APTARA | MAR | mar20913 | Dispatch: June 2, 2016 | CE:
Journal | MSP No. | No. of pages: 18 | PE: XXXXX

Face and Emotion Recognition on Commercial Property under EU Data Protection Law

Q1
Peter Lewinski
Université de Neuchâtel and University of Amsterdam

Jan Trzaskowski
Copenhagen Business School

Joasia Luzak
Q2
Exeter University and University of Amsterdam

ABSTRACT

This paper integrates and cuts through domains of privacy law and biometrics. Specifically, this paper presents a legal analysis on the use of Automated Facial Recognition Systems (the AFRS) in commercial (retail store) settings within the European Union data protection framework. The AFRS is a typical instance of biometric technologies, where a distributed system of dozens of low-cost cameras uses psychological states, sociodemographic characteristics, and identity recognition algorithms on thousands of passers-by and customers. Current use cases and theoretical possibilities are discussed due to the technology's potential of becoming a substantial privacy issue. First, this paper introduces the AFRS and EU data protection law. This is followed by an analysis of European Data protection law and its application in relation to the use of the AFRS, including requirements concerning data quality and legitimate processing of personal data, which, finally, leads to an overview of measures that traders can take to comply with data protection law, including by means of information, consent, and anonymization. © 2016 Wiley Periodicals, Inc.

Information society and its constellation of associated technologies, including search engines, social media and e-commerce shops, in particular, has spurred a massive production and processing of personal data that can be used for marketing purposes. Nanotechnologies introduce new ways of collecting and extracting personal data and provide examples of how the information society is gradually bleeding over into the physical world. This paper explores the possibilities in and legal implications of non-invasive and portable technologies that can detect and analyze faces to determine emotions and other biophysiological parameters. The purpose is to examine EU data protection law in this context to provide guidelines for compliance when using automated facial recognition systems (the "AFRS") in retail stores. For further information, the researchers encourage readers to watch this brief video: youtu.be/IUtRl8HO7Vg (AdMobilize, 2015).

The AFRS has traditionally been deployed in high-security facilities like airports (Buckley & Hunter, 2011; Olsen, 2002), but today it is increasingly being used in shopping malls and similar consumer settings (Buckley et al., 2011; Singer, 2014). For example, a recent UK survey of 150 senior IT, marketing, or digital retail executives found that almost 75% of the retailers used some technology to track consumers in the store, while 27% specifically used the AFRS (CSC, 2015). News reports include stories of large, multinational producers cooperating with supermarket chains to identify and target consumers who would be more likely to purchase their products (Buckley & Hart, 2011; Hill, 2011; Wadhwa, 2012). Q3

For many years, the face and fingerprints have been relied upon as a source of biometric data, and it is now recognized that in addition to determining identity, facial recognition can be used to establish "physiological and psychological characteristics such as ethnic origin, emotion, and well-being" (Opinion 3/2012 on developments in biometric technologies (WP 193), p. 21).

The development of the digital market deepened an imbalance in the relationship(s) between traders and consumers, leading to new questions as to the ethical boundaries of marketing and retailing (De George, 2001; Introna, 2005; Palmer, 2005). In this respect, scholars focus either on analyzing ethical consequences

Psychology & Marketing, Vol. 00(0): 1–18 (xxxx 2016)
View this article online at wileyonlinelibrary.com/journal/mar
 DOI: 10.1002/mar.20913

of tracking internet users' behavior online and which systems allow for collection and further processing of personal data (Charters, 2002; Miyazaki, 2008; Palmer, 2005), or on the infringements of privacy in the offline world resulting from the use of digital technology like video surveillance (Atrey et al., 2013; Senior, 2009; Wright & Kreissl, 2015). The use of the AFRS by retailers may fall into both of these categories. On the one hand, consumer privacy may be infringed by the AFRS tracking consumer behavior offline. On the other hand, this software would also enable retailers to gather and process consumers' personal data online, due to its emotion and face recognition functions, which are embedded into distributed systems that generate big data processed "in the cloud." These practices may infringe upon a person's right to his own image, which is protected as part of the right to privacy under Article 8 of the European Convention on Human Rights (2010, amended) as ruled in Sciacca v. Italy (no. 50774/99, § 29, ECHR 2005-I) (Buckley et al., 2011). Moreover, these practices may equally be contrary to the system established by the EU data protection law, unless traders using the AFRS take some precautionary steps to prevent this infringement (Buckley et al., 2011), as will be discussed below.

The controversies and compliance questions that arise from the use of the AFRS in retail stores is the main subject of this paper, owing to its impact on consumers and the protection of their privacy. In this respect, the research aims to identify the future applications of the AFRS, together with the identification of which types of data are necessary to achieve a given purpose. Conceivably, not all uses of the AFRS would lead to infringement of the EU data protection law (Buckley et al., 2011).

First, the following sections will present the AFRS and explore its various uses for retailers. Next will be an introduction to the EU framework for data protection in the context of consumer privacy and an illustration of how the AFRS may impose on consumer privacy. In the last part, the researchers suggest guidelines for the use of the AFRS and compliance with EU data protection law, which adds perspectives as to the future of the AFRS, including consequences of the new General Data Protection Regulation. The core of the paper shows how the data protection law can be applied to the field of the AFRS, in particular, whether the AFRS can be used to process personal data without the subject's consent and kinds of measures that traders may use to ensure compliance with the law.

THE AFRS IN RETAIL

Continuous and unobtrusive measurement of both consumers' emotions and their attention simultaneously on the shelves and the store in general could give retailers additional insights into their customers' decision-making process (Lewinski, Fransen, & Tan, 2014). The literature has already established that objective emotion responses can be captured using the AFRS with near-human accuracy rates (88% average recognition rate; Lewinski, den Uyl, & Butler, 2014) or even better than humans under some circumstances (Lewinski, 2015a). This is important, because while mobile eye-tracking glasses have so far proven useful for measuring how consumer attention is captured (Bulling & Gellersen, 2010), until recently nothing similar has existed for facial tracking (unless obtrusive head-mounted cameras were used; Dickie, Vertegaal, Sohn, & Cheng, 2005). Researchers and retailers may capture facial expressions through ordinary industrial CCTV, but due to the camera's location, and hence low image quality, measurements via this system are not ideal.

A practical example would be a monitoring system installed in a retail store such that a couple approaching a shelf of moderately priced bottles of wine can be observed. They stand there for two minutes and look at each other, and back at the shopping shelves. With eye-tracking software, a viewer could only infer that the couple was looking at the bottles on the shelf—but do they like what they see? This can only be inferred if emotional responses can be measured. The AFRS can achieve that step by showing the couple smile, frown, raise their eyebrows or otherwise display emotion. Will the couple buy the retailer's wine? On the basis of the couple's facial expressions when looking at a particular shelf, certain inferences may be drawn as to their emotional responses to the products displayed there. This may allow a retailer to predict their attitude towards the product (e.g., Lewinski et al., 2014) and more precisely, whether they might be inclined to watch it longer (Lewinski, 2015b) or buy it (e.g., Lewinski, Tan, Fransen, Czarna, & Butler, 2016). Such information on the consumer's decision-making process is valuable to the retailer and makes the use of the AFRS attractive to retailers.

A clothing store presents another theoretical scenario demonstrating the application of the AFRS. First, a new client named Elizabeth registers herself with the software. The next time she walks into the shop, the software identifies her as Elizabeth, 35 years old, who has purchased products three times in this store in the last two months. It tracks her around the store, registers at which racks with designer-label clothes she has lingered, and which items she has picked for closer inspection. The AFRS not only observes this scene, but it learns about her attitude towards the things she has paid attention to by analyzing her facial expressions of interest, happiness, or disgust through a cloud-based AFRS module (e.g., FaceReader Online, 2015). It estimates changes in heart rate through the remote PPG (photoplethysmography) module (rPPG is a camera-based heart rate detection; Tasli, Gudi, & den Uyl, October 2014). This leads to the "Circumplex Model of Valence and Arousal" (Russell, 1980; FaceReader, 2015), which helps to create a personalized, emotional profile of the shopper for this specific store and type of clothing. The system network may then notify the digital signage

system—a digital screen that displays various advertisement content, such as digital images and video in public spaces—about the fashion items Elizabeth had expressed interest in, allowing it to provide personalized digital content to Elizabeth during her online and offline shopping trips.

Retailers may be quite keen on moving toward testing and using the AFRS in their stores. For example, Noldus IT (Noldus, 2015), in collaboration with i3B (2015a), already has "Shop Lab" (2015b) in place. The Shop Lab consists of a rack of shelves with supermarket products equipped with a specialized camera-tracking system. The shelves are monitored by EagleEye 3D (Eaglevision, 2015) camera units and Ubisense (2015) sensors from above (to track consumer movements) and Axis (2015) cameras from the side (to view close-range behavior). They also have Tobi (2015) eye-tracking calibration points. Technically, it would be easy to move on to the next step in their design and mount a few miniature cameras in racks facing outward to experiment with facial expression capture of a person inspecting products on a shelf. Equipping such strategically placed and customized sets of cameras with a cloud-based AFRS (e.g., FaceReader Online, 2015) would allow for a thorough facial emotion analysis. However, as will be pointed out in the following sections, compliance with the data protection law must be ensured.

The AFRS may be designed as an off-the-shelf application of a mobile system for human observation, produced at low prices (less than $200) and high volume (see e.g., CNET, 2015 for a review of 35 such cameras). Consequently, the AFRS could be perceived as an innovative fusion between advanced human observation software and fast, energy-efficient and cost-efficient hardware. Moreover, the advantages of the AFRS extend beyond merely large retail chains. Additional feasible applications include health care, security businesses, and private use (e.g., Buckley et al., 2011; Silver, Goodman, Knoll, & Isakov, 2004). For this software–hardware integration to be successful, effective and efficient, the system needs to guarantee desired speed, performance and reliability (for a description of an ineffective AFRS, see Stanley & Steinhardt, 2002). These three key indicators of commercial success could only be achieved if the AFRS system can rely on powerful, energy-efficient processing units that provide the required stability for such a mobile and embedded system.

If retailers are able to guarantee the stability of the system, they could benefit from the AFRS in many ways. Currently, the most promising market within the retail domain is digital signage. These screens can be equipped with the AFRS to collect information about the people looking at the screen. Furthermore, as has previously been pointed out, data gathered by the AFRS in other settings (like the inside of a shop) can then be employed by the digital signage system. This means that information appearing on screens would depend on a shopper's facial expressions of emotion, age, and gender that have previously been recorded by the AFRS and subsequently retrieved by it. There are a few companies that offer software solutions for digital signage already: Quividi (2015) provides measures of age and gender; Intel (2015) provides age, gender, and viewing times; IMRSV (2015) provides age, gender, viewing times, and emotions; AdMobilize (2015) provides age, gender, viewing times, six basic emotions, and people counting; VicarVision B.V. (2016) provides age, gender, viewing times, six basic facial emotions, people counting, heart rate detection, face features detection (facial hair, glasses), and ethnicity.

Apart from digital signage, the AFRS can also be used to collect consumer information in more general retail settings, such as people counting purposes; visitor movement and attraction patterns, which influence the layout of products in a shop; personalization of an in-store online ecommerce shop of a given brand tailored to an individual customer; and even safety and care (e.g., aggression detection, fall detection, deceit detection). Preliminary tests of using the AFRS in a digital signage environment are already underway (see Figure 1 for an illustration).

The AFRS can be used for tracking and profiling even if there is no knowledge of the real-world identity of an individual. It is thus possible to "track routes and habits of individual shoppers" for the purpose of effective queue management, product placement, and targeted advertising or other specific services (Opinion 3/2012 on developments in biometric technologies (WP 193), p. 23).

In the next section, an analysis of the legal implications of the AFRS under EU data protection law in three specific use cases will be presented. The AFRS for retail applications can essentially be used to perform recognition of (in increasing order of privacy intrusion): (a) psychological states (basic emotions, arousal/valence, heart beat rate, head orientation, gaze direction), (b) sociodemographic characteristic/traits (e.g., gender, age, ethnicity, facial hair, glasses) and (c) identity.

The common step for all those applications is face detection (e.g., by Viola & Jones, 2004; cascaded classifier algorithm), feature extraction, and then normalization. Importantly, an AFRS in principle *does not* require storing/acquiring an actual image/video for (a) and (b), but does need to store such data for (c). The AFRS can work in a "hot mode" without actually storing anything, i.e., using only random access memory (RAM) instead of hard disk memory. A parallel would be a photo camera that can detect and mark faces (or even smiles) on its liquid crystal display (LCD) in real time.

Most AFRS detect emotions, attention, and different psychological states (a) by face modeling (e.g., using Active Appearance Model, Cootes & Taylor, 2000) in order to extract features, and then some form of compression is used (e.g., Principal Component Analysis; Jackson, 1991) to reduce the dimensionality (i.e., normalization). Finally, the AFRS classifies the psychological states of a person by comparing how an individual's specific expression deviates from a baseline computed from tens of thousands of examples of manually annotated images

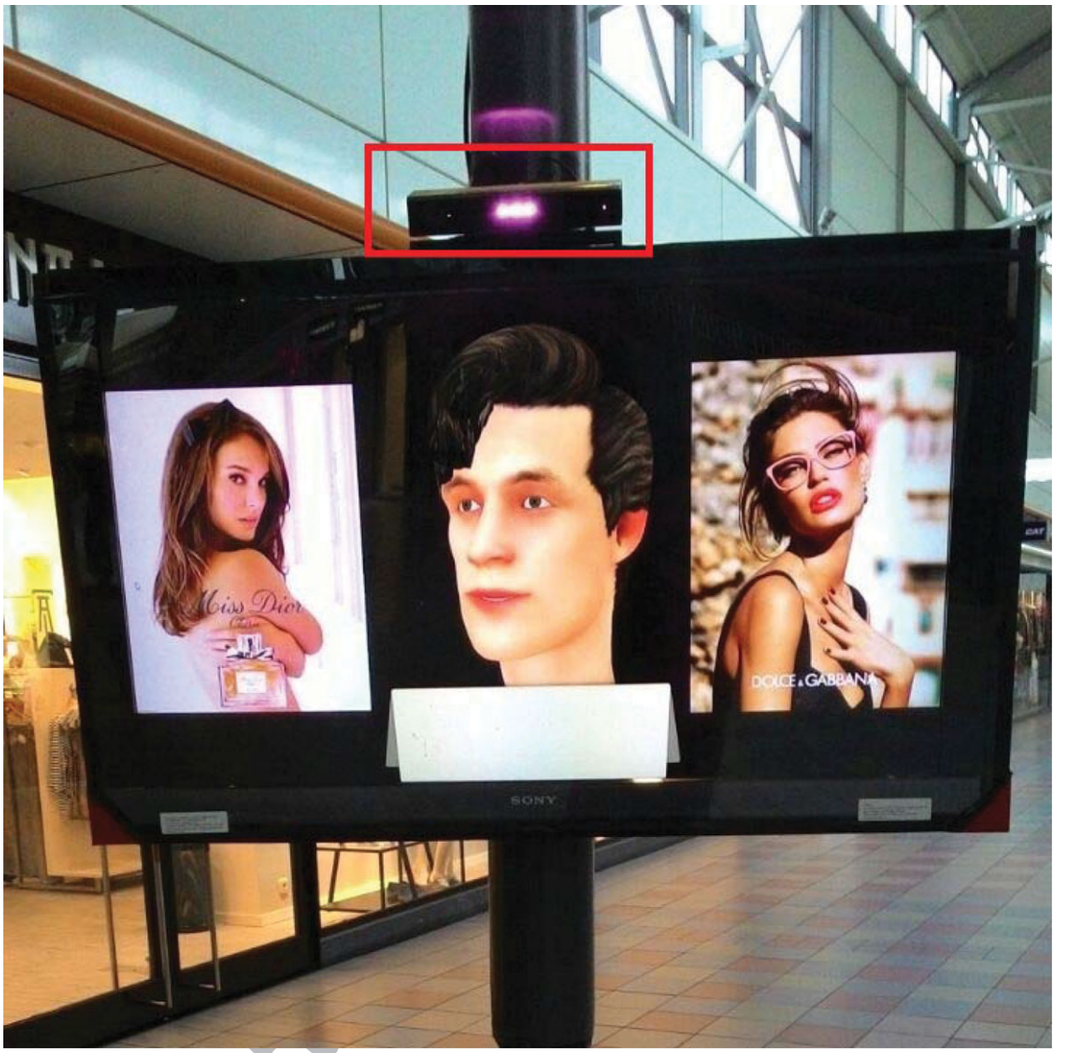


Figure 1. *An example of a virtual shopping assistant in a commercial center in the Netherlands with a mounted AFRS on top of it*. The position of the AFRS is marked with a red rectangle. Reproduced with permission.

(e.g., such as ones in Olszanowski et al., 2015) using an artificial neural network (Bishop, 1995). A similar process is applied to the estimation of sociodemographic characteristics (b).

Facial, i.e., identity recognition (c) is conceptualized into the following steps: (1) image acquisition; (2) face detection; (3) normalization; (4) feature extraction; (5) enrollment; (6) comparison (Park et al., 2014). Thus, the image or video is acquired, then the face(s) are detected and normalized, as with previous applications. Afterwards, the facial features are extracted and stored for later comparison. Knowing the identity allows the trader to link the observations to information from other sources such as online behavior. This vein is not further pursued in this context, as this paper focuses on activities within the physical store.

In the shopping context, the retailer may use any of the above-reviewed applications of the AFRS for one or both of two main purposes: *understanding behavior* and *influencing behavior*. The AFRS can be used, in an increasing degree of complexity and personal data needed, for (1) testing advertisements and store layout effectiveness, (2) creating varying degrees of market segmentation, and (3) interacting with customers in real time.

Beyond the retail context, the AFRS can be used for many purposes, including access verification/authentication (e.g., at the airport), suspect matching (e.g., by police), or automatic person tagging (e.g., social media). That being said, the current examination will only be concerned with applications for commercial purposes in a physical store.

While retailers can use an AFRS that allows for not only facial recognition (recognizing a person), but also emotion recognition (recognizing the emotional state of a person from observing facial expressions), there are fundamental differences between these software options and their impacts on consumer privacy. Different settings of the AFRS provide a different type of information on consumers, and hence the AFRS may enable retailers the recognition of consumers' identity, emotion and/or sociodemographic characteristics. As mentioned in the previous section, not all this information could be considered as providing retailers with consumers' personal data. Privacy issues are likely to arise when—possibly unwanted, unexpected and not consented to—observations of a person, in a more or less permanent registration system, are connected to a personal identity. In other words, the system knows: "You were there, at that time, doing this." As explained, this would allow for the possibility of identifying the consumer, which would lead to the classification of this software as processing personal data. While the first function of the AFRS, which enables recognition of the consumer's identity, clearly qualifies as processing personal data, the other function, namely recognizing consumer emotions and sociodemographic characteristics, cannot necessarily be traced to an identifiable consumer.

Furthermore, facial recognition, i.e., specifically identifying a person, is not necessarily as important to retailers as the possibility of segmenting consumers based on their emotions and sociodemographic characteristics. The issue with the taxonomy for the AFRS is that facial recognition (vs. emotion and/or sociodemographic recognition) is not very insightful for retailers. Previously in this paper, a scenario with "Elizabeth" was presented where she first registers and then later is recognized by her name via the AFRS. However, in reality, retailers are not necessarily interested in identity recognition capabilities in the sense of knowing who a person is with precision. While it is true that better segmentation of the market could be achieved by not counting the same person more than once, it still would be enough for a retailer to know which sociodemographic groups (i.e., segments) tend to re-visit the store. Considering the privacy issues, exact identification of individuals seems more relevant in the security domain, such as access control or suspect matching, rather than in connection with the commercial/retail use of the AFRS.

PROTECTION OF PERSONAL DATA IN THE EUROPEAN UNION

The protection of personal data is a fundamental right in the European Union (See Article 8 of the Charter of Fundamental Rights of the European Union (2012) and Joined Cases C-92/09 and C-93/09, *Volker und Markus Schecke*). However, the European and national legislators allow traders to gather and process personal data provided that (according to Article 8(2) of the Charter of Fundamental Rights) "such data [are] processed fairly for specified purposes and on the basis of the *consent* of the person concerned *or some other legitimate basis laid down by law*" [emphasis added]. This entails that data protection law must be interpreted in the light of the fundamental rights and that any processing of personal data is a potential interference with fundamental freedoms (Joined Cases C 465/00, C 138/01 and C 139/01, *Österreichischer Rundfunk and Others*, paragraph 68, and Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger et al*.). The fundamental rights to privacy and personal data are granted to individuals in their capacity of being citizens, which also includes the role of being a consumer as dealt with in this paper.

The Data Protection Directive (1995) (hereafter "the Directive") lays down common rules for the processing of personal data in the EU (see in general Trzaskowski, Savin, Lundqvist, & Lindskoug, 2015, chapter 3). The regulations provided in the Directive amount to harmonization that is generally complete—even though the Directive provides the Member States with a margin for maneuver in certain areas (Case C-101/01, *Lindquist*, paragraphs 96–98). The use of facial recognition may be subject to additional regulation or control in various Member States, including by means of prior authorization (Opinion 02/2012 on facial recognition in online and mobile services (WP 192), p. 5).

Pursuant to Article 29 of the Directive, the European Commission and supervisory authorities in the area of privacy enforcement established an "Article 29 Working Party" whose opinions, despite no binding force, play a significant role in suggesting interpretations of the provisions of the Directive in the absence of case law. To some extent, these opinions are used in this context, with proper precautions, as to the likely outcome of decisions from the Court of Justice of the European Union (CJEU).

The Directive applies to any operation or set of operations that are performed upon personal data, such as "collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction" (processing) of any information relating to an identified or identifiable natural person (personal data) (Article 29 Working Party, Opinion 4/2007 on the concept of personal data and the Directive's definitions). Due to the broad scope of application, it is virtually impossible to use the AFRS without processing personal data, as the mere monitoring by means of video surveillance (e.g., CCTV) already amounts to processing of personal data (see e.g. Case C-212/13, *Rynes v. Urad pro ochranu osobnich udaju*).

Consumers need not to be identified by the AFRS in order for the use to be qualified as processing personal data, but there rather needs to be a possibility that this software would enable consumer's identification (e.g., see Shi, Samala, & Marx, 2006). In this respect, it is

important to consider (a) for what purposes the AFRS is and could be used, (b) what the cost of piecing together consumer's identification would be (if feasible at all), (c) what safety mechanisms have been adopted by the controller to protect against data breaches, and (d) what the interests of consumers are (Trzaskowski et al., 2015). By recording central physiological features of consumers that make facial recognition possible, the AFRS could facilitate the identification of consumers and, therefore, EU data protection law applies. Nevertheless, as of 2015 identification from physiological features to facial/identity recognition is far from perfect (e.g., see Chen, Xu, Zhang, & Chen, 2015; Stanley et al., 2002).

DATA QUALITY AND JUSTIFICATION OF DATA PROCESSING

A retailer may collect personal data, according to Article 6(1)(b) of the Directive, only for specified, explicit, and legitimate purposes. This requirement is particularly relevant, as the purpose is an important yardstick for determining whether personal data is being lawfully processed. Thus the purpose is used to determine whether personal data is "adequate, relevant, and not excessive" and "accurate," as well as not kept "longer than necessary." A retailer may not process personal data further (than collection) in a way incompatible with this purpose. The focus on "collection" in Article 6(1)(b) entails that the retailer must specify any purposes prior to, and in any event not later than, the time when the collection of personal data occurs. However, not all instances of future processing are foreseeable at the time of collection. The compatibility of further processing of the collected data may, according to the Article 29 Working Party, be determined by considering: (1) the relationship between the purposes for which the retailer has collected data, and the purposes of further processing, (2) the context in which the retailer has collected data and the reasonable expectations of the data subjects as to its further use, (3) the nature of the data and the impact of the further processing on the data subjects, and (4) the safeguards applied by the controller to ensure fair processing and to prevent any undue impact on the data subjects (Article 29 Working Party, Opinion 03/2013 on purpose limitation (WP 203), p. 43).

The retailer must sufficiently define the purpose of data collection to delimit the scope of data processing and to enable necessary safeguards. "A purpose that is vague or general, such as "improving users' experience,' "marketing purposes," "IT-security purposes" or "future research" will—depending on the particular context—usually not be perceived as sufficiently specific (Article 29 Working Party, Opinion 03/2013 on purpose limitation (WP 203), p. 16). In addition, the purpose must be unambiguous and clearly revealed, explained, or expressed in some intelligible form with a view to ensure transparency. However, the transparency standards have not been further harmonized (see also: Luzak, 2013; Luzak, 2014).

In the context of this paper, the focus is on data collection for commercial purposes in retail. The purpose of increasing profits by, among other things, improving customer experiences based on the use of personal data (and thus encouraging them to shop more often) is generally recognized as a legitimate purpose. Nevertheless, this purpose is comparatively less compelling than, for instance, processing of personal data for crime prevention or prosecution. Moreover, the scope of this paper concerns facial recognition, which falls within the scope of biometrics, and the use thereof has a high potential impact on personal privacy and could facilitate infringements of the right to data protection of individuals (Opinion 3/2012 on developments in biometric technologies (WP 193), p. 3). The use of biometric data by means of facial recognition raises issues of proportionality, which must be assessed in light of the purpose behind the processing—bearing in mind that the "data may only be used if adequate, relevant, and not excessive." This implies "a strict assessment of the necessity and proportionality of the processed data and if the intended purpose could be achieved in a less intrusive way" (Ibid, p. 8).

In addition to compliance with the fundamental requirements discussed above, the processing of personal data must also be legitimate, i.e., justified under Articles 7 and/or 8 of the Directive, which concern normal data and sensitive data, respectively. Sensitive data are data revealing/concerning racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health, or sex life. Article 8 supplements Article 7, as the intention is to provide a better protection for sensitive data. Thus, a data processor should take both provisions into account when sensitive data are to be processed. Even though the expression "data concerning health" must be given a wide interpretation (Case C-101/01, *Lindquist*, paragraph 50), it is not likely to comprise facial expressions, as long as the intention is not to extract data concerning the health of individuals. Therefore, the justification for processing data in the context of the AFRS must be found in Article 7 concerning "normal data." However, it should be emphasized that processing of biometric data can "be used to determine sensitive data, in particular those with visual cues such as race, ethnic group or perhaps a medical condition" (Opinion 3/2012 on developments in biometric technologies (WP 193), p. 23; Buckley et al., 2011).

Two of the six legal bases from Article 7 of the Directive that can justify the processing of normal data may be relevant in this context: (a) "the data subject has unambiguously given his consent"; and (f) "processing is necessary for the purposes of the legitimate interests pursued by the controller [. . .] except where such interests are overridden by the interests" or fundamental rights and freedoms of the data subject (Buckley et al., 2011). The latter option entails a "balancing test"

and may, to some extent, be used to process personal data without the data subject's consent. Basically, the two options may be perceived as models for opt-in and opt-out application of the AFRS to consumer transactions, respectively. It should be emphasized that the balancing test is not reserved for exceptional cases and it may be used in certain instances "as a legitimate basis for processing personal data for conventional direct marketing and other forms of marketing or advertising" (Article 29 Working Party, Opinion 06/2014 on the Notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (WP217), pp 24–25). Nonetheless, there are variations in the application of the balancing test in Member States (Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (WP 217), p. 5). The section below is a brief illustration of the requirements for the balancing test. The first legal basis of obtaining consumers' consent to processing of their personal data is further discussed in the following section, as it constitutes an important measure that retailers may take to legitimize their use of the AFRS.

The Balancing Test

The balancing test requires a careful examination of the context and the circumstances concerning data collection and further processing, including the trader's legitimate interests and the potential interference with the data subject's interests and fundamental rights. According to the Article 29 Working Party, the balancing test may include consideration of the following factors:

> "(1) the nature and source of the legitimate interest and whether the data processing is necessary for the exercise of a fundamental right, is otherwise in the public interest, or benefits from recognition in the community concerned; (2) the impact on data subjects and their reasonable expectations about what will happen to their data, as well as the nature of the data and how they are processed; and (3) additional safeguards which could limit undue impact on the data subject, such as data minimization, privacy-enhancing technologies; increased transparency, general and unconditional right to opt-out, and data portability" (Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (WP 217), p. 3; see also Trzaskowski et al., pp. 92–94).

The trader's "interest" is closely related to, but distinct from, the concept of "purpose" discussed above. To begin with, it must be emphasized that the trader's interest in increasing profits (the pursuit of economic interests) is legitimate, and it may cover conventional direct marketing and other forms of marketing or advertisement; however, a trader's economic interest to learn as much as possible about consumers to develop better-targeted advertising is not very pressing for society as a whole (Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (WP 217), pp. 24–25).

All relevant interests of the data subject should be taken into account in the balancing test. These interests may range from serious to trivial (Article 29 Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (WP217), p. 30). Several elements can be useful to consider, including "the nature of personal data, the way the information is being processed, the reasonable expectations of the data subjects and the status of the controller and data subject" (Ibid, p. 36). The impact on the data subject comprises any possible consequences of the data processing, as the more sensitive the information involved, the more consequences there may be for the data subject (Ibid, p. 39).

The purpose of the balancing test is not to prevent any negative impact on the data subject, but to avoid "disproportionate impact" (Ibid, p. 41). In order to mitigate the impact, the trader may provide "an easily workable and accessible mechanism to ensure an unconditional possibility for data subjects to opt-out of the processing" (Ibid, p. 41). To the extent the interest pursued by the trader is not convincing, the interests and rights of the data subject are less likely to be overridden by the legitimate—but less substantial—interests of the trader (Ibid, p. 26). Since the retailer's legitimate interest in the use of the AFRS to sell more products is not particularly compelling, the balancing test may only be used for justification of data processing that is an insignificant intrusion of the data subject's privacy and does not have any other undue impact.

Given the data subject's interest in not being monitored, the balancing test does not seem to be the proper legal basis for using the AFRS (see also Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (WP 217), p. 46). Previously, in the context of the use of biometrics for ensuring the general security of property and individuals, the legitimate interests to ensure such security did not override the data subject's interests or fundamental rights and freedoms (Opinion 3/2012 on developments in biometric technologies (WP 193), p. 13).

MEASURES TO LIMIT THE IMPACT ON THE DATA SUBJECTS

From the analysis above, it seems clear that obtaining consumers' consent is the most obvious solution for justifying the processing of personal data by means of the AFRS in the retail sector. The following paragraphs will illustrate the effects of information, consent, and anonymization on privacy protection and the use of the AFRS, including whether and to what extent implementation of such measures may provide sufficient counterweight to justify the processing of personal data without consent.

Information on Data Processing and its Transparency

The Directive provides the data subject with certain rights in Articles 10, 11, 13, and 14. Pursuant to Article 10 of the Directive, the data controller (the retailer, in case of the AFRS) must at least provide the data subject with the following information:

> "(a) the identity of the controller and of his representative, if any; (b) the purposes of the processing for which the data is intended; (c) any further information such as (1) the recipients or categories of recipients of the data, (2) whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply, or (3) the existence of the right of access to and the right to rectify the data concerning him in so far as such further information is necessary, having regard to the specific circumstances in which the data is collected, to guarantee fair processing in respect of the data subject."

Since consumers are generally perceived as the weaker party, who suffer from information deficits and biases preventing them from making rational choices, the European legislator has opted to restore some of the balance in the transaction by placing such information obligations on the data controller, in this case the retailer. Generally, with regard to privacy concerns, many studies have confirmed that consumers are unaware both of the fact that their data is being gathered and processed, and for what purposes this occurs (Milne & Culnan, 2004; Nowak & Phelps, 1995; IMCO, 2011). Therefore, for information obligations to be effective, such information does not only need to reach consumers, but also needs to be accessible to them (Luzak, 2013; Luzak, 2014). Without transparent provision of information on these practices, consumers could not provide a valid consent to the collection and processing of their data (Opinion 2/2010 on online behavioral advertising (WP 171), p. 17). Therefore, only compliance with this first requirement by a retailer—to provide transparent and comprehensive information to consumers on data processing—could lead to the fulfillment of the second requirement, i.e., obtaining a valid consent for such practices (Helberger et al., 2013; Luzak, 2014). The information must be provided directly to the individuals, and "it is not enough for information to be "available" somewhere" (Article 29 Working Party's Opinion 15/2011 on the definition of consent (WP 187), p. 20).

Thus, prior to giving their consent to the use of the AFRS by a retailer, consumers should be well-informed that the retailer uses the AFRS and for what purposes their data will be used. Since the AFRS, in principle, can be installed on any camera, it is important to consider how the use of different surveillance measures might impact consumers and their perception of the technology. Given the ability of retailers to install the AFRS on existing surveillance systems, consumers may lack clarity regarding the *purpose* of the camera recording system. They could be unaware of the merger of commercial and security functions in the AFRS, security being the purpose behind the original surveillance system. As such, a distinction should be made between already existing, nearly ubiquitous CCTV cameras, which are used for security and surveillance, and dedicated recording systems, installed with the main purpose of gathering customers' data for commercial purposes. In both scenarios, an informed consent could only be perceived as such if the large retailer clearly indicated to consumers that the surveillance system is used for commercial purposes related to the registration and processing of not only their physical appearance, but also of their emotional responses. Normally, the data subject must be able to foresee to what ends the data recorded in a public place will be used (see, e.g. Peck v. the United Kingdom, no. 44647/98, §§ 60–63, ECHR 2003-I). However, in the first case, the information should be more explicit and clearly dissuade any misleading notions consumers may have about their image being registered for security purposes only.

Large retailers may install the AFRS equipped with different processing protocols. On the one hand, the AFRS could simply gather consumer data through the original video input file, analyze it immediately in the cloud, and—without storing the data—draw actionable conclusions before deleting the original data. On the other hand, the original video file could be stored for future reference. Traders will not be able to release themselves from the information obligations as provided by Article 10 of the Directive by claiming that they use cloud services (or any other data processor) and do not store consumers' personal data. Under both circumstances, if the gathered data allowed for the identification of a consumer, it should be considered as personal data, and the trader would be seen as processing it, even if the data were not stored. Therefore, as appealing as this argument could be for commercial entities to claim that they do not *store* any personal data, it would *not* mean that they do not process it. Thus, arguably the only value that can be derived from cloud-based processing protocols (i.e., immediate destruction of the input video) is diminishing *potential* traceability of the person (which could lead to the retailer attempting to claim that the data was anonymized – see further below) and thus avoid a *potential* breach of data (e.g., through hacking, as there would be nothing to hack). Additionally, in the second scenario, chances for fair and legitimate use of personal data by the data controller are lower, since he may himself lose control of customers' personal data if, for instance, he allows it to be exported to a third party. Moreover, with regard to obtaining consumers' informed consent, a retailer might find it difficult to provide consumers with sufficient information as to what purposes their data may be used for in the future and by which parties. A consent granted by consumers without them knowing

what will happen to their data could hardly be seen as informed (Luzak, 2014). The European Court of Justice ruled that even transferring personal data from the national tax authority to the national health insurance authority without informing the data subject does not comply with the Directive (C-201/14, *Smaranda Bara et al. v. Presedintele Casei Nationale de Asigurari de Sanatate* (CNAS), et al.). The following paragraph discusses the validity of obtaining consumers' consent to the processing of their personal data.

Informed Consent

As mentioned previously, the most reliable way to legitimize the processing of personal data would be for retailers to obtain an informed consent, within the meaning of Article 7(1)(a) of the Directive, in the context of the use of the AFRS (see e.g., Trzaskowski et al., pp. 95–98). Also, the Charter of Fundamental Rights (2012) in its Article 8 para 2 specifies that personal data may be processed, among other things, on the basis of the consent of "the person concerned." Of course, merely by informing consumers about the data collection and purposes for which it will be processed, the retailer would not be able to freely dispose of this data. The general standards for data collection and processing, as discussed above, e.g., of a legitimate purpose and fairness, remain applicable (see Section I—Principles Relating to Data Quality, Article 6, of Directive 95/46/EC). However, consumer protection would still increase if the fact that such activities may occur and information about the scope of these activities were provided to consumers.

The data subject's consent is defined in article 2(1)(h) as "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed." Due to the flexible structure of the Directive, the nature of the personal data and processing involved is likely to influence the threshold for a freely given, specific, and informed consent. For consent to be unambiguous, which is the requirement for obtaining consent for processing normal data, the procedure to consent must leave no doubt as to the data subject's intentions, which compels the data controllers to create robust procedures for individuals to deliver their consent. Thus, the data controller should create and retain verifiable evidence showing that consent was actually given (Article 29 Working Party's Opinion 15/2011 on the definition of consent (WP 187), p. 21).

Therefore, consumers may consent to the processing of their personal data, surrendering their right to privacy (Luzak, 2013). However, this consent, in order to be valid, has to be (a) unambiguous, (b) freely given, (c) specific, and (d) informed, pursuant to Article 2 (h) of the Data Protection Directive (1995). These requirements rule out the appropriateness of a consent *in blanco*, without the data controller specifying for what purposes the personal data will be processed, as well as of a consent given without the consumer obtaining other relevant and transparent information.

Figure 2. An example of warning/implicit consent message. Google Images, labeled for reuse.

Since consent may not be coerced, the question arises as to whether the inability to conclude a contract with the trader without having consented—in this case, by not being able to enter a store without consenting to the use of the AFRS—which would be a similar sanction to the one applied by website providers blocking access to a given website if a consumer does not accept cookies, could amount to economic duress. Consumers should be able to grant, but more importantly, to also refuse consent to data processing without having been excluded from participation in the market (Helberger et al., 2013; Luzak, 2014). In practice, even if consumers theoretically could be seen as being able to refuse granting consent to data collection and processing, the drastic consequences of consent refusal could leave them helpless to do so. The choice to grant a consent may, therefore, not be a real choice at all (see also Article 29 Data Protection Working Party, 2011, p. 9).

Aside from consumers not having a real opportunity to say "no" to large retailers, it is still disputed in the scholarship how they may say "yes." That is to say, to what extent consumers' consent could be implied (Luzak, 2013). For normal, not sensitive, data, the consent does not have to be explicit but rather (only) unambiguous. This means that if it is evident from the consumer's behavior that he has agreed to the data collection and processing, e.g., when a consumer enters a shop with a big and obvious sign out front that the AFRS is being used, the retailer could *potentially* imply such consent (see Figure 2 below for an example of using such a construction with regard to CCTV surveillance). However, the burden of proof that consent was obtained rests on the retailer, which should motivate retailers to actively pursue consumers and to obtain such consent in writing. In addition, as a commercial setting is usually judged as public, not personal, space, the retailers cannot argue that video recording is done outside of the public space. For example, the CJEU ruled that even video surveillance of one's house and surrounding that also records an adjacent road (which constitutes public space already) requires consent of the data subjects to process such data (C-212/13, *Rynes v. Urad pro ochranu osobnich udaju*).

Figure 3. *A digital signage panel installed at Amsterdam Central Station.* On the left side is a standard advertising billboard, which is simply a TV screen and shows varying video advertisements (that is why on the left image there is a blue-colored advertisement and on the right side a red-colored advertisement even though it is the same advertising billboard). On the right side, it is a zoom-in picture of an Xbox Kinect sensor, with an assumed function of tracking the passersby (i.e., with AFRS capabilities). Xbox Kinect sensor is marked with a red rectangle. Picture taken: April 2015 by the first author.

Figure 4. *Real-life user interaction with a virtual shopping assistant in a commercial center in the Netherlands*. It is a standard TV screen with an Xbox Kinect (with AFRS) installed on top of it. In figure, the AFRS is marked with a red rectangle. The avatar is able to recognize that in front of it stands (a) a man and (b) that he is wearing a pair of glasses. The avatar greets the person with the text visible above. Reproduced with permission.

The AFRS can be used for many objectives, but it seems that so far it has only been used to either gather and later analyze biometrical data of passers-by (as in digital signage, see Figure 3) or to provide tailored, interactive, and real-time communication. In the second example, a person's biometrical data are used to react appropriately to consumers' responses, e.g., when a person looks surprised, the system could ask: "Why are you surprised?" (for an example, see Figure 4). A large retailer acting as a data controller can effortlessly ask for an informed consent from the consumer, when the purpose of data collection is an interaction with the system in real time, because currently people have to stand in front of the system to interact with it. In addition, scholars could argue that if a consumer chooses to engage with such a system that would qualify as an informed consent. In particular, the assumption of informed consent would be more robust if the system began by introducing itself and explaining the purposes for which it is being used, such as data collection and processing.

The situation looks different in the case of digital retail signage. In this scenario, the AFRS is often hidden and not instantly visible to passers-by. Therefore, it is difficult to suggest how retailers may appropriately obtain informed consent.

It is obvious that consent can be given orally to a computer or by unambiguous gestures that can be recognized. For the consent to be informed, the consumer must be aware of the fact that (1) there is a CCTV system in operation and (2) it is used for facial recognition purposes. Even though the Article 29 Working

Party has emphasized that consent "cannot be derived from the general user's acceptance of the overall terms and conditions of the underlying service unless the primary aim of the service is expected to involve facial recognition" (Opinion 3/2012 on developments in biometric technologies (WP 193), p. 22), it is possible to obtain consent in connection with another interaction with the consumer, such as in the context of enrollment in a loyalty program, as long as the above-mentioned requirements are satisfied.

Anonymizing Data

Thorough anonymization of data may help retailers lawfully use the AFRS, as it significantly minimizes the impact on consumers' privacy. Specifically, data anonymization may (a) render the data protection law inapplicable, (b) help in the balancing test (minimizing the impact on the data subject), and (c) be a requirement under data minimization.

Recital 26 of the Directive provides that the principles of protection do not apply to data rendered anonymous, as the data subject is no longer identifiable. In order to "determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person." However, it follows from the definition of personal data that "an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his *physical, physiological, mental, economic, cultural, or social identity*" [emphasis added]. It is thus sufficient information to constitute personal data when "identifiers" are used to single someone out and identify the behavior and personality of that individual to attribute certain decisions to him. This includes categorizing individuals on the basis of socioeconomic, psychological, philosophical, or other criteria. (Article 29 Working Party, Opinion 4/2007 on the concept of personal data). For example, the absence of a first and last name in a publication does not protect an individual's anonymity sufficiently (as ruled in T-259/03, *Nikolaou v. Commission*).

Anonymization consists of data processing that may be justified under Article 7(1)(f) (balancing test); but the data subject's interest in protecting his privacy—including his rights to rectification, erasure, blocking objection, and to bring legal proceedings—should also be taken into account (see Case C-553/07, *College van burgemeester en wethouders van Rotterdam v M. E. E. Rijkeboer*, paragraph 64). Provided that sufficient information has been given to the data subject, it cannot be ruled out that the use of AFRS can be justified under the balancing test to the extent that data is immediately anonymized.

According to the Article 29 Working Party, it is clear "that the creation of a truly anonymous dataset from a rich set of personal data [. . .] is not a simple proposition," as a dataset considered to be anonymous may "be combined with another dataset in such a way that one or more individuals can be identified" (Opinion 05/2014 on Anonymisation Techniques (WP216), p. 5). As per this opinion, the robustness of anonymizing techniques is based on three criteria: "(1) is it still possible to single out an individual, (2) is it still possible to link records relating to an individual, and (3) can information be inferred concerning an individual?" (Ibid, p. 3). Furthermore, "an important factor is that the processing must be irreversible. Thus the outcome of anonymization should be as permanent as erasure, i.e., making it impossible to process personal data" (Ibid, p. 6). If those criteria are not fully met, this results in a pseudonymization of the data, which may allow for identifiability, and hence still be inside the data protection law scope.

Enabling recognition of consumer identity, which is generally regarded as the least important function of the AFRS, clearly qualifies as processing personal data. On the other hand, usages focused on recognizing consumer emotions and sociodemographic characteristics may not necessarily allow for the identification of consumers. Processing such data by an advanced sensor system should not be perceived as processing personal data, and thus not amount to a substantial privacy issue, unless this data could be linked to a specific individual and would, therefore, allow for his identification. That is to say, in terms spelled out in Article 29 Data Protection Working Party, such "biometric" templates should (a) "not be too large so as to avoid the risks of biometric data reconstruction" and (b) "be a one-way process, in that it should not be possible to regenerate the raw biometric data from the template" (Opinion 3/2012 on developments in biometric technologies (WP 193), p. 4). The pertinent question is whether it is possible to identify a consumer based on his pattern of emotions (e.g., first smiles, then is surprised and then smiles again). The same question may also be posed with regard to any unique sociodemographic data that is collected and processed (e.g., female, 35–40 years old, Caucasian).

Therefore, anonymization is one possible solution, provided it is (1) done well and (2) has a range of x% probability of specifically identifying a person based on "n" anonymized unique data points. For example, an anonymization of three unique data points vs. six unique data points could give, respectively, a range of 40–60% or 50–70% of probability of indirectly re-identifying a person. Empirical testing will be required (possibly in each case—see the section on *the balancing test* above). For example, de Montjoye, Radaelli, and Singh (2015) discovered that 90% of individuals could have been re-identified based only on four spatiotemporal points of their credit card metadata. The empirical question to be tested is: how many data points extracted from psychological states and sociodemographic traits of an individual are enough to identify the individual reliably?

In principle, consumer identification could occur through the collection and processing of certain

sociodemographic data, but not of emotions. There are infinitely more combinations of emotional temporal pattern responses (e.g., people can make up to 10,000 distinct combinations of facial movements at any given point; Ekman & Rosenberg, 1997) than combinations of demographic data, which would render the identification process unfeasible. As such, the gathering of sociodemographic data should be classified as potentially allowing the processing of personal data (i.e., re-identifying the person), but registering emotions should probably be taken out of this equation.

Another crucial factor in this analysis is whether the gathered type of data is *logged* (e.g., written in the file for later retrieval) with or without a unique identifier (ID number for each person). If logged data are *anonymized* (see an example of this in Figure 5), and it is impossible to restore the original data that could lead to the identification of particular customers, then, as mentioned, the issue does not involve personal data whatsoever. However, if the logged data is *not* anonymized—in other words, some or all persons receive a unique ID number—and the gathered data allows for the identification of consumers, then the large retailer gathers "personal data" in the sense of the Directive.

In order to be sure that even within anonymized data, consumers cannot be re-identified by any method, the data controller could log only aggregated data without raw files (see an example of this in Figure 6). This would hinder potential commercial insights but would increase data protection. Large retailers may not find this tradeoff attractive, because the purpose of their data collection is clearly to generate as much commercial value as possible. Those two approaches would fit into "privacy-by-design" frameworks if they were hard coded into the AFRS (e.g., Langheinrich, 2001; Schaar, 2010). Further, as Article 29 Working Party (2014) states in their "Opinion 05/2014 on Anonymisation Techniques," such anonymized data are no longer considered personal data and, hence, does not fall under the Directive.

The evaluation of the role that the AFRS could have in identifying consumers also depends on whether it allows not only for the processing of data in real time but also for storing this data. If the latter is true, it becomes important who has access to this data and how well it is protected against a security breach. A processing protocol of "do not store anything" could then be seen by large retailers as a radical solution for a "privacy incorporated" sensing system. If they do not store any facial image material, the chances of using this software for identification purposes are significantly diminished, and thus the problem of privacy issues seems to be solved. However, there are two fundamental problems with this approach.

First, an interactive expression analysis system needs to keep some local representation of personal identity over some time for reasonable performance in interaction (or in temporally integrated reporting) in order to make sense commercially. This means that even if the retailer chooses not to store the face image, the system could still be installed to allow for storing such data as the vectors of facial expression coordinates as internal system parameters (van Kuilenburg, Wiering, & den Uyl, 2005; see Figure 7A). Consequently, a veridical face reconstruction can still be produced and possibly lead to a given consumer's identification. For an example of such possible veridical face reconstruction, see Figure 7B, where the multilayered superimposed 3D mesh on the actor's face represents the same facial expression coordinates from Figure 7A. However, as mentioned earlier, such face reconstruction is still not possible (Chen et al., 2015), and the face in Figure 7B is only possible to visualize because the original facial image was also recorded and stored. According to the Article 29 Working Party, the original facial image on Figure 7B would be a source of biometric data, while Figure 7A would be actual biometric data (2012).

Importantly, the Article 29 Working Party recognizes that:

> "A template or set of distinctive features used only in a categorisation system would not, in general, contain sufficient information to identify an individual. It should only contain sufficient information to perform the categorization (e.g., male or female). In this case it would not be personal data provided the template (or the result) is not associated with an individual's record, profile or the original image (which will still be considered personal data)" (Opinion 02/2012 on facial recognition in online and mobile services (WP 192), p. 4).

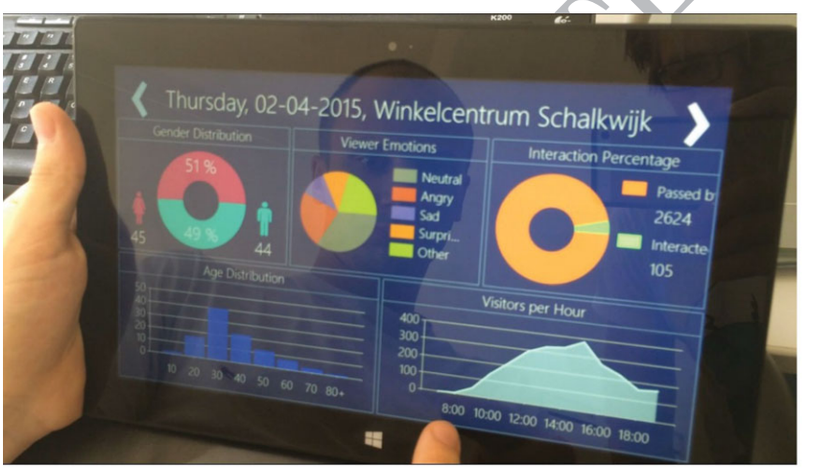
Second, personal identity verification can, in theory, be performed on any conceivable record of detailed behavioral observation. In particular, any stored temporal pattern could be used not only for identity verification (Jain, Ross, & Prabhakar, 2004), but also for more relevant, temporal facial expressions patterns, such as the ones in Figure 8 (O'Toole, Roark, & Abdi, 2002). Therefore, in the future, even if the data controller chooses not to store the facial image itself, it could still be possible to reconstruct the identity from facial expression coordinates, temporal facial expression patterns, or the combination of both.

CONCLUSIONS AND RECOMMENDATIONS

On the basis of the analyses above, it is impossible to use automated facial coding software (the AFRS) without processing personal data, which forces traders within the European Union to comply with EU privacy rules on data protection. The Article 29 Working Part has already issued an opinion on facial recognition, claiming that the advent of such technology may soon make it impossible for consumers to maintain their anonymity (Article 29 Data Protection Working

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	PersonID	TimeFirstSeen	ViewingTime	Age	Gender	Condition	Condition Name	Neutral	Happy	Sad	Angry	Surprised	Scared	Disgusted
2	7.21E+16	12:13:05	3	43	Male	1	Advertisement	0.089005	5.67E-05	0.82199	0.016072	4.88E-09	0.000502	0.118293
3	7.21E+16	12:32:44	3.1	31	Male	1	Advertisement	0.198725	0.54429	0.000291	0.000224	0.015784	0.00099	0.090388
4	7.21E+16	13:01:50	2.8	27	Female	1	Advertisement	0.312985	0.001812	0.172899	0.087655	0.003194	0.000564	0.159076
5	7.21E+16	13:04:09	1.1	40	Male	1	Advertisement	0.292159	0.025086	0.42142	0.00197	1.15E-05	0.103429	4.24E-06
6	7.21E+16	15:11:35	9.9	24	Female	1	Advertisement	0.659694	0.074598	0.000486	0.000713	0.045152	0.210804	0.001801
7	7.21E+16	15:12:30	1.8	20	Female	1	Advertisement	0.364578	0.000181	0.012879	0.27328	0.002816	3.46E-05	1.62E-06
8	7.21E+16	15:13:57	1	58	Male	1	Advertisement	0.101079	0.000178	0.798076	0.000379	4.09E-07	0.000742	0.006699
9	7.21E+16	15:23:45	3	27	Male	1	Advertisement	0.186284	2.08E-05	1.48E-05	0.02352	0.627523	0.026093	2.44E-06
10	7.21E+16	15:28:54	1.4	38	Female	1	Advertisement	0.115094	6.82E-05	0.011236	0.769812	1.44E-06	0.000176	0.114235
11	7.21E+16	15:34:50	4.3	27	Female	1	Advertisement	0.318776	0.068518	0.00448	0.295004	0.003377	0.001403	0.006383
12	7.21E+16	15:40:49	3.9	6	Female	1	Advertisement	0.02072	2.26E-05	0.003112	0.958938	3.32E-06	0.000976	0.161103
13	7.21E+16	15:42:21	3.7	20	Female	1	Advertisement	0.351017	0.012615	0.299484	0.005059	0.000126	4.17E-06	0.000446
14	7.21E+16	15:51:06	3.3	37	Female	1	Advertisement	0.452478	0.041459	2.40E-05	0.15143	0.007597	1.32E-06	0.000202
15	7.21E+16	15:51:06	3.8	25	Female	1	Advertisement	0.863384	0.129599	0.000556	0.008241	0.005943	7.86E-06	0.000862
16	7.21E+16	15:52:53	2.2	27	Female	1	Advertisement	0.437764	0.000359	0.025186	6.44E-05	0.000141	0.127482	0.00861
17	7.21E+16	08:05:42	1.2	38	Male	1	Advertisement	0.134872	8.15E-06	0.000641	0.730256	0.000108	0.379785	0.004808
18	7.21E+16	08:08:16	0.6	14	Unknown	1	Advertisement	0.185808	0.002561	0.628387	0.487267	3.76E-07	1.48E-06	0.298652
19	7.21E+16	08:10:05	1.8	14	Female	1	Advertisement	0.239689	0.003389	0.291963	0.230161	4.18E-06	0.000225	0.304602
20	7.21E+16	10:25:59	3.4	53	Male	1	Advertisement	0.319202	0.071621	0.000182	0.001364	0.011137	0.308413	0.000629
21	7.21E+16	10:27:10	1.8	25	Female	1	Advertisement	0.367216	0.01546	0.217786	0.091473	4.91E-06	0.005417	0.008874
22	7.21E+16	10:29:33	1	16	Female	1	Advertisement	0.111632	0.029986	0.003203	0.039181	1.38E-07	1.82E-06	0.776758
23	7.21E+16	10:38:51	2.5	37	Female	1	Advertisement	0.100308	0.000169	0.003236	0.80016	0.000181	0.000689	0.144127
24	7.21E+16	11:00:55	3.2	35	Unknown	1	Advertisement	0.387752	0.174256	0.000175	0.112618	1.12E-05	1.52E-06	0.061315
25	7.21E+16	11:06:08	2.9	54	Male	1	Advertisement	0.165806	0.032044	0.003337	0.000462	1.58E-05	3.65E-06	0.668388

Figure 5. *An excerpt from a database of aggregated and anonymized data from facial tracking system in a commercial center in the Netherlands*. PersonID = same ID automatically assigned to each person to anonymize the data; ViewingTime = number of second the person viewed the screen; Condition = person saw either only an interactive text with advertisements, an interactive avatar with advertisements or only the advertisements. Neutral-Disgusted = different emotions present in the person's face. Printscreen taken by the first author.



	A	B	C	D
1			avg viewtime	
2	**Text**			
3	totalPass	5988	2.9	
4	nInterested	381	11.5	6.36%
5	nSeenAds	124	24.2	2.07%
6	nFinishedAd	19	64.3	0.32%
7			102.9	
8	**Ads**			
9	totalPass	5795	2.7	
10	nInterested	270	7.3	4.66%
11	nSeenAds	60	18.9	1.04%
12	nFinishedAd	0	0	0.00%
13			28.9	
14	**Avatar**			
15	totalPass	6961	3.4	
16	nInterested	583	15	8.38%
17	nSeenAds	213	30.2	3.06%
18	nFinishedAd	49	60	0.70%
19			108.6	

A B

Figure 6. *Simple retail analytics from an AFRS in a commercial center in the Netherlands for one week in March 2015*. Part A—aggregated data in a visual form. Part B—aggregated data in numerical form; totalPass = number of people that were detected; nSeenAds = number of people that saw the advertisement, nFinishedAd = number of people that finished watching all the advertisements; avg viewtime = average viewing time for each of categories. Picture and printscreen taken by the first author.

Party, 2012). Facial recognition (and to a lesser extent, emotion recognition) for commercial purposes has been widely discussed by regulatory bodies around the world, including in the U.S. (The Federal Trade Commission, 2012), in the European Union(Article 29 Data Protection Working Party, 2012), in Canada (Research Group of the Office of the Privacy Commissioner of Canada, 2013), and in Great Britain (Hastings, October 2012).

The authors find that an informed consent by consumers to collection and further processing of personal data—in particular because of its reliability as a legal basis—plays an important role in lawful use of the

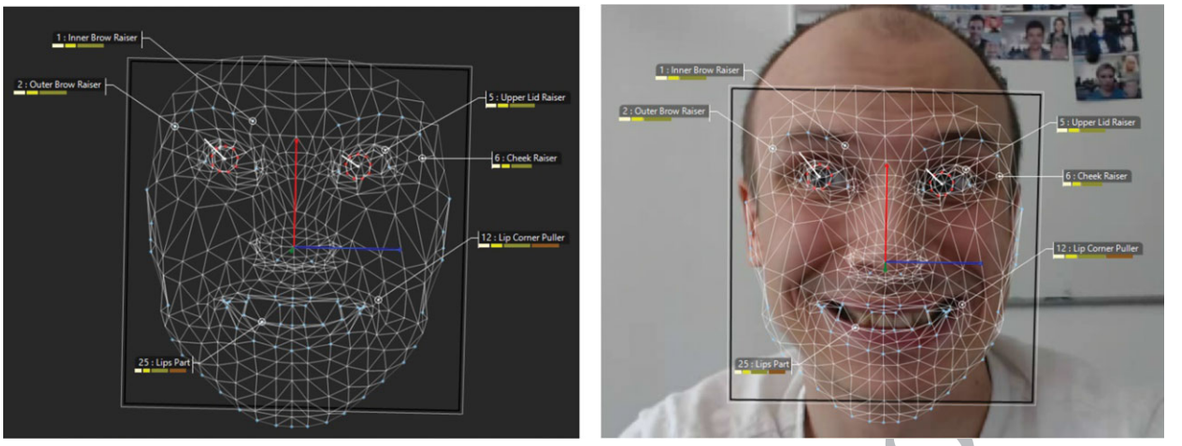


Figure 7. . (A) Left: —*Facial expression and (B) right: identify recognition.* Picture and printscreen taken by the first author. Q10

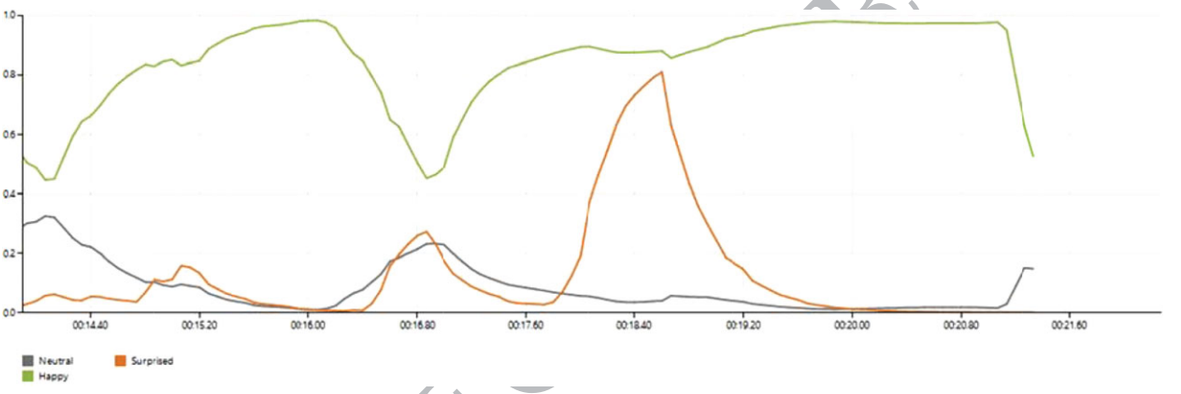


Figure 8. *An example of a temporal facial expression pattern*. The *x*-axis shows time interval in seconds, the *y*-axis shows intensity and probability of one of the emotions (happy, surprised, neutral) on a scale from 0.0 to 1.0. Different colors indicate different emotions; see a legend below the *x*-axis.

AFRS, thus the recommendations of this paper focus on this element. However, it cannot be ruled out that the AFRS can be used lawfully based on the balancing test, provided that the system is not used for identification and the personal data and the trader (data controller) apply the above-mentioned measures to limit the impact on the data subjects. However, it is the trader's responsibility to comply with the law, which is the reason that the authors recommend informed consent as the basis for processing personal data; in particular, because consumers are not likely to be aware of the existence of and possibilities in these technologies.

With regard to a retailer obtaining consumers' explicit informed consent to the operation of the AFRS, one solution would be the creation of "members only" stores. There are some shops, such as Macro or Hanos (in the Netherlands), that already only allow their members and their invitees to enter the premises. When registering for a loyalty program, a consumer could be informed in detail about the AFRS and its purposes, and be required to consent thereto. The possibility granted to the members of such shops to bring invitees with them presents a small problem, because they would need to sign a similar disclosure. If that should prove problematic, instead of creating "members only" shops, a retailer desiring to use the AFRS could set up a secured entrance to the shopping mall. The retailer would then only grant access to the store to people having, for instance, watched a one-minute long video on the AFRS and its purposes, and who have subsequently clicked on the "I agree" button or otherwise indicated their consent unambiguously.

Both of these solutions should clearly stipulate that consumers agree to have their data processed in accordance with the Data Protection Directive (1995). Unfortunately, neither of these solutions are easy to implement, and they could discourage the retail stores' owners from applying the AFRS in practice. However, it is possible to frame the use of the AFRS as a benefit for the consumer, who—considering the wide use of social media, etc.—do not seem concerned about trading privacy for convenience. Above-mentioned loyalty shops such as Macro or Hanos are pioneers in the adoption of this technology and may provide practical examples of lawful use of the AFRS.

Because large retailers may be convinced that making their shops less accessible could discourage their patrons from visiting them, they would be more likely to lobby the legislators and legal enforcement to be more flexible with regard to what should be perceived as the processing of personal data and as an explicit informed consent. For example, they could claim that if the AFRS does not allow the storage of consumer data and only collects information on consumers' emotion and sociodemographic characteristics, the possibility of consumer identification diminishes and, therefore, the AFRS does not process personal data. They could also argue that if the equipment used by the AFRS is separate from the surveillance equipment, consumers would not easily confuse it for a security surveillance system and, therefore, they could just by shopping in a store with visible AFRS equipment consent to its operation. If one of the above-mentioned solutions could be applied, especially in combination with the anonymization and aggregation of consumers' data, this could provide a good balance between the need to protect consumer privacy and allowing retailers to obtain valuable commercial insights from such data.

THE FUTURE OF THE AFRS IN RETAIL

Today, the AFRS may be used to read consumers' emotions and predict their decisions. In a colloquial way, this is likely to be perceived as infringing with consumers' privacy, since it gives retailers insights into the consumers' thoughts and feelings. To the extent the gathered data allows for identification of consumers, it should be treated as personal data from a legal perspective, and the expectation would be for the AFRS to be in compliance with EU data protection laws.

However, these privacy concerns are only the beginning of issues to be faced in the future. AFRS technologies will be integrated into single automated systems, which are capable of remotely and automatically determining the affective and cognitive states of consumers, based entirely on their upper body posture and other cues. Below is a list of some existing technologies that register physiological information about consumers, and which can be combined to move away from separate channels of input into one complex system interpreting both affective and cognitive states, with low economic costs involved to run it all together. Such systems are already in place (e.g., see iMotions, which is a "biometric platform for eye tracking software, facial expression analysis, EEG and GSR—all synchronized;" iMotions, 2015).

By integrating such systems, it will be possible to remotely gather the following data on physiological and psychological signals by observing consumers' upper body: (a) facial expressions, such as basic emotions (Ekman & Friesen, 1969; Lewinski, 2015c), valence and arousal (Russell, 1980, 2003), specific Facial Action Coding System ("FACS") action units (Ekman & Rosenberg, 1997); (b) heart rate and variability through remote PPG (Tasli et al., 2014); (c) eye gaze, number of eye blinks, head position, and movement (attention indicator) (see manual of FaceReader, 2015); (d) respiratory rates (Bartula, Tigges, & Muehlsteff, July 2013); and (e) gesture/body tracking (Bouma et al., October 2013) (used to establish stress levels, interests, or where the person will go next).

Furthermore, because all these systems are camera based, it is possible to use them with infrared lights, which enables the measuring of these signals in total darkness. Lastly, with more expensive and dedicated hardware, even more capabilities can be added. For example, with regard to eye tracking, if a better measure of pupil dilation and of the exact position of the consumer's gaze were introduced, it would offer a higher accuracy than only the use of camera-based estimations (Cavanagh, Wiecki, Kochar, & Frank, 2014). Therefore, an inevitable advancement in number and precision of biometric measures is looming. In the future, the crucial privacy questions will be which inputs are treated as personal data and at which point the combination of inputs will allow for almost unequivocal identification of individuals.

An interesting paradox that could arise in the near future would be a switch to tailor-made privacy protection, pursuant to consumer needs and requests. In order to observe consumer privacy pursuant to their individual needs, existing software would need to first gather data on and to identify a given consumer. Only upon conducting identification of a consumer, the software could know the particular consumer's privacy preferences. Considering that the coming years are likely to bring about an increase in high surveillance within "city" environments, with citizens continuously being watched from multiple cameras, phones, tablets, and dedicated surveillance systems, the introduction of design software allowing the blockage of some of these images and the disabling of personal data processing functions can be expected. It would definitely be of interest to consumers if a reliable "I am here incognito" or "do not track me" protocol could be developed for a single web-based or multiple-connected person observation system, similar to incognito or "track the trackers" settings in a web browser (Ohana & Shashidhar, 2013). However, in order for such different subsystems to respect consumers' privacy preferences, these systems will have to agree on a consumer's local identity in some way. A machine decision-making pattern might go something like this: "Is this another image of X who did not want to be recorded?"; "It is impossible to determine, all reference materials on X were just deleted."

The Article 29 Working Party recognizes this issue and understands that a retailer (i.e., a data controller) could actually perform such identification to establish if a customer has provided informed consent or not:

> "[. . .] the data controller may [. . .] assess whether a user has provided consent or not as a legal basis for the processing. This initial processing (i.e. image acquisition, face detection, comparison, etc)

may in that case have a separate legal basis, notably the legitimate interest of the data controller to comply with data protection rules. Data processed during these stages should only be used for the strictly limited purpose to verify the user's consent and should therefore be deleted immediately after" (Opinion 02/2012 on facial recognition in online and mobile services (WP 192), p.5).

From 25 May 2018 the newly adopted General Data Protection Regulation (Regulation (EU) 2016/679 of 27 April 2016) will enter into force. This data protection reform will strengthen data protection, which entails that the analyses and conclusions presented in this paper will still be applicable. The reform entails stronger (more centralized) enforcement and substantial administrative fines of up to EUR 20,000,000, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year (whichever is higher, see Article 83). The principles of importance for the present analyses concerning purpose, data quality, justification, and consent are largely unaltered by these new developments. However, the Regulation contains more detailed requirements concerning consent (Article 7), along with revised provisions on profiling (Article 22) combined with particular rules on biometric data. Biometric data includes "data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images [. . .]," which are categorized as sensitive data (Article 9) that in this context requires consent for processing to be lawful. Thus, the recommendation of the researchers to acquire consent is only further emphasized. In addition, the regulation requires the trader to carry out an assessment of the impact of the envisaged processing operations prior to the processing ("impact assessment", see Article 35).

REFERENCES

AdMobilize (2015). Retrieved from http://web.admobilize.com/.

AmScreen (2015). Retrieved from http://www.amscreen.eu.

Article 29 Data Protection Working Party (2011). Opinion 15/2011 on the definition of consent. 01197/11/EN WP187.

Article 29 Data Protection Working Party (2012a). Opinion 02/2012 on facial recognition in online and mobile services, March 22, 2012. 00727/12/EN WP 192.

Article 29 Data Protection Working Party (2012b). Opinion 3/2012 on developments in biometric technologies, April 27, 2012. 00720/12/EN WP193.

Article 29 Data Protection Working Party (2014a). Opinion 05/2014 on anonymization techniques, April 10, 2012. 0829/14/EN WP216.

Article 29 Data Protection Working Party (2014b). Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC. 844/14/EN WP 217.

Atrey, P. K., Kankanhalli, M. S., & Cavallaro, A. (2013). Intelligent multimedia surveillance: Current trends and research. Berlin, Heidelberg: Springer.

Axis. (2015). Retrieved from http://www.axis.com/global/en/products/network-cameras.

Bartula, M., Tigges, T., & Muehlsteff, J. (2013, July). Camera-based system for contactless monitoring of respiration. In Engineering in Medicine and Biology Society (EMBC), 2013 35th Annual International Conference of the IEEE (pp. 2672–2675), IEEE.

Bishop, C. M. (1995). Neural networks for pattern recognition. Oxford: Clarendon Press.

Bouma, H., Baan, J., Borsboom, S., van Zon, K., Luo, X., Loke, B., et al. (2013, October). WPSS: Watching people security services. In SPIE Security+ Defence (pp. 89010H-89010H). International Society for Optics and Photonics.

Buckley, B., & Hunter, M. (2011). Say cheese! Privacy and facial recognition. Computer Law & Security Review, 27, 637–640.

Bulling, A., & Gellersen, H. (2010). Toward mobile eye-based human-computer interaction. IEEE Pervasive Computing, 9(4), 8–12.

Cavanagh, J. F., Wiecki, T. V., Kochar, A., & Frank, M. J. (2014). Eye tracking and pupillometry are indicators of dissociable latent decision processes. Journal of Experimental Psychology: General, 143(4), 1476.

Charter of Fundamental Rights of the European Union (2012). Official Journal of the European Union, c 326/02.

Charters, D. (2002). Electronic monitoring and privacy issues in business-marketing: The ethics of the DoubleClick experience. Journal of Business Ethics, 35, 243–254.

Chen, F., Xu, Y., Zhang, D., & Chen, K. (2015). 2D facial landmark model design by combining key points and inserted points. Expert Systems with Applications, 42(21), 7858–7868. doi:10.1016/j.eswa.2015.06.015

CNET. (2015). Delve into DIY security with these 35 connected cameras. Retrieved from http://www.cnet.com/news/security-camera-roundup/.

Cootes, T., & Taylor, C. (2000). Statistical models of appearance for computer vision. Technical report, University of Manchester, Wolfson Image Analysis Unit, Imaging Science and Biomedical Engineering.

Council of the European Union (2015). Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) - Chapters I and XI. Retrieved from http://data.consilium.europa.eu/doc/document/ST-7700-2015-INIT/en/pdf.

CSC. (2015). New csc research reveals where shoppers and retailers stand on next generation in-store technology. Retrieved from http://www.csc.com/uk/press_releases/133753-new_csc_research_reveals_where_shoppers_and_retailers_stand_on_next_generation_in_store_technology.

Data Protection Directive. (1995). Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

de Andrade, N. N. G., Martin, A., & Monteleone, S. (2013). All the better to see you with, my dear: Facial recognition and privacy in online social networks. IEEE security & privacy, 11(3), 21–28.

de George, R. T. (2001). Law and Ethics in the Information Age. Business & Professional Ethics Journal, 20, 5–18.

de Montjoye, Y. A., Radaelli, L., & Singh, V. K. (2015). Unique in the shopping mall: On the reidentifiability of credit card metadata. Science, 347(6221), 536–539. doi:10.1126/science.1256297

Dickie, C., Vertegaal, R., Sohn, C., & Cheng, D. (2005, October). eyeLook: Using attention to facilitate mobile media consumption. In Proceedings of the 18th annual ACM symposium on User interface software and technology (pp. 103–106). ACM.

Directive on Privacy and Electronic Communications. (2002). Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.

Eaglevision. (2015). Retrieved from www.eaglevision.nl.

Ekman, P., & Friesen, W. V. (1969). Nonverbal leakage and clues to deception. Psychiatry, 32(1), 88–10

Ekman, P., & Rosenberg, E. L. (1997). (Eds.), What the face reveals: Basic and applied studies of spontaneous expression using the Facial Action Coding System (FACS). Chicago: Oxford University Press.

European Commission (2015a). Data Protection Reform and Big Data: Factsheet. Retrieved from http://ec.europa.eu/justice/data-protection/files/data-protection-big-data_factsheet_web_en.pdf.

European Commission (2015b). Data Protection Day: Concluding the EU Data Protection Reform essential for the Digital Single Market. Retrieved from http://europa.eu/rapid/press-release_MEMO-15-3802_en.htm?locale=EN.

FaceReader Online. (2015). Retrieved from http://www.facereader-online.com.

FaceReader. (2015). FaceReader: Tool for automated analysis of facial expression: Version 6.0. Wageningen, The Netherlands: Noldus Information Technology B.V.

Global Industry Analysts. Digital signage: The right information in all the right places ITU-T Technology Watch Report November 2011.

Hastings, R. (2012). New HD CCTV puts human rights at risk. Independent. Retrieved from http://www.independent.co.uk/news/uk/crime/new-hd-cctv-puts-human-rights-at-risk-8194844.html.

Helberger, N., Guibault, L., Loos, M., Mak, C., Pessers, L., & Van Der Slot, B. (2013). Digital consumers and the law. Alphen aan den Rijn: Kluwer Law International.

Hill, K. (2011). Kraft to use facial recognition technology to give you macaroni recipes. Forbes, Retrieved September 1, 2011, from http://www.forbes.com/sites/kashmirhill/2011/09/01/kraft-to-use-facial-recognition-technology-to-give-you-macaroni-recipes/.

I3b. (2015a). Retrieved from http://www.i3b.org/.

I3b. (2015b). Retrieved from http://www.i3b.org/content/facilities

IMCO (Committee on the Internal Market and Consumer Protection of the European Parliament). (Consumer Behaviour in a Digital Environment: Study. Retrieved August 2011, from http://www.europarl.europa.eu/committees/en/studiesdownload.html?languageDocument=EN&file=42591.

iMotions. (2015). Retrieved from http://imotions.com/.

IMRSV. (2015). Retrieved from https://www.imrsv.com/.

Intel. (2015). Retrieved from http://www.intel.com.

Introna, L. D. (2005). Disclosive ethics and information technology: Disclosing facial recognition systems. Ethics and Information Technology, 7, 75–86.

Jackson, J. E. (1991). A user's guide to principal components. John Wiley and Sons, Inc.

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

Langheinrich, M. (2001). Privacy by design—principles of privacy-aware ubiquitous systems. In Ubicomp 2001: Ubiquitous computing (pp. 273–291). Berlin Heidelberg: Springer.

Lewinski, P. (2015a). Automated facial coding software outperforms people in recognizing neutral faces as neutral from standardized datasets. Frontiers in Psychology, 6, 1386. doi:10.3389/fpsyg.2015.01386

Lewinski, P. (2015b). Don't look blank, happy, or sad: Patterns of facial expressions of speakers in banks' YouTube videos predict video's popularity over time. Journal of Neuroscience, Psychology, and Economics, 8(4), 241–249. doi:10.1037/npe0000046

Lewinski, P. (2015c). Commentary: Rethinking the development of "nonbasic" emotions: A critical review of existing theories. Frontiers in Psychology, 6, 1967. doi:10.3389/fpsyg.2015.01967

Lewinski, P., den Uyl, T. M., & Butler, C. (2014). Automated facial coding: Validation of basic emotions and FACS AUs recognition in FaceReader. Journal of Neuroscience, Psychology, and Economics, 7(4), 227–236. doi:10.1037/npe0000028.

Lewinski, P., Fransen, M. L., & Tan, E. S. H. (2014). Predicting advertising effectiveness by facial expressions in response to amusing persuasive stimuli. Journal of Neuroscience, Psychology, and Economics, 7(1), 1–14. doi:10.1037/npe0000012

Lewinski, P., Tan, E. S. H., Fransen, M. L., Czarna, K., & Butler, C. (2016). Hindering facial mimicry in ad viewing: Effects on consumers' emotions, attitudes and purchase intentions. Advances in advertising research (Vol. 6, pp. 281–288). Springer.

Luzak, J. (2013). Much Ado about Cookies: The European Debate on the New Provisions of the ePrivacy Directive regarding Cookies. European Review of Private Law, 1, 221–246.

Luzak, J. (2014). Privacy Notice for Dummies? Towards European Guidelines on How to Give "Clear and Comprehensive Information" on the Cookies' Use in Order to Protect the Internet Users' Right to Online Privacy. Journal of Consumer Policy, 37, 547–559.

McClurg, A. J. (2007). In the face of danger: Facial recognition and the limits of privacy law. Harvard Law Review, 120(7), 1870–1891.

Milne, G. R., & Culnan, M. J. (2004). Strategies for reducing online privacy risks: why consumers read (or don't read) online privacy notices. Journal of Interactive Marketing, 18, 15.

Miyazaki, A. D. (2008). Online privacy and the disclosure of cookie use: effects on consumer trust and anticipated patronage. Journal of Public Policy & Marketing, 27, 19–33.

Noldus. (2015). Retrieved from http://www.noldus.com/about-noldus.

Nowak, G. J., & Phelps, J. (1995). Direct marketing and the use of individual-level consumer information: Determining how and when "privacy" matters. Journal of Direct Marketing, 9, 46.

Ohana, D. J., & Shashidhar, N. (2013). Do private and portable web browsers leave incriminating evidence?: A forensic analysis of residual artifacts from private and portable web browsing sessions. EURASIP Journal on Information Security, 2013(1), 1–13.

Olsen, S. (2002, March 31). Can face recognition keep airports safe? *CNET*. Retrieved from http://www.cnet.com/news/can-face-recognition-keep-airports-safe/

Olszanowski, M., Pochwatko, G., Kuklinski, K., Scibor-Rylski, M., Lewinski, P., & Ohme, R. K. (2015). Warsaw Set of Emotional Facial Expression Pictures: A validation study of facial display photographs. Frontiers in Psychology, 5(1516). doi:10.3389/fpsyg.2014.01516.

O'Toole, A. J., Roark, D. A., & Abdi, H. (2002). Recognizing moving faces: A psychological and neural synthesis. Trends in cognitive sciences, 6(6), 261–266.

Palmer, D. E. (2005). Pop-Ups, Cookies, and Spam: Toward a Deeper Analysis of the Ethical Significance of Internet Marketing Practices. Journal of Business Ethics, 58, 271–280.

Quividi. (2015). Retrieved from http://www.quividi.com/.

Research Group of the Office of the Privacy Commissioner of Canada. (2013). Automated Facial Recognition in the Public and Private Sectors Report. Retrieved from www.priv.gc.ca/information/research-recherche/2013/fr_201303_e.asp.

Russell, J. A. (1980). A circumplex model of affect. Journal of Personality and Social Psychology, 39(6), 1161.

Russell, J. A. (2003). Core affect and the psychological construction of emotion. Psychological review, 110(1), 145

Schaar, P. (2010). Privacy by design. Identity in the Information Society, 3(2), 267–274.

Senior, A. W. (2009). Protecting privacy in video surveillance. Dordrecht; New York: Springer.

Shi, J., Samal, A., & Marx, D. (2006). How effective are landmarks and their geometry for face recognition?. Computer Vision and Image Understanding, 102(2), 117–133. doi:10.1016/j.cviu.2005.10.002

Silver, H., Goodman, C., Knoll, G., & Isakov, V. (2004). Brief emotion training improves recognition of facial emotions in chronic schizophrenia. A pilot study. Psychiatry Research, 128, 147–154.

Singer, N. (2014, February 1). When no one is just a face in the crowd. The New York Times. Retrieved from http://www.nytimes.com/2014/02/02/technology/when-no-one-is-just-a-face-in-the-crowd.html?_r=1.

Stanley, J., & Steinhardt, B. (2002). Drawing a Blank. Humanist, 62, 14–17.

Tasli, H. E., Gudi, A., & den Uyl, M. (2014, October). Remote PPG based vital sign measurement using adaptive facial regions. In Image Processing (ICIP), 2014 IEEE International Conference on (pp. 1410-1414). IEEE.

The Federal Trade Commission. (2012). Facing Facts: Best practices for Common Uses of Facial Recognition Technologies.. Retrieved October 2012, from https://www.ftc.gov/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies.

Tobi. (2015). Retrieved from http://www.tobii.com.

Trepte, S., & Reinecke, L. (.eds.) (2011). Privacy Online. Berlin, Heidelberg: Springer Berlin Heidelberg.

Trzaskowski, J., Savin, A., Lundqvist, B., & Lindskoug, P. (2015). Introduction to EU Internet Law. Copenhagen: Ex Tuto Publishing.

Ubisense. (2015). Retrieved from http://ubisense.net/en/products/smart-factory.

van Kuilenburg, H., Wiering, M., & den Uyl, M. (2005). A model based method for facial expression recognition. In D. Hutchison, T. Kanade, J. Kittler, J.M. Kleinberg, F. Matern, J.C. Mitchell, M. Noar, & G. Weikum (Eds.), Lectures notes in computer science: Vol. 3720. Machine Learning: ECML 2005 (pp. 194–205). Berlin, Germany: Springer-Verlag. doi:10.1007/11564096_22.

VicarVision. (2016). Retrieved from http://www.vicar analytics.com/.

Viola, P., & Jones, M., 2004. Robust Real-time Face Detection. International Journal of Computer Vision 57(2), 137–154.

Wadhwa, T. (2012). What Do Jell-O, Kraft, and Adidas have in common? They all want to know your face. Forbes. Retrieved 8 August 2012, from http://www.forbes.com/sites/singularity/2012/08/08/billboards-and-tvs-detect-your-face-and-juice-up-ads-tailored-just-for-you/.

Waldo, J., Lin, H. S., & Millett, L. I. (2007). Engaging privacy and information technology in a digital age. Washington, D.C.: National Academic Press.

Witzleb, N. (2014). Emerging challenges in privacy law: Comparative perspectives. New York: Cambridge University Press.

Wright, D., & Kreissl, R. (2015). Surveillance in Europe. London, New York: Routledge.

Yampolskiy, R. V., & Govindaraju, V. (2008). Behavioural biometrics: A survey and classification. International Journal of Biometrics, 1(1), 81–113.

Some of the research leading to these results has received funding from the People Programme (Marie Curie Actions) of the European Union's Seventh Framework Programme FP7/2007-2013/ under REA grant agreement 290255. The first author thanks Marten den Uyl for useful first insights on this paper.

Correspondence regarding this article should be sent to: Peter Lewinski, Faculty of Economics, Université de Neuchâtel (peter.lewinski@gmail.com).

Author Query Form

Journal **MAR**

Article **mar20913**

Dear Author

During the copy-editing of your paper, the following queries arose. Please respond to these by marking up your proofs with the necessary changes/additions. Please write your answers clearly on the query sheet if there is insufficient space on the page proofs. If returning the proof by fax do not write too close to the paper's edge. Please remember that illegible mark-ups may delay publication.

Query No.	Description	Remarks
Q1	Author: Please confirm that given names (red) and surnames/family names (green) have been identified correctly.	
Q2	Wiley: Please check affiliations 1 and 3 as typeset for correctness.	
Q3	Ref. Buckley & Hart (2011) has not been included in the Reference List, please supply full publication details.	
Q4	Author: The reference citation "Tobii (2015)" has been changed to "Tobi (2015)" to match the reference list.	
Q5	Author: Ref. "Park et al., 2014" has not been included in the Reference List, please supply full publication details.	
Q6	Author: Please check Ref. citation "Charter of Fundamental Rights of the European Union (2012)" as typeset for correctness.	
Q7	Author: The Ref. "Herlberger et al., (2013)" has been changed to "Herberger et al., (2013)" to match the Reference List, please check.	
Q8	Wiley: Please check citation of Figure 7A and Figure 7B in the text as typeset for correctness.	
Q9	Author: Please check whether "2012a" or "2012b" is intended in the Ref. citation "Article 29 Data Protection Working Party, 2012."	
Q10	Author: Please check caption of Fig. 7 as typeset for correctness.	
Q11	Author: If Ref. "AmScreen 2015" has not been cited in the text. Please indicate where it should be cited; or delete from the Reference List.	
Q12	Author: Please provide the title in Refs. "AdMobilize 2015" and "AmScreen 2015."	
Q13	Author: Please provide accessed date when the URLs were last accessed in all URLs type references.	
Q14	Wiley: Please check Ref. "Article 29 Data Protection Working Party 2011" as typeset for correctness.	
Q15	Wiley: Please check Ref. "Article 29 Data Protection Working Party 2012a" as typeset for correctness.	
Q16	Wiley: Please check Ref. "Article 29 Data Protection Working Party 2012b" as typeset for correctness.	
Q17	Wiley: Please check Ref. "Article 29 Data Protection Working Party 2014" as typeset for correctness.	

Q18	Author: Please check Ref. “Article 29 Data Protection Working Party 2014a” as typeset for correctness.	
Q19	Author: If Ref. “Article 29 Data Protection Working Party 2014a” and “Article 29 Data Protection Working Party 2014b” have not been cited in the text. Please indicate where it should be cited; or delete from the Reference List.	
Q20	Wiley: Please check Ref. “Article 29 Data Protection Working Party 2014b” as typeset for correctness.	
Q21	Author: Please provide the title in Ref. “Axis, 2015.”	
Q22	Author: Please provide the publisher location for Ref. “Bartula et al. 2013.”	
Q23	Author: Please provide publisher location for Ref. “Bouma et al., 2013.”	
Q24	Author: If Ref. “Cavanagh et al., 2014” is not a one-page article please supply the first and last pages.	
Q25	Author: Please provide all publication details for Ref. “Charter of Fundamental Rights of the European Union 2012.”	
Q26	Author: Please provide publisher location for Ref. “Cootes and Taylor, 2000.”	
Q27	Wiley: Please check “Data Protection Directive, 1995” as typeset for correctness.	
Q28	Author: Ref. “de George, 2001” has not been cited in the text. Please indicate where it should be cited; or delete from the Reference List.	
Q29	Author: Please provide publisher location for Ref. “Dickie et al., 2005.”	
Q30	Wiley: Please check “Directive on Privacy and Electronic Communications 2002” as typeset for correctness.	
Q31	Author: If Ref. “Directive on Privacy and Electronic Communications 2002” has not been cited in the text. Please indicate where it should be cited; or delete from the Reference List.	
Q32	Author: Please provide journal title for Ref. “Eaglevision 2015.”	
Q33	Author: Please provide title in Ref. “FaceReader Online 2015.”	
Q34	Author: Ref. “Global Industry Analysts” has not been cited in the text. Please indicate where it should be cited; or delete from the Reference List.	
Q35	Author: Please provide year of publication for Ref. “Global Industry Analysts.”	
Q36	Author: Please provide title in Refs. “I3b, 2015a” and “I3b, (2015b).”	
Q37	Author: Please provide publisher location for Ref. “Jackson, 1991.”	
Q38	Author: If Ref. “Lewinski, 2015c” is not a one-page article please supply the first and last.	
Q39	Author: Please provide publisher location for Ref. “Lewinski et al., 2016.”	
Q40	Ref. “McClurg, 2007” has not been cited in the text. Please indicate where it should be cited; or delete from the Reference List.	
Q41	Author: If Ref. “Milne and Culnan, 2004” is not a one-page article please supply the first and last pages.	
Q42	Author: Please provide title for Ref. “Noldus, 2015.”	

Q43	Author: If Ref. “Nowak and Phelps, 1995” is not a one-page article please supply the first and last pages.	
Q44	Author: Please provide page range for Ref. “Olszanowski et al., 2015.”	
Q45	Author: Please provide title for Ref. “Quividi 2015.”	
Q46	Author: If Ref. “Russell, 1980” is not a one-page article please supply the first and last pages.	
Q47	Author: If Ref. “Russell, J. A” is not a one-page article please supply the first and last pages.	
Q48	Author: Please provide publisher location for Ref. “Tasli et al., 2014.”	
Q49	Author: Please provide title for Ref. “Tobi 2015.”	
Q50	Ref. “Trepte & Reinecke, 2011” has not been cited in the text. Please indicate where it should be cited; or delete from the Reference List.	
Q51	Author: Please provide title for Ref. “Ubisense 2015.”	
Q52	Author: Please provide title for Ref. “VicarVision 2016.”	
Q53	Ref. “Waldo et al., 2007” has not been cited in the text. Please indicate where it should be cited; or delete from the Reference List.	
Q54	Ref. “Yampolskiy and Govindaraju, 2008” has not been cited in the text. Please indicate where it should be cited; or delete from the Reference List.	
Q55	Please check funding information and confirm its correctness.	
Q56	Author: Please provide a current full postal address (including post/zip code) for the corresponding author.	