implement a biometric self-boarding gate using facial recognition.	facial characteristics
	Changi Aiport (Singapore)	implementation of an end-to-end fast and seamless travel (FAST) program using fingerprint and facial recognition.	facial characteristics fingerprints
	Hertz	ability to use fingerprints or face scans (instead of a physical ID) to reduce the time spent on the rental admin process.	facial characteristics fingerprints
	Malibu Poke	Implementation of facial recognition to allow payment through facial recognition, as well as bringing up customers past orders and favorite options in to order process.	facial characteristics
Healthcare	23andMe	genetic testing allowing to trace back ancestry and scan for various medical conditions and health predispositions.	DNA
	Amazon Halo	smart bracelet analyzing body composition, tone of voice, sleep, activity, heart rate, and more to provide behavioral recommendations (e.g., adapted diet, sports) and insights into social well-being via emotion-tracking.	heart rate body composition voice bodily motion body temperature sleep
	Northwell Health	application of iris scanning and facial recognition to register patients to speed up later visits and simplify access to medical records.	iris facial characteristics
	DEEP	biofeedback VR game designed to teaching people emotion regulation techniques through breathing exercises.	breathing
Automotive	Subaru	implementation of the DriverFocus monitoring system to determine if drivers are drowsy or distracted.	facial characteristics eye movement
	B-Secur	application of HeartKey technology relying on EKG monitoring to record a driver's unique heartbeat, usable for authenticating identity and detecting changes in heart rhythm, stress levels, fatigue and respiration.	heart rhythm
	Hyundai	integrated fingerprint scanning lets drivers enter its Santa Fe 2019 model and turn on the ignition without a key.	fingerprints
	Affectiva Automotive AI	in-cabin sensing solution capturing driver and passenger emotions to adjust vehicle settings (e.g., music, lighting, temperature) and routes	facial characteristics bodily movement
Retail	Saks Fifth Avenue	application of facial recognition to identify VIPs and apprehend shoplifters	facial characteristics
	Microsoft Dynamics 365 Connected Store	application making use of cameras and IoT sensors to track customer behaviors and movement within stores	bodily movement facial recognition
	Amazon One	introduction of a biometric device allowing shoppers to pay contactless using their palm in the Amazon Go stores.	hand palm
	CyberLink FaceMe	facial detection solution helping retailers track who enters and leaves a store, calculating time spent in the store, detecting gender, age, mood and head pose to understand customer demographics and behavior.	bodily movement facial characteristics age gender
Financial Services/ Insurances	*Alibaba Dragonfly*	POS devices boosting self-service facial recognition payment technology.	facial characteristics
	Barclay's	implementation of finger vein authentication scans to verify access to online accounts and authorize payments without the need for PIN, passwords or codes.	finger vein
	Sureify	adoption of Ai-powered solution - Lapetus Chronos - allowing to estimate biodemographic information from a selfie to generate an insurance quote, cross-sell products and provide health tips.	facial characteristics age gender body mass index
	John Hancock Vitality	insurance program using fitness and health data collected through smartwatches (e.g., Amazon Halo, Apple Watch) to reward participants for healthy behaviors using a points-based system and adapting insurance pricing accordingly.	heart rate body composition voice bodily motion body temperature sleep
Market Research	Nielsen	adoption of neuroscience technology to complement traditional market research methods and predict individual behavior.	brain activity skin conductance heart rate facial characteristics eye movement

literature (i.e., marketing, management, human resources, operations) has remained relatively quiet on the immense potential of such biometric data (Du et al. 2021), as well as on the various dangers and ethical concerns that come with its collection and usage.

We therefore believe it is critical to start discussing the upsides and potential pitfalls associated with biometric data in business settings, with the ultimate objective of promoting a sustainable and responsible usage of biometric data in both research and practice. The goals of this paper are therefore to: (1) detail what biometric data entails and outline its varied usage, (2) describe the vast business opportunities associated with biometric data, (3) discuss a variety of business challenges and ethical issues related to biometric data collection and usage, privacy and personal security, data storage and safety, and inclusiveness and bias, and (4) put forth several avenues for future research. To achieve these goals, we build on industry and policy insights, trends, and data. It is our hope this work provides a foundation for future academic work on and with biometric data in the business field, while offering practitioners more insights into the implications of biometric data for business strategy and its responsible usage.

2. Biometrics

2.1. A traditional view – Biometric data for identification purposes

From its conception, the biometrics field has focused on measuring individual traits as a way to establish and/or authenticate one's unique identity (Dantcheva et al., 2011; Jain et al., 2011), including biological (e.g., iris, face, fingerprint, DNA), behavioral (e.g., gait, voice) and more recently adhered (e.g., marks, tattoos) traits (Unar et al. 2014). These forms of biometric data provide a natural and reliable solution for establishing and/or authenticating an individual's identity and offer clear benefits compared to possession-based systems (i.e., tokens or security tags may be lost), and knowledge-based authentication systems (i.e., passwords may be forgotten). In essence, biometric data helps establish one-to-one correspondence between an individual and a piece of data and provides reliable evidence of an individual's identity (Bhattacharyya et al., 2009; Byun & Byun, 2013). This is done through Artificial Intelligence (AI)-driven biometric systems that rely on data input by means of dedicated sensors (e.g., fingerprint scanner) and analysis through pattern recognition algorithms (i.e., comparing and matching biometric trait input and stored biometric trait information) (Nait-Ali 2011).

An 'ideal' biometric trait is set to satisfy seven specific requirements – (1) universality (i.e., every individual in a population possesses the trait), (2) distinctiveness (i.e., the trait should sufficiently differentiate one individual from all others), (3) permanence (i.e., the trait should be sufficiently invariant over a period of time), (4) collectability (i.e., the trait should be easy to measure), (5) performance (i.e., the trait can be recognized with high accuracy, speed and robustness) (6) acceptability (i.e., trait measurement should have public acceptance and the device used for measurement should be harmless), and (7) circumvention (i.e., spoofing of the trait should be difficult) (Chan et al., 2018; Jain et al., 2004; 2011). While no single biometric trait fully satisfies all requirements in a real-life setting (Jain et al. 2016), many significantly enhance identity establishing and verification processes (Jain et al. 2011).

Biometric data may be conceptualized on a hard to soft continuum (see Fig. 1). On the one end, 'hard' biometric data entails basic and primary data like fingerprints, DNA and hand geometry that score very high on distinctiveness and permanence (Srinivasa & Gosukonda 2014). Therefore, any application of biometric data involving individual identification/authentication typically makes use of one or more hard biometric traits. Soft biometric data, in turn, represent ancillary traits about the user like age, gender, race, hair color, eye color, weight, and height (Dantcheva et al. 2016). These are often, but not always, derived from hard biometrics (e.g., eye color from iris scanner) (Dantcheva et al. 2011). Soft biometric data are more intuitive for human understanding and labeling– e.g., brown hair, red t-shirt, green eyes (Dantcheva et al. 2011), yet less applicable for the traditional purpose of person identification/authentication. Nonetheless, soft biometric data may provide a wealth of additional information to characterize an individual and are generally less intrusive to collect (Srinivasa & Gosukonda 2014).

2.2. An expanded view – Toward biometric profiling

While the biometrics research field almost exclusively focuses on the usage of biometric data for person identification/authentication, the commercial application of biometric data in combination with AI now allows organizations to build customer/employee profiles along five levels: (1) identification profiling, (2) physical profiling, (3) emotion profiling, (4) behavioral profiling, and (5) cognitive profiling (see Fig. 2).

Identification profiling, which establishes or authenticates the identity of an individual (i.e., who is this person?), remains the dominant use case for biometrics, also in business (Drozdowksi et al., 2020; eMarketer, 2019). Examples of identification profiling entail registering individuals whose identities need to be created biometrically (e.g., registering a user within their smartphone), as well as authenticating an individual to validate a claimed identity (e.g., border control), controlling access to tangible materials or areas (e.g., admittance to restricted areas), and verifying access to data (e.g., admission to a PC, smartphone or IT network) through biometric traits like fingerprints, iris, and retina (Day 2009) and 'hidden' traits like brain activity through tools like EEG (electroencephalography) (Goudiaby et al. 2019).

Physical profiling relates to characterizing and classifying an individual based on biometric data (i.e., what type of person is this?) (Andronikou et al. 2008). Adhered biometric data like gender, age, ethnicity, weight, height, tattoos, and clothing are popular here and used to draw individual inferences and classify individuals (or groups of individuals) into specific cohorts (e.g., age classification). Physical profiling is often used in surveillance applications, since soft biometric data can be obtained at a distance or from low quality footage (Reid et al., 2013; eMarketer, 2019). In addition, physical profiling may also be used to assess an individual's physical condition (e.g., BMI estimation). A recent study by Maor et al. (2020), for instance, demonstrates how voice signal analysis may be used to uncover hidden heart problems without requiring a physical exam.

Emotional profiling, often labeled as affective computing, is focused on the emotional state of an individual (i.e., what is this person feeling?) and is a major area where the use of biometric data is thriving (McStay 2020). People express affect in a variety of ways, including facial expressions, body movement, gestures, and tone of voice (Jones & Troen 2007). This type of biometric data has been used for emotion recognition – albeit recent research questions the ability to which current algorithms are capable of accurately deducing emotions (Barrett et al. 2019).

Behavioral profiling is focused on tracking and coding human behaviors (i.e., what is this person doing?). Behavioral biometric data may, for instance, allow to identify and predict suspicious and criminal activities, such as leaving of objects, fighting, vandalism and looting (Ko 2008). During the Covid-19 pandemic, biometric data has been used to create alerts of non-mask wearing, crowding, people in distress, occupancy analytics and person-to-person proximity to monitor the spread of disease and ensure public safety (Carlaw 2020). Another application of behavioral profiling is activity tracking through wearables (e.g., Apple Watch), where various data points like steps, distance, floors climbed, active minutes, and sleep are registered and analyzed (Piwek et al., 2016).

Finally, cognitive profiling relates to capturing cognitive processes within individuals (i.e., what is the person thinking?) (Verhulst et al. 2019). A popular application is the usage of eye tracking tools to identify attention and assess cognitive effort of consumers walking in retail stores (Wästlund et al. 2015) or looking at advertisements (Pieters et al. 2010). Eye tracking systems allow measuring the position and movement of the eyes, as well as pupil dilation and amount of blinking (Verhulst et al. 2019), making it a perfect tool for exploring cognitive

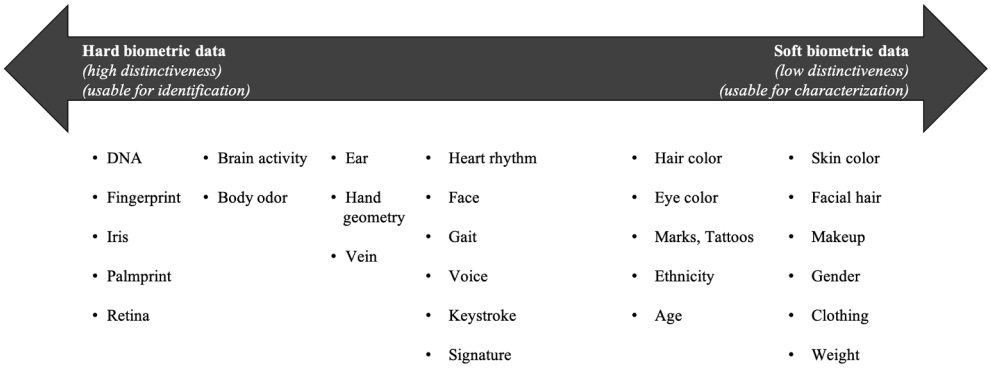

Fig. 1. Biometric Data Continuum. Note: Illustrative positioning of different biometric traits from 'hard' to 'soft'. As new research becomes available and insights update, the position of every biometric trait may change. For specific details on every biometric trait and how it adheres to the seven 'ideal' biometric requirements, we refer the reader to specialized biometrics research

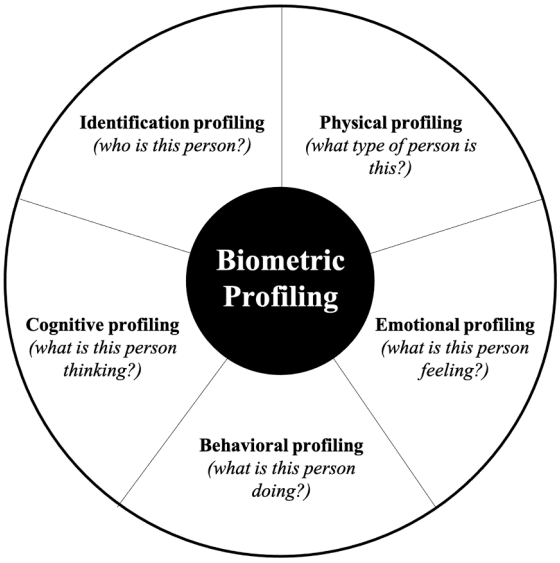

Fig. 2. Biometric Profiling for Business.

processes (Carter & Luke 2020). In addition, cognitive profiling is also used to help predict consumer preferences. The likelihood of movie success, for instance, can be estimated using biometric data collected from audiences watching trailers (Boksem & Smidts 2015).

In sum, the usage of biometric data is evolving rapidly and applied in a variety of ways that go beyond establishing/authenticating one's identity. In fact, many of the popular applications of AI are in large part driven by the growing availability of biometric data – for instance, facial and emotion recognition algorithms would not perform without facial data, while personalized AI-driven training schedules are reliant on smartwatches delivering 24/7 biometric data on heartbeat, sleep patterns, weight, oxygen levels and physical activity. Without such detailed information to help profile individuals, be they customers or employees, even the most advanced algorithm would fail to deliver on its promise. Clearly, biometric data take on a unique position as opposed to traditional sources like survey, experimental, CRM, panel, and clickstream data. The latter sources may suffer from measurement biases (Verhulst et al. 2019), highlight conscious and explicit processes only (Plassmann et al. 2015) or have organizations rely too heavily on easily available data leading to a so-called streetlight effect (Du et al. 2021). Biometric data may help expand business-relevant information extracted from customers and/or employees and inform managers to make better choices to ensure long-term success (Du et al. 2021) and push the further usage of AI.

Given the explosive growth of biometrics in practice, it is imperative business research focuses on the wide applicability and potential of biometric data (Sheth & Kellstadt 2021). As such, in the next sections of the paper we discuss how biometric data may create opportunities in a business setting and conclude with a discussion on the challenges that underlie the sustainable and responsible use of biometric data for business purposes and discern several research avenues. Due to a lack of academic research, we extracted key discussions and topics in this area based on industry research (e.g., eMarketer, 2019; Thales, 2020), public policy documents (e.g., European Data Protection Supervisor, 2020; Wiewiórowski, 2020); industry platform and association (e.g., BiometricsInstitute.org; BiometricUpdate.com) reports, and other practitioner-oriented outlets (e.g., Biometric Technology Today).

3. Biometrics - opportunities

In this section of the paper, we highlight six opportunities the adoption and usage of biometric data holds for business: (1) deepening consumer insights, (2) personalizing the marketing mix, (3) automating the customer journey, (4) strengthening security, (5) enhancing personal health and well-being, and (6) assisting employee hiring, support and management.

3.1. Deepening consumer insights

Biometric data may serve dual purpose in collecting better and more detailed consumer insights. At a basic level, the collection of individual demographic characteristics, like gender and age, may be done unobtrusively, without asking customers to spend effort or time to formulate and transmit information that is relevant to the organization and acquire it without customers' active involvement (Lewinski et al. 2016). Moreover, biometric technologies allow organizations to collect previously hard-to-collect information like a customer's height, emotional state, movement and other behaviors in a retail space. All this may be of significant help for marketing research purposes such as customer segmentation, profiling and behavioral predictions (Du et al. 2021), as well as to optimize store layout and enhance environmental safety (Lewinski et al. 2016). Note this covert manner of data collection also raises several concerns around privacy and permission which we discuss in Section 4 of the paper.

Taking consumer insights to a next level, biometric data delivers a level of customer understanding previously unattainable with traditional research methods (Kumar et al., 2013; Plassmann et al., 2015). Especially relevant here is the fast-growing application of the neuroscientific method to study affective processes, decision making, memory and attention (Plassmann et al. 2012). Adopting the neuroscientific method helps reduce several typical research problematics such as social

desirability, nonresponse, and common method bias which are inherent to traditional marketing research and allowing real-time observation of internal processes (Verhulst et al. 2019). Danish entertainment company Nordisk Film, for instance, makes use of galvanic skin response testing to screen movie trailers and understand consumers' emotional responses (iMotions 2020), moving beyond simple (and often limited) survey-based research methods.

3.2. Personalizing the marketing mix

As organizations capture and utilize biometric data to collect real-time information and develop more accurate, in-depth profiles of customers, they can provide customers with a more individualized experience. The use of biometrics may be an important differentiating factor in light of the strong shift toward personalized marketing efforts that tailor the marketing mix to individual customers (Bleier et al. 2018). The key benefit here is that offerings provide increased personal relevance and are designed to enhance the customer experience (De Keyser et al. 2020).

For instance, hospitality industry observers suggest that hotel frontline employees could use facial recognition in combination with augmented reality technology to identify customers before they arrive at the front/concierge desk, allowing employees to quickly review customer profiles and provide personalized greetings (Revfine 2020). In another application, car manufacturer Kia is rolling out R.E.A.D (Real-time Emotion Adaptive Driving) system that deciphers drivers' emotions through facial expressions and heartbeat, and creates a personalized driver's space adapting lighting, sound, cabin temperature, seat vibration and scent (Kia 2019). Insurers are also using biometrics to personalize life insurance policies and save costs through tracking biometrics that help assess health conditions (e.g., smoking-related ailments), fitness (e.g., level of daily exercise) and individual differences (e.g., age, gender, body mass index). John Hancock's Vitality program, for instance, collects fitness and health data through their clients' smartwatches (e.g., Amazon Halo, Apple Watch), which allows the company to reward clients for healthy behaviors using a points-based system and personalize insurance pricing accordingly.

3.3. Automating the customer journey

Biometric data may offer several opportunities to smoothen or even automate service processes. For organizations, the result is more cost-effective service, while maintaining high quality standards (Wirtz & Zeithaml 2018). For customers, biometric automation leads to increased convenience levels to interact with organizations across various touchpoints in the customer journey, which matches the strategic imperative of many organizations today to invest in the creation of seamless customer journeys (Lemon & Verhoef, 2016; De Keyser et al., 2020). The key goal is to make customers' lives simpler and hassle-free (Kumar et al. 2021).

An important application here is that of biometric-based entry, with customers gaining access to a physical/online space (e.g., car, lounge, banking app) by authentication through biometric data like fingerprints or one's face. Compared to traditional methods such as using physical keys, ID cards, passwords or PINs, biometrics allow customers to unlock a door without having to look for a key, pull out a card, or type in a code—weaving a sense of convenience, speed and coolness into the customer journey (Liu & Mattila 2019). In the lodging industry, for instance, Marriott International and Alibaba Group partnered to roll out facial recognition check-in kiosks in China, where guests can scan their faces to check in and bypass the lengthy queues at the front desk, reducing check-in times to as short as one minute (Wang 2018).

Payments are another aspect of the customer journey greatly enhanced through biometrics (Liu & Mattila, 2019; Ogbanufe & Kim, 2018). Besides the ubiquitous availability of smartphone contactless payment systems relying on facial and fingerprinting biometrics, a growing number of retailers are experimenting with direct biometric payments as well. For example, KFC China has introduced the "Smile to Pay" program, where customers can scan their faces to order meals on a touchscreen with 3D camera and facial recognition software (Gilchrist 2017).

3.4. Strengthening security

Biometrics may be used to mitigate identity theft and fraud and are increasingly used as an initial layer of protection (e.g., smartphone access through one's fingerprint) or as part of a multi-layered authentication solution (e.g., combination of pin-code and fingerprint) to help overcome the typical safety issues with passwords and PIN codes (Hung 2017). Today, traditional passwords account for most data breaches (Sudhakar & Gravrilova 2020), which explains why an increasing number of organizations are turning toward biometric solutions – both aimed at securing internal (i.e., employee) and external (i.e., customer) access to specific services and information. Market research suggests over 80% of customers prefer biometric authentication methods over passwords (King 2018), while a recent survey with mobile finance app users found that 34% of millennials and 36% of Gen X customers would like to see biometrics on their apps to enhance the security of financial transactions (Beer 2019).

Visa, for example, launched the "Visa Ready for Biometrics" program to enable client banks to incorporate voice, eye, fingerprint, and face authentication into their mobile apps. Mastercard has partnered with Apple and Goldman Sachs to design and launch Apple Card that enables customers to authenticate transactions through Apple Touch ID or Face ID. Besides biometric-infused mobile apps, voice authentication (e.g., Citi), facial recognition (e.g., ATMs at Caixabank and China Merchants Bank), and finger vein scanners (e.g., Barclays) have been adopted by banks around the globe for advanced security. In the hospitality industry, the application of biometric data develops in a similar manner. The Nine Zero hotel in Boston, for instance, has installed iris recognition systems to identify guests for upscale suites (Bergstein 2004), while the Borgata Hotel Casino and Spa in Atlantic City uses facial recognition systems to identify dysfunctional and unwelcomed guests and cheaters (Littleton 2003).

3.5. Enhancing personal health and well-being

With biometric data being tracked by smartphones and wearables, today's consumers are offered plenty of opportunities to monitor and improve their health and wellbeing on a continuous basis (Shin et al. 2019). Through tracking individual health indicators – heartbeat, daily movement, sleep patterns – customers may develop and maintain a series of wellness habits, and receive guidance based on their own data patterns. Moreover, changes of the body may be discerned early on, resulting in timely alerts to users and their physicians linked to immediate recommended actions and better disease prevention and treatment. While activity levels of individuals may be impacted positively, it is worth noting quantification may hinder an individual's enjoyment of activities being tracked through impeding intrinsic motivation (Etkin 2016).

One example here is Amazon's Hale bracelet and connected app. The key goals of this setup are providing a comprehensive understanding of users' health and wellness, as well as tools to take actions for improvement. Specifically, the Halo offering is built around five core features – activity (e.g., tracking of movement, sports activities), sleep (e.g., tracking of in-sleep heartbeat, sleep time, sleep temperature), body (e.g., tracking of weight, BMI), tone (e.g., tracking of voice patterns to analyze social and emotional well-being), and labs (i.e., challenges, experiments and workouts to build healthier habits) that are combined into an integrated health platform (Amazon 2020). Similarly, the automobile industry is investing heavily in driver well-being. Nissan's ProPilot and Subaru's DriverFocus monitoring systems use sensors, eye tracking and facial recognition to prevent driver distraction and fatigue through alerts and auto-corrections. Toyota has been working on AI technology that monitors the driver's feelings of distress or agitation through analyzing facial expressions and tone of voice.

Equally, employee well-being may be informed by biometric monitoring. Stress and anxiety, for instance, can be measured with wearables allowing firms to gain valuable information regarding an employee's emotional state and to intervene where needed (Chamorro-Premuzic and Bailie 2021). On a more advanced level, biometric data may even transform people analytics through biometric data driven insights and thus change the HR function as we will discuss in the next paragraphs.

3.6. Supporting employee hiring, support, and management

The use of biometrics may help innovate employee hiring, support and management practices. Similar to building more accurate profiles of customers, biometric data may be used to enhance insights about present and potential employees. Biometrics may prove useful in the hiring process through the adoption of a so-called "biometric resume," where potential candidates can be assessed by a physical, behavioral and emotional profile (van Esch et al. 2020). Biometric input may also support frontline employees to enhance their performance (De Keyser et al. 2019). Henkel et al. (2020), for instance, find that augmenting call center employees with AI emotion recognition software enables more effective interpersonal emotion regulation, and has a subsequent positive impact on employees' affective well-being. In addition, the tracking of biometrics on the job may also enhance performance through delivering real-time feedback on employee behaviors.

People analytics software provider Humanyze, for instance, developed a smart I.D. card to track activity in the workspace including employee motion, talking, and the frequency and duration of in-person interactions. In a project with a large financial institution, data patterns revealed that simply allowing call center workers to take a break together, rather than in shifts, lowered stress levels as indicated by voice patterns captured by employee badges, and employee satisfaction surveys. This resulted in higher employee happiness, and lower turnover rates (Heath 2016). McDonald's franchises in Japan went a step further using facial recognition to evaluate the quality of the customer service provided by employees (Prakash 2018). If an employee doesn't smile enough, they receive a system alert indicating their performance is below standard. And CallMiner developed AI-driven software that tracks call center employees' voice patterns and speech to rate professionalism, politeness, and empathy, allowing to identify working points and provide coaching. While these examples show how biometric data, in combination with AI, can be used for HR practices, we note it should be used in a responsible manner as it may put significant strain on employees – which we will discuss in the next section.

4. Toward a responsible implementation of biometrics – A research agenda

So far, this paper discussed the wide range of opportunities biometric data offers in a business environment. Yet, the collection and usage of biometric data is not self-evident and comes with various challenges and risks that need to be addressed. Moreover, there is growing criticism and debate on the role biometric data may and should play in society at large, as it represents information previously difficult or impossible to access (Verhulst et al. 2019). Biometric data is very often sensitive and highly personal in nature, and potentially biased toward some population groups (Castelvecchi 2020). Therefore, it is critical that organizations (and their employees and customers) recognize while biometric data may lead to valuable outcomes, it also hold great potential for misuse, manipulation and exploitation of (vulnerable) individuals. In an attempt to highlight the importance of responsible and "better" business practices (see Moorman 2018), we consider some of the key challenges the biometrics realm is facing in relation to (1) data collection and usage, (2) privacy and personal security, (3) data storage and safety, and (4) inclusiveness and bias. While outlining each of these challenges, we also identify several key questions that need to be addressed by future research and practice (for an overview – see Table 2).

4.1. Data collection & usage

A first consideration relates to the impact biometric data collection may have on individuals – be that in a customer or employee role. Whereas many biometrics traits may be easily collected without active (and/or willing) participation of an individual through the use of cameras or hidden sensors, the collectability and acceptability of specific biometric traits like DNA, eye movement and brain activity may pose significant challenges (Jain et al., 2004; Verhulst et al., 2019). Biometric data collection may necessitate a certain level of invasiveness (e.g., wearing an eye tracker or donating a blood/saliva sample) for participants that needs to be managed ethically requiring clear consent of the individual(s) involved (Verhulst et al. 2019). Given that the use of biometric data may be unclear to individuals, leading to confusion or even a significant underestimation of the potential and risk the collection and usage of biometric holds, it is critical to work on a clear frame that aids individuals in understanding when biometric data is collected and how this data is being used, moving beyond often-ignored and confusing terms of use (Obar & Oeldorf-Hirsch 2020). Therefore,

Table 2
Future Research Opportunities.

Research Area	Research Avenues
Data collection & usage	■ How does the collection of the various biometric traits impact individuals? What biometric data is more or less acceptable for business purposes? ■ How can organizations minimize the invasiveness of biometric data collection, without foregoing informed consent and responsible usage? ■ What is the best way to inform individuals about biometric collection and usage while ensuring comprehension? ■ How can organizations mitigate biometric error and its potentially adverse impact on individuals? ■ How can organizations track and account for inherent changes in individuals' biometric traits longitudinally? ■ How does inaccurate interpretation of biometric data impact the customers/employee-organization relationship?
Privacy & personal security	■ In what ways does the covert (vs overt) collection of biometric data impact individuals? ■ When are customers/employees willing to give organizations permission to collect biometric data? What trade-offs come into play when weighing privacy concerns and enhanced offering relevance? ■ How does the implementation of privacy regulation impact the intention to adopt biometric-based offerings/systems? ■ To what extent does privacy regulation help overcome privacy concerns related to biometric data? ■ What benchmarks might support the design, development and deployment of responsible biometric applications?
Data storage & safety	■ To what extent do biometric-related data breaches impact organizations more negatively compared to 'conventional' data breaches (e.g., passwords)? ■ To what extent may cancelable biometric data help mitigate privacy concerns? ■ Does the personal nature of biometric data necessitate higher levels of trust in the organization/relationship partner collecting and/or using it? ■ To what extent does providing third parties (e.g., governmental agencies) access to biometric data impact customer/employee concerns and their willingness to provide data?
Inclusiveness & bias	■ What is the impact of bias in biometric applications on customer, employees, and organizations? ■ How can organizations make biometric applications more inclusive? And avoid bias?

RQ1: How does the collection of the various biometric traits impact individuals? What biometric data is more or less acceptable for business purposes?

RQ2: How can organizations minimize the invasiveness of biometric data collection, without foregoing informed consent and responsible usage?

RQ3: What is the best way to inform individuals about biometric collection and usage while ensuring comprehension?

Furthermore, the reliability of biometric sensors, devices and algorithms may be troublesome at times given that biometric systems are complex and inherently probabilistic (Pato & Millett 2010). While the collection of some biometric data may be short (e.g., fingerprint scan), other data may be tracked continuously and thus require sustained monitoring devices connected to an individual (e.g., heart rate patterns via smart bracelets). Relatedly, biometric traits in the form of voice, facial features, typing patterns and physical movements may change over time naturally (e.g., age) or artificially (e.g., plastic surgery) (Jain et al. 2016), while external factors like humidity, cold, and heath may hinder the biometric recognition system. Therefore,

RQ4: How can organizations mitigate biometric error and its potentially adverse impact on individuals?

RQ5: How can organizations track and account for inherent changes in individuals' biometric traits longitudinally?

The usage of biometric applications may also (still) be overpromising (Chen 2019), especially with regard to emotion recognition – an industry estimated to grow to US$37 billion by 2026 (Crawford 2021). Research by Barrett et al. (2019) concludes that it is very hard to use facial expressions alone to accurately predict how someone is feeling. The reliability of data representing expressions of anger, disgust, fear, happiness, sadness and surprise have been questioned. At present, it is not possible to confidently deduce happiness from at the display of a smile, or sadness from a frown. Facial expressions of emotion vary significantly across contexts and cultures. This suggests at present, many tech companies may be more in the business of detecting facial movement, rather than emotion recognition (Barrett et al., 2019; Chen, 2019). Moreover, testimonials from employees working in call centers report AI-driven analyses of biometric data like one's voice patterns and speech are rather clumsy, failing to capture small nuances and understand specific contextual factors at play. One example of such a failure is an exchange between customer and employee flagged for review due to misinterpreted biometric data. Specifically, a call center employee was incorrectly instructed to repeatedly apologize to a customer who was laughing with joy over the birth of a child. However, the firm's AI sounded an "empathy alarm" due to mischaracterizing the customer's affect (Dzieza 2020). This raises questions as to the impact the usage of emotion recognition technologies has on the customer/employee-organization relationship and how accurate measurements reflect reality. If organizations misread customer or employee emotions, it may lead to unnecessary stress and negative customer and employee experiences. Therefore,

RQ6: How does inaccurate interpretation of biometric data impact the customers/employee-organization relationship?

4.2. Privacy & personal security

Given the personal nature of biometric data and its potential to uniquely identify individuals, it holds great value to organizations. The personal nature of biometric data and the ability to collect such data without consent or permission is of increasing concern as biometric data such as gender, ethnicity, facial expressions, weight, and height may be captured covertly. Moreover, this data could be connected to publicly available data on social network sites such as Facebook, Twitter, and Instagram – which all make use of profile pictures – to gather detailed information on individuals. Such covert collection and usage are a major threat to the privacy and the power of individuals to control their private data and may significantly hurt individuals' trust in an organization when such practices surface. There may even be situations in which avoiding biometric data collection is (nearly) impossible such as border control and camera-based security systems in stores and outdoor streets.

Aguirre et al. (2015) find that the usage of covertly collected data for ad personalization heightens consumers' perceived vulnerability compared to ads based on overtly collected information. Moreover, individuals increasingly turn to privacy notices on websites (Awad & Krishnan, 2006), and may even be willing to pay a premium from websites that disclose their privacy policies (Tsai et al., 2011). When data usage goes beyond accepted norms and/or individuals figure out their data has been collected and used without their knowledge, they may have concerns and feel their privacy is being violated (Bleier et al. 2020). Taken together, we posit:

RQ7: In what ways does the covert (vs overt) collection of biometric data impact individuals?

RQ8: What are the best ways to overcome biometric-related privacy concerns?

As previously discussed, biometric data may also lead to offerings having higher relevance for individuals through personalization, enhanced security, and improved convenience. Given the growing adoption of wearables and related biometric data providing insights into an individual's daily life and biometric driven feedback on improving well-being, it is clear that many individuals are willing to share personal data if they perceive the value provided is worth the risks of sharing personal data. Therefore,

RQ9: When are customers/employees willing to give organizations permission to collect biometric data? What trade-offs come into play when weighing privacy concerns and enhanced offering relevance?

In relation to privacy and personal security, customers and employees may also be looking to lawmakers to help regulate the biometric data collection, storage and usage (Bleier et al. 2020), which may ultimately help overcome concerns (Milberg et al. 2000). This is especially important as several technology giants have been connected to violating data protection laws, and sometimes operate in grey zones (Daviet et al. 2021). Europe's "General Data Protection Regulation" (GDPR) represents one of the first legal frameworks addressing the topic of biometrics. Under article 4 of the GDPR, biometric data is considered as sensitive personal data, whereas article 9 prohibits the processing of such data with the exception of explicit consent of the natural person behind the data, among others. Organizations processing this data, in turn, must perform a data protection impact assessment (DPIA), including a description of how the data is processed, an assessment of its necessity, an assessment of the right and freedoms of the individual behind the data, and what measures and safeguards are taken to uphold those rights (McDowell 2019). A key aspect of the GDPR is the fundamental right individuals have to revoke consent given to organizations. In other words, individuals hold the right to be 'forgotten'. In the U.S., at the time of writing, a majority of states allows software to identify individuals using images taken without their consent in public areas, with the exception of New York (i.e., SHIELD act), California (i.e., California Consumer Privacy Act), Washington, Illinois (i.e., Biometric Information Privacy Act), and Texas where it is banned for commercial use. The increasing complexity of biometric technologies, however, may give rise to a knowledge gap between parties developing and deploying the technologies and parties like civil society, regulators, and independent advocates needed to ensure this happens in a responsible and accountable way (Snijder 2016). More precisely, there is potential risk that lawmakers, data protection authorities, and relevant legal frameworks may not match technological progress, making the assessment of risks more difficult. Therefore,

RQ10: How does the implementation of privacy regulation impact the intention to adopt biometric-based offerings/systems?

RQ11: To what extent does privacy regulation help overcome privacy concerns related to biometric data?

Finally, while biometric applications provide organizations and society with many benefits, the association of biometric data with an individual, and the ability for this data to be detected remotely, without consent, and their lifelong connection with identity records raise

numerous social, cultural, and legal concerns. These issues will most certainly affect biometrics' user acceptance and performance. Biometric data usage raises severe concerns on authority and remediation, reliability and privacy. Ultimately, these factors are critical and should be considered in the design, development, and deployment of any biometric application. Therefore,

RQ12: What benchmarks might support the design, development and deployment of responsible biometric applications?

4.3. Data storage & safety

To further address the fundamental privacy and security challenges, safe storage of biometric data is of key importance to individuals and organizations (Snijder 2016). Organizations that collect and store customers' and/or employees' personal data are under constant threat from hackers as this data is highly valuable for misconduct. The irreplaceable nature of biometric data necessitates organizations to treat such data with increased security and caution in order to stay ahead of fraud advancements – something both expensive and technically difficult. If a password or pin is compromised, there is always the option of changing it. The same cannot be said for a person's biometric data. Specifically, unlike other forms of data such as user identifications and passwords, if a biometric database containing fingerprints, iris scans, and palm scans gets compromised, this biometric data cannot be cancelled, changed or re-issued as it is mostly inherent and unique to an individual.

Therefore, security breaches of databases containing biometrics are potentially more of a concern than other types of customer data as the damage to customers/employees could be irreversible. This may result in customers/employees choosing to not patronize organizations that cannot secure their personal data, which may have a direct negative impact on an organization's value and attractiveness (Janakiraman et al. 2018). This is because in addition to direct loss in revenue, there is risk of litigation as consumer groups and labor unions may take legal action against the organizations. All of which may make customers/employees think twice about sharing their biometric data with organizations and questioning the security of their data. Therefore, research looks into so-called cancelable biometric data (Patel et al. 2015). The latter is distorted on purpose, making that the original biometric data is never used, and the distorted biometric data may be cancelled or revoked. Taken together, we posit the following

RQ13: To what extent do biometric-related data breaches impact organizations more negatively compared to 'conventional' data breaches (e.g., passwords)?

RQ14: To what extent may cancelable biometric data help mitigate privacy concerns?

As with any form of personally identifiable data, there are supplementary concerns of data security that customers/employees may experience (Wierenga et al. 2021). Is biometric data totally under the control of the organization? Who else has access to the data? Is it securely stored? Additionally, customers face the challenge of whether they can fully trust the organization to whom they give their data to, and more recently also wondering about the foreclosure of data and access by governmental agencies (Bleier et al. 2020).

Therefore,

RQ15: Does the personal nature of biometric data necessitate higher levels of trust in the organization/relationship partner collecting and/or using it?

RQ16: To what extent does providing third parties (e.g., governmental agencies) access to biometric data impact customer/employee concerns and their willingness to provide data?

4.4. Inclusiveness & bias

While the biometrics field has advanced and expanded rapidly in recent years, biometric usability has been somewhat under researched and discussions about the inclusivity of biometric applications have been overlooked (Jain et al. 2016). The few studies on this topic offer significant evidence that people with disabilities in fact experience more challenges and display higher levels of anxiousness and nervousness about biometric applications (Parsheera 2020). Movement-impaired individuals or individuals with an amputation may experience difficulties using fingerprint scanners, iris scanners may pose challenges for visually impaired people, while people with cognitive disabilities may have difficulties with speaker recognition (Blanco-Gonzalo et al. 2018; Pasheera 2020).

In addition, there is a growing concern and debate around inherent racial and gender bias underlying facial recognition technology (Castelvecchi 2020), especially in the context of law enforcement. While biometric technology may be viewed as being impartial or neutral because of its non-human nature, it is not free from bias or failure and is likely to "transform every sector of society and touch every civil right we enjoy" (Fussell 2020). Most facial recognition packages today tend to be more accurate for white, male faces than for people of color or for women (Buolamwini & Gebru 2018). A study by the US National Institute of Standards and Technology (NIST), for instance, showed faces classified in NIST's database as African American or Asian were 10 to 100 times more likely to be misidentified compared to individuals classified as white (Grother et al. 2019). While the same study reports current technology is greatly improving, it is clear error in biometric recognition may have severe consequences for any individual, ranging from unwarranted or denied access to specific data to being wrongfully accused of crimes based on an erroneous misidentification (Buolamwini & Gebru 2018). Much of this error is caused by the algorithmic discrimination through training with biased data (Castvelvecchi, 2020) and will thus require further addressing.

Taken together, if the use of biometrics – especially in the area of individual authentication/identification – increasingly becomes standard across a wide range of services, several groups like people with physical or learning disability, elderly, and people of minority race or religion may increasingly face social exclusion and be faced with an unethical lack of equity. Therefore,

RQ17: What is the impact of bias in biometric applications on customer, employees, and organizations?

RQ18: How can organizations make biometric applications more inclusive? And avoid bias?

5. Conclusion

Given the striking lack of attention to the use of biometrics in the academic business literature, we relied on multi-sector industry and government insights and trends to examine various forms of biometric data and described how it is utilized (i.e., identification profiling, physical profiling, emotional profiling, behavioral profiling, cognitive profiling), outlined the opportunities biometric data offers in a business environment (i.e., deepening consumer insights, personalizing the marketing mix, automating the customer journey, strengthening security, enhancing personal health and well-being, and supporting employee hiring, support and management), discussed the challenges that come with biometric data collection and usage, privacy and personal security, data storage and safety, and inclusiveness and bias, and outlined several avenues for future research.

Taken together, we believe there are a great number of promising applications of biometric data that may strengthen organizational practices and improve the lives of customers and employees. However, many challenges must first be addressed to make sure biometric data is not used inappropriately or discriminates against certain groups. The recently published guidelines by the Biometrics Institute, the industry's leading representative body, may offer an initial starting point on how to best utilize biometric data: **(1)** Policy: the use of biometrics is proportionate, with basic human rights, ethics and privacy at its heart, **(2)** Process: safeguards are in place to ensure decisions are rigorously reviewed, operations are fair and operators are accountable, and **(3)** Technology: Know the algorithm, biometric system, data quality and

operating environment and mitigate vulnerabilities, limitations and risks (Biometrics Institute 2020). As business practitioners and scholars, we should always strive for the responsible and inclusive usage of biometric data, following high-level ethical standards. Taken together, we urge future research to empirically explore the challenges the biometrics field is facing and formulate clear recommendations for business scholars and practitioners working with biometric data. Given the nature of biometric data and the various challenges it brings, a multidisciplinary approach may be the best way forward.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgment

The authors would like to thank Lerzan Aksoy and Jay Kandampully for setting up this special issue and their valuable guidance throughout the entire review process.

References

Andronikou, V., Yannopoulos, A., & Varvarigou, T. (2008). Biometric profiling: Opportunities and risks. In M. Hildebrandt, & S. Gutwirth (Eds.), *Profiling the European citizen* (pp. 131–145). Springer.

Aguirre, E., Mahr, D., Grewal, D., de Ruyter, K., & Wetzels, M. (2015). Unraveling the personalization paradox: The effects of information collection and trust-building strategies on online advertisement effectiveness. *Journal of Retailing, 91*(1), 34–49.

Amazon (2020). Introducing Amazon Halo and Amazon Halo Band – A New Service that Helps Customers Improve Their Health and Wellness. Retrieved from https://press.aboutamazon.com/news-releases/news-release-details/introducing-amazon-halo-and-amazon-halo-band-new-service-helps..

Awad, N. F., & Krishnan, M. S. (2006). The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS Quarterly, 30*(1), 13–28.

Barrett, L. F., Adolps, R., Marsella, S., Martinez, A. M., & Pollak, S. D. (2019). Emotional expressions reconsidered: Challenges to inferring emotion from human facial movements. *Psychological Science in the Public Interest, 20*, 1–68.

Beer, C. (2019). What Consumers Want From Banks in 2019 and Beyond. Retrieved from https://blog.globalwebindex.com/chart-of-the-week/consumer-banking-trends-2019/.

Bergstein, B. (2004). Biometric technology getting more use in consumer areas. Retrieved from https://www.semissourian.com/story/144036.html.

Bhattacharyya, D., Ranjan, R., a, F. A., & Choi, M. (2009). Biometric Authentication : A Review. International Journal of Service, Science and Technology, 2(3), 13–28.

Biometrics Institute (2020). The Three Laws of Biometrics. Retrieved from https://www.biometricsinstitute.org/the-three-laws-of-biometrics/.

Blanco-Gonzalo, R., Lunerti, C., Sanchez-Reillo, R., & Guest, R. M. (2018). Biometrics: Accessibility challenge or opportunity? *PLoS ONE, 13*(4).

Bleier, A., De Keyser, A., & Verleye, K. (2018). Customer engagement through personalization and customization. In R. W. Palmatier, V. Kumar, & C. M. Harmeling (Eds.), *Customer Engagement Marketing* (pp. 75–94). Palgrave Macmillan.

Bleier, A., Goldfarb, A., & Tucker, C. (2020). Consumer privacy and the future of data-based innovation and marketing. *International Journal of Research in Marketing, 37*(3), 466–480.

Boksem, M. A. S., & Smidts, A. (2015). Brain Responses to Movie Trailers Predict Individual Preferences for Movies and Their Population-Wide Commercial Success. *Journal of Marketing Research, 52*(4), 482–492.

Buolamwini, J., & Gebru, T. (2018). Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. *Proceedings of Machine Learning Research, 81*(1), 1–15.

Byun, S., & Byun, S. E. (2013). Exploring perceptions toward biometric technology in service encounters: A comparison of current users and potential adopters. *Behaviour and Information Technology, 32*(3), 217–230.

Carlaw, S. (2020). Impact on biometrics of Covid-19. Biometric Technology Today, 2020 (4), 8–9. 3.

Carter, B. T., & Luke, S. G. (2020). Best practices in eye tracking research. *International Journal of Psychophysiology, 155*(May), 49–62.

Castvelvecchi,. (2020). Beating Biometric Bias. *Nature, 587*, 347–349.

Chamorro-Premuzic, T. & Bailie, I. (2020). Tech is transforming people analytics. Is that a good thing? Retrieved from https://hbr.org/2020/10/tech-is-transforming-people-analytics-is-that-a-good-thing.

Chan, H. L., Kuo, P. C., Cheng, C. Y., & Chen, Y. S. (2018). Challenges and Future Perspectives on Electroencephalogram-Based Biometrics in Person Recognition. *Frontiers in Neuroinformatics, 12*(October), 1–15.

Chen, A. (2019). Computers can't tell if you're happy when you smile. Retrieved from https://www.technologyreview.com/2019/07/26/238782/emotion-recognition-technology-artifical-intelligence-inaccurate-psychology/#:~:text=Emotion%20recognition%20is%20set%20to,popular%20method%20is%20deeply%20flawed.

Crawford, K. (2021). Time to regulate AI that interprets human emotions. *Nature, 592*, 167.

Dantcheva, A., Elia, P., & Arun, R. (2016). What else does your biometric data reveal? A survey on soft biometrics. *IEEE Transactions on Information Forensics and Security, 11*(3), 441–467.

Dantcheva, A., Velardo, C., D'Angelo, A., & Dugelay, J. L. (2011). Bag of soft biometrics for person identification: New trends and challenges. *Multimedia Tools and Applications, 51*(2), 739–777.

Daviet, R., Nave, G., & Wind, J. (2021). Genetic Data: Potential Uses and Misuses in Marketing. *Journal of Marketing, forthcoming.*

Day, . (2009). Biometric Applications, Overview. In S. Z. Li, & A. Jain (Eds.), *Encyclopedia of Biometrics*. Springer.

De Keyser, A., Köcher, S., Alkire, L., Verbeeck, C., & Kandampully, J. (2019). Frontline Service Technology infusion: Conceptual archetypes and future research directions infusion. *Journal of Service Management, 30*(1), 156–183.

De Keyser, A., Verleye, K., Lemon, K. N., Keiningham, T. L., & Klaus, P. (2020). Moving the Customer Experience Field Forward: Introducing the Touchpoints, Context, Qualities (TCQ) Nomenclature. *Journal of Service Research, 23*(4), 433–455.

Drozdowksi, P., Rathgeb, C., Dantcheva, A., Damer, N., & Busch, C. (2020). Demographic bias in biometrics: A survey on an emerging challenge. *IEEE Transactions on Technology and Society, 1*(2), 89–103.

Du, R. Y., Netzer, O., Schweidel, D. A., & Mitra, D. (2021). Capturing Marketing Information to Fuel Growth. *Journal of Marketing, 85*(1), 163–183.

Dzieza, J. (2020). How hard will robots make us work? Retrieved from https://www.theverge.com/2020/2/27/21155254/automation-robots-unemployment-jobs-vs-human-google-amazon?fbclid=IwAR30wsRkDzg2xTGEBAX5GNI3UeG_9XWH4H0gQh5D80PkUz9T3AlZKzWBjTE.

eMarketer (2019). Biometric Marketing 2019 - Revolutionary Personalization Tool or Targeting Gone Awry.

Etkin, J. (2016). The hidden cost of personal quantification. *Journal of Consumer Research, 42*(6), 967–984.

European Data Protection Supervisor (2020). 14 misunderstandings with regard to biometric identification and authentication. Retrieved from https://edps.europa.eu/sites/default/files/publication/joint_paper_14_misunderstandings_with_regard_to_identification_and_auuthentication_en.pdf.

Fussell, S. (2020). This Film Examines the Biases in the Code That Runs Our Lives. Retrieved from https://www.wired.com/story/film-examines-biases-code-runs-our-lives/.

Gilchrist, K. (2017). Alibaba launches 'smile to pay' facial recognition system at KFC in China. Retrieved from https://www.cnbc.com/2017/09/04/alibaba-launches-smile-to-pay-facial-recognition-system-at-kfc-china.html.

Goudiaby, B., Othmani, A., & Nait-ali, A. (2019). EEG Biometrics for Person Verification. In A. Nait-ali (Ed.), *Hidden Biometrics* (pp. 45–69). Springer.

Grother, P., Ngan, M., Hanaoka, K. (2019). Face Recognition Vendor Test (FRVT) - Part 2: Identification. Retrieved from https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8271.pdf.c.

Heath, T. (2016). This employee ID badge monitors and listens to you at work - except in the bathroom. Retrieved from https://www.washingtonpost.com/news/business/wp/2016/09/07/this-employee-badge-knows-not-only-where-you-are-but-whether-you-are-talking-to-your-co-workers/.

Henkel, A. P., Bromuri, S., Iren, D., & Urovi, V. (2020). Half human, half machine – augmenting service employees with AI for interpersonal emotion regulation. *Journal of Service Management, 31*(2), 247–265.

Hung, T. (2017). Shifting shape of banking biometrics. *Biometric Technology Today, 4*, 5–8.

iMotions (2020), Enabling Emotion-Driven Audience Insights for Movie Trailers. Retrieved from https://imotions.com/cases/nordisk-film/.

Jain, A. K., Nandakumar, K., & Ross, A. (2016). 50 years of biometric research: Accomplishements, challenges and opportunities. *Pattern Recognition Letters, 79*, 80–105.

Jain, A. K., Ross, A., & Nandakumar, K. (2011). *Introduction to biometrics*. Springer (US).

Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to Bbiometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology, 14*(1), 4–20.

Janakiraman, R., Lim, J. H., & Rishika, R. (2018). The effect of a data breach announcement on customer behavior: Evidence from a multichannel retailer. *Journal of Marketing, 82*(2), 85–105.

Jones, C. M., & Troen, T. (2007). Biometric valence and arousal recognition. *Australasian Computer-Human Interaction Conference, OZCHI'07*, 191–194.

Kia (2019). Amplify Your Jory with Emotive Driving. Retrieved https://pr.kia.com/en/future/future/emotive-driving-ces.do.

King, R. (2018). Multiple surveys find acceptance of biometrics by U.S., U.K. consumers mixed. Retrieved from https://www.biometricupdate.com/201802/multiple-surveys-find-acceptance-of-biometrics-by-u-s-u-k-consumers-mixed.

Ko, T. (2008). A survey on behavior analysis in video surveillance for homeland security applications. Proceedings - Applied Imagery Pattern Recognition. *Workshop.*

Kumar, V., Chattaraman, V., Neghina, C., Skiera, B., Aksoy, L., Buoye, A., & Henseler, J. (2013). Data-driven services marketing in a connected world. *Journal of Service Management, 24*(3), 330–352.
Kumar, V., Ramachandran, D., & Kumar, B. (2021). Influence of new-age technologies on marketing: A research agenda. *Journal of Business Research, 125*, 864–877.
Lemon, K. N., & Verhoef, P. C. (2016). Understanding Customer Experience and the Customer Journey. *Journal of Marketing, 80*(November), 69–96.
Lewinski, P., Trzaskowski, J., & Luzak, J. (2016). Face and Emotion Recognition on Commercial Property under EU Data Protection Law. *Psychology & Marketing, 33*(9), 729–746.
Littleton, M. (2003). Borgata Hotel Casino & Spa Turns to Viisage to Enhance Gaming Security. Retrieved from https://www.businesswire.com/news/home/20030923005549/en/Borgata-Hotel-Casino-Spa-Turns-Viisage-Enhance.
Liu, S. Q., & Mattila, A. S. (2019). Apple Pay: Coolness and embarrassment in the service encounter. International Journal of Hospitality Management, 78(April 2018), 268–275.
Maor, E., Perry, D., Mevorach, D., Taiblum, N., Luz, Y., Mazin, I., … Shalev, V. (2020). Vocal Biomarker Is Associated With Hospitalization and Mortality Among Heart Failure Patients. *Journal of the American Heart Association, 9*(7).
McDowell, B. (2019). Three ways in which GDPR impacts authentication. *Computer Fraud & Security, 2019*(2), 9–12.
McStay, A. (2020). Emotional AI, soft biometrics and the surveillance of emotional life: An unusual consensus on privacy. *Big Data and Society, 7*(1).
Milberg, S. J., Smith, H. J., & Burke, S. J. (2000). Information privacy: Corporate management and national regulation. *Organization Science, 11*(1), 35–57.
Moorman, C. (2018). Call for Papers - Journal of Marketing Special Issue: Better Marketing for a Better World. Retrieved from https://www.ama.org/2018/11/20/call-for-papers-journal-of-marketing-special-issue-better-marketing-for-a-better-world/.
Marketing Science Institute (MSI) (2020). Research Priorities 2020-2022. Retrieved from https://www.msi.org/wp-content/uploads/2020/06/MSI_RP20-22.pdf.
Nait-Ali, A. (2011). Hidden biometrics: Towards using biosignals and biomedical images for security applications. 7th International Workshop on Systems. *Signal Processing and Their Applications, WoSSPA, 2011*, 352–356.
Obar, J. A., & Oeldorf-Hirsch, A. (2020). The biggest lie on the Internet: Ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society, 23*(1), 128–147.
Ogbanufe, O., & Kim, D. J. (2018). Comparing fingerprint-based biometrics authentication versus traditional authentication methods for e-payment. *Decision Support Systems, 106*, 1–14.
Parsheera, S. (2020). Participation of persons with disabilities in India's Aadhaar project. Working Paper. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3700984.
Patel, V. M., Ratha, N. K., & Chellappa, R. (2015). Cancelable biometrics: A review. *IEEE Signal Processing Magazine, 32*(5), 54–65.
Pato, J. N., & Millett, L. I. (2010). *Biometric Recognition: Challenges and Opportunities*. National Academies PressNational Research Council & Whither Biometrics Committee.
Pieters, R., Wedel, M., & Batra, R. (2010). The stopping power of advertising: Measures and effects of visual complexity. *Journal of Marketing, 74*(5), 48–60.
Piwek, L., Ellis, D. A., Andrews, S., & Joinson, A. (2016). The Rise of Consumer Health Wearables: Promises and Barriers. *PLoS Medicine, 13*(2), 1–9.
Plassmann, H., Ramsoy, T. Z., & Milosavljevic, M. (2012). Branding the brain: A critical review and outlook. *Journal of Consumer Psychology, 22*(1), 18–36.
Plassmann, H., Venkatraman, V., Huettel, S., & Yoon, C. (2015). Consumer Neuroscience: Applications, Challenges, and Possible Solutions. *Journal of Marketing Research, 52*(4), 427–435.
Prakash, A. (2018). Facial Recognition Cameras and AI: 5 Countries With the Fastest Adoption. Retrieved from https://www.roboticsbusinessreview.com/ai/facial-recognition-cameras-5-countries/.
Reid, D. A., Samangooei, S., Chen, C., Nixon, M. S., & Ross, A. (2013). Soft biometrics for surveillance: An overview. *Handbook of Statistics, 31*, 327–352.
Revfine (2020). 4 Ways Facial Recognition Can Be Used in the Travel Industry. Retreived.
Sheth, J., & Kellstadt, C. H. (2021). Next frontiers of research in data driven marketing: Will techniques keep up with data tsunami? *Journal of Business Research, 125*, 780–784.
Shin, G., Jarrahi, M. H., Fei, Y., Karami, A., Gainfowitz, N., Byun, A., & Lu, X. (2019). Wearable activity trackers, accuracy, adoption, acceptance and health impact: A systematic literature review. *Journal of Biomedical Informatics, 93*.
Snijder, M. (2016). Biometrics, surveillance and privacy. Retrieved from https://erncip-project.jrc.ec.europa.eu/sites/default/files/JRC104392_biometrics_surveillance_and_privacy_final.pdf.
Srinivasa, K. G., & Gosukonda, S. (2014). Continuous multimodal user authentication: Coupling hard and soft biometrics with support vector machines to attenuate noise. *CSI Transactions on ICT, 2*(2), 129–140.
Sudhakar, T., & Gavrilova, M. (2020). Cancelable Biometrics Using Deep Learning as a Cloud Service. *IEEE Access*, 112932–112943.
Thales (2020). Biometrics at the heart of digital innovation. Retrieved from https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/documents/facial-recognition.
Tsai, J. Y., Egelman, S., Cranor, L., & Acquisti, A. (2011). The effects of online privacy information on purchasing behavior: An experimental study. *Information Systems Research, 22*(2), 254–268.
Unar, J. A., Seng, W. C., & Abbasi, A. (2014). A review of biometric technology along with trends and prospects. *Pattern Recognition, 47*(8), 2673–2688.
van Esch, P., Stewart Black, J., Franklin, D., & Harder, M. (2020). AI-enabled biometrics in recruiting: Insights from marketers for managers. *Australasian Marketing Journal, forthcoming.*
Verhulst, N., De Keyser, A., Gustafsson, A., Shams, P., & Van Vaerenbergh, Y. (2019). Neuroscience in Service Research: An Overview and Discussion of its Possibilities. *Journal of Service Management, 30*(5), 621–649.
Wang, J. (2018). You Can Now Check In With Facial Scan At Marriot in China. Retrieved from https://www.forbes.com/sites/jennawang/2018/07/24/you-can-now-check-in-with-a-facial-scan-at-marriott/#5c73d8f23f7a.
Wästlund, E., Otterbring, T., Gustafsson, A., & Shams, P. (2015). Heuristics and resource depletion: Eye-tracking customers' in situ gaze behavior in the field. *Journal of Business Research, 68*(1), 95–101.
Wierenga, J., Kannan, P. K., Ma, X., Reutterer, T., Risselda, H., & Skiera, B. (2021). Data analytics in a privacy-concerned world. *Journal of Business Research, 122*, 915–925.
Wiewiórowski (2020). The state of biometrics. Retrieved from https://edps.europa.eu/sites/default/files/publication/20-10-07_edps_biometrics_speech_en.pdf.
Wirtz, J., & Zeithaml, V. (2018). Cost-effective service excellence. *Journal of the Academy of Marketing Science, 46*(1), 59–80.

Arne De Keyser is Associate Professor of Marketing at EDHEC Business School (France). His research focuses on customer experience, service recovery and frontline service technology. Arne has published articles in the *Journal of Service Research*, *International Journal of Research in Marketing*, *Journal of Business Research*, *Journal of Service Management* and the *Journal of Service Theory and Practice*. He has won numerous research and teaching awards, including the SERVSIG Best Dissertation Award (2015) and the *Journal of Service Research* best paper award (2019). Arne serves on the editorial boards of the *Journal of Service Research*, *Journal of Business Research*, *Journal of Service Management* and the *Journal of Service Theory and Practice*.

Yakov Bart is Associate Professor of Marketing, Thomas E. Moore Faculty Fellow and Patrick F. and Helen C. Walsh Research Professor at D'Amore-McKim School of Business, Northeastern University. His research examining marketing implications of new digital technologies and business models has been funded with multiple research awards and grants, presented at numerous academic conferences across the globe, and published in leading marketing and management journals, including *Marketing Science*, *Journal of Marketing Research*, *Journal of Marketing*, *Management Science*, and *Harvard Business Review*. Yakov won Best Paper awards for his research published in *Decision Analysis* and *Journal of Interactive Marketing*.

Xian Gu is an Assistant Professor in Marketing at the Kelley School of Business at Indiana University. She received her Ph.D. in Marketing from University of Maryland in 2019. Her research interests are in quantitative marketing with applications of treatment effect estimation, field experiments, and econometric models to the substantive areas of digital marketing focusing on mobile marketing, multichannel marketing, and freemium models.

Stephanie Q. Liu PhD, is an Associate Professor of Consumer Sciences at The Ohio State University. Her research focuses on consumer behavior and marketing strategies related to experiential consumption, with special interests in three strategic themes: service encounter management, persuasion in advertising & social media, and technology innovations in the service industry.

Stacey G. Robinson is an Associate Professor at the University of Alabama. Her research focuses on innovating and understanding the customer, and frontline employee experience, in retail and service exchanges. Her research has been published in the *Journal of Marketing, Journal of the Academy of Marketing Science, International Journal of Research in Marketing, Journal of Service Research, Journal of Business Research,* and has been presented at a number of international and national conferences. Stacey serves on the editorial review board for the *Journal of the Academy of Marketing Science, the Journal of Retailing, Journal of Service Research, Journal of Public Policy and Marketing,* and *the Journal of Business Research.*

P. K. Kannan (PK) is Dean's Chair in Marketing Science at the Robert H. Smith School of Business and a Distinguished Scholar-Teacher at the University of Maryland. He has a Ph. D. degree in Management Science and Marketing from Purdue University and previously has been on the faculty of information systems and the faculty of marketing at University of Arizona. His main research focus is on marketing modeling and strategy, applying statistical, econometric, AI and machine learning methods to marketing data. His current research stream focuses on digital marketing, path to purchase models, social tags, attribution modeling, media mix modeling, and customer relationship management (CRM).

PK has received several grants from National Science Foundation and other agencies for his work in this area and has been published in *Marketing Science, Management Science, Journal of Marketing Research*, and *Journal of Marketing*. His research has won the John Little Best Paper Award (2008), the ISMS-MSI Gary Lilien Practice Prize Award (2007), and the IJRM Best Paper Award (2017). His research has also been selected as a finalist

thrice for the Paul Green Award (2008, 2014, 2019) for the best paper published in *Journal of Marketing Research* and he has won the AMA/MSI Paul Root Award twice for papers published in *Journal of Marketing* (2014 and 2016). He is also one of five 2018 Distinguished Scholar Teacher awardees at the University of Maryland, College Park.

PK is the editor-in-chief of *International Journal of Research in Marketing,* an Associate Editor for *Journal of Marketing Research* and serves on the editorial boards of the *Marketing Science*, *Journal of Marketing*, *Journal of Service Research*, and *International Journal of Electronic Commerce*. PK has served as an AE for *Journal of Marketing* and the Chair for the American Marketing Association SIG on Marketing Research and as a chair of the INFORMS Service Science section.

PK has worked with Marriott International and Adobe on attribution and big data related research. He is a scientific advisor for several marketing analytics firms advising in these areas. He teaches Marketing Analytics, CRM, Digital Marketing and Marketing Models for the MBA and doctoral students. He has extensive executive teaching experience and has consulted for companies such as Marriott, Choice Hotels, Accor Hotels, Frito-Lay, Pepsi Co, Giant Food, Stanley Black and Decker, SAIC, Fannie Mae, and IBM.