J Multidisciplinary Scientific Journal

Article

Nothing to Be Happy about: Consumer Emotions and AI

Mateja Durovic [1,*] and Jonathon Watson [2,*]

[1] Reader in Law, Dickson Poon School of Law, Kings College London, Strand, London WC2R 2LS, UK
[2] Post-Doc Researcher, Faculty of Law and Administration of the Jagiellonian University, Golebia 24, 31-007 Krakow, Poland
* Correspondence: mateja.durovic@kcl.ac.uk (M.D.); j.m.watson@uni-muenster.de (J.W.)

Abstract: Advancements in artificial intelligence and Big Data allow for a range of goods and services to determine and respond to a consumer's emotional state of mind. Considerable potential surrounds the technological ability to detect and respond to an individual's emotions, yet such technology is also controversial and raises questions surrounding the legal protection of emotions. Despite their highly sensitive and private nature, this article highlights the inadequate protection of emotions in aspects of data protection and consumer protection law, arguing that the contribution by recent proposal for an Artificial Intelligence Act is not only unsuitable to overcome such deficits but does little to support the assertion that emotions are highly sensitive.

Keywords: AI; consumer law; new technologies; regulation; emotions; EU Law

check for updates

Citation: Durovic, M.; Watson, J. Nothing to Be Happy about: Consumer Emotions and AI. *J* **2021**, *4*, 784–793. https://doi.org/10.3390/j4040053

Academic Editors: Ugo Pagallo and Massimo Durante

Received: 17 October 2021
Accepted: 9 November 2021
Published: 16 November 2021

1. Introduction

The advancements in artificial intelligence (AI) technologies together with the diverse amounts of insights that can be derived from the immense volume of (consumer) data has allowed for the development of a range of new and innovative consumer goods and services which detect and respond in real time to a consumer's emotional state. Such ability to interact with technology on a highly intimate and personal level thereby adds new dimension to the personalisation of consumer interaction with such products. Whereas considerable potential surrounds the technological ability to detect and respond to an individual's emotions, it is not without controversy due to the highly sensitive and private nature of emotions.

The capability of AI technologies in relation to emotions has not escaped the attention of the European Commission. Its recent proposal for an Artificial Intelligence Act (PAIA; COM (2021) 206 final) makes express reference to Emotion Recognition Systems (ERS) not only in relation to their use by public authorities but also provides for rules applicable in the consumer context.

In this paper, we give insights into the PAIA as proposed *de lege ferenda* and consider the implications of emotions and ERS in relation to the protection of the consumer. We begin with an overview of emotions and AI, in which we highlight applications of the nascent technology and underlying questions about the legal classification of emotions in data protection law (Section 2). This is followed by an analysis of the inadequate treatment of emotions in the Commission's proposal for an Artificial Intelligence Act (Section 3). In our penultimate section, we look at the role to be played by certain transparency obligations in consumer law *de lege lata* (Section 4) before concluding that the potential applications of AI with relation to emotions require a more robust legal framework (Section 5).

2. Emotions and AI

The potential for computing to relate to, arise from, or influence emotions is not a new phenomenon. Already in 1995, the term 'affecting computing' was coined for such applications [1] Today, the term 'Emotion AI' (or 'emotional AI') is used to describe the use of affective computing together with AI—via predetermined rules or Big Data analytics [2]—in order to 'autonomously sense expressions and behaviour, profile, learn, simulate understanding and react' [3]. Such capabilities allow for new levels of personalisation and understanding of consumer behaviour, impacting on the interaction between humans and technology as well as interpersonal relationships [3].

2.1. Application

The use of 'emotion AI' in such interactions and interpersonal relationships may be in its infancy, but the technology is nevertheless growing in its application. Although considerable doubt has been cast on the accuracy of such systems, especially facial expression detection [4,5], dismissing the technology in its current form would not be in line with a future-proof approach to the legal framework, especially as the advancements in data capture allow for an individual's emotions to be identified or inferred from data acquired from various sources. Whereas facial expressions and voice are the two common forms of 'sentic modulation' [1], the analysis of words and images, gaze and gestures, gait, and physiological responses (such as heart rate, blood pressure, respiratory patterns, body temperature, skin conductance, and pupillary dilation), as well as the physical interaction with the device itself (e.g., through the force exerted), also provide the data from which inferences about an individual's emotional state of mind can be drawn [1,6–11].

Using this and other data for context (e.g., location or even weather), the emotion can be inferred at degrees and speeds exceeding human capabilities to allow for real time interactions and responses [1,12]. For instance, the data acquired from eye tracking may reveal not just a particular emotion but also its intensity [8].

Whereas the technology has been highlighted as being especially controversial in relation to its use by the state for law enforcement and border control purposes [5], emotion AI also features in a range of consumer goods and services. Examples include the interactions with customers calling service hotlines: voice analysis at the automated stage of customer service hotlines allows for 'angry' consumers to be redirected to a human operator who, with the support of AI, can receive real-time information on how to manage the conversation and how to best engage with the caller [2]. Vehicles equipped with a range of sensors can respond to indicators of driver tiredness or aggression thus contributing to better road safety (e.g., Hyundai's 'Emotion Adaptive Vehicle Control' (EVAC)). Streaming services as well as voice assistants can recommend content based on the user's emotional state of mind [12]. More novel applications include emotion detection devices to assist autistic people in their daily lives [13], or 'BioEssence', a device that infers the emotional state based on the user's heart and respiratory rates and releases a calming or uplifting scent where appropriate.

Such examples reflect the benevolent use of emotions in technology to advance not only an individual's well-being and quality of life but also contribute to the worthwhile goal of a safer and more efficient society. Nonetheless, all that glitters is not gold. Emotions are of course 'potent, pervasive, predictable, sometimes harmful and sometimes beneficial drivers of decision making' [14]. In this respect, the reference to 'the battle to control, influence or manipulate emotions' [12] highlights the potential for malevolent use by exploiting an individual's emotional state for profit (e.g., through targeted advertising or prices), but also the short- and long-term effects on psychological and behavioural development [15].

2.2. Emotions as Data

Data are required for AI to determine a person's emotional state. As can be seen from the preceding section, various sensors capture and provide the data necessary for this purpose. In essence, details about an individual's emotional state are ultimately automated inferences drawn from the data provided and the statistical similarities with a particular quality ('profiling') (for details [16]). How such inferences are protected under the EU General Data Protection Regulation 2016/679 ('GDPR') is subject to debate with regard to whether inferences are viewed as personal data for the purposes of the GDPR and thus the extent of the individual's rights thereunder [17].

In the interests of brevity, the pertinent question here surrounds the legality of the collection and processing of the data for the purposes of inferring an emotional state of mind. As the application of the GDPR depends primarily on the processing of 'personal data' (Article 2(1) GDPR), if the data do not relate to an identified or identifiable natural person (Article 4 No. 1 GDPR), the Regulation will not apply [18].

In principle, personal data will open the material scope of application of the GDPR. As the degree of protection under the GDPR varies between different personal data and special categories of personal data, the question arises whether emotions fall into this latter class. After all, the EU proposal for an ePrivacy Regulation places emotions on par with medical conditions, sexual preferences, and political views as types of 'highly sensitive information' (Recital 2 COM (2017) 10 final).

Pursuant to Article 9(1) GDPR, it is prohibited to process personal data which reveals sexual preferences or political views. Such information constitutes 'special categories of personal data' for which particular conditions apply, e.g., express consent (Article 9(2) GDPR). Such data are, by their nature, 'particularly sensitive in relation to fundamental rights and freedoms [and] merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms' (Recital 51 GDPR). As noted by Wachter and Mittelstedt, the purpose of protecting against the revelation of one of the protected attributes means that the provision may cover data that directly or indirectly reveal such information [17]. Be that as it may, emotions are not listed as a special categories of personal data under the GDPR. Whether the data are inferred or not is moot, in principle.

From the aforementioned examples, it is clear that determining an individual's emotions requires data, inter alia, on her physiological responses. Biometric data are a special category of personal data under Article 9(1) GDPR and defined in Article 14 No. 4 GDPR. The definition refers to processing relating to the physical, physiological, or behavioural characteristics of a natural person. This may include facial structure, voice, or retinal patterns as well as keystrokes or gait [19]. Nonetheless, the scope of this provision only extends to such data insofar as they are used for the purpose of uniquely identifying a natural person. The use of biometric data for any other purpose, including inferences about an individual's emotional state, would not fall under this exception. There is thus a distinct irony that data protection serves to protect the individual's control over her personal data and thus the 'selective presentation' of the different facets of her personality [17,20], yet the GDPR does not provide additional protections to an aspect of one's personality that one, despite best efforts, may not be able to control.

Subsuming emotions under 'health data' may provide an escape route. Prior to the GDPR, the notion of 'health data' included 'emotional capacity', with the raw sensor data potentially constituting health data when there is an intention to evaluate them as such [19]. However, this may stretch the boundaries of health data thus challenging the extent to which emotions are classified and protected under data protection law [21]. Legal certainty about the status of emotions would best be achieved by amending the list of special category personal data under Article 9(1) GDPR.

In short, the protection of emotions under the GDPR contradicts the understanding as 'highly sensitive information' as the specific protections for 'sensitive data' seemingly do not apply.

3. Proposal for an Artificial Intelligence Act

3.1. Overview

The succinct insight into emotion AI suffices to express the considerable potential surrounding such technology but also certain risks. With the recent proposal for 'Regulation laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act)' the European Commission seeks to promote the uptake of AI and to address the risks associated with certain uses of such AI technology in pursuit of the ultimate aim of 'increasing human well-being' (COM (2021) 206 final, p. 1).

The proposed Regulation aims to provide a comprehensive, future-proof, and harmonised regulatory framework for AI systems that does not 'unduly constrain or hinder technological development' (COM (2021) 206 final, p. 2). It recognises that AI may have risks or negative implications for individuals or society in general, with the type of harm also varying, with its provisions constituting the minimum requirements necessary (COM (2021) 206 final, p. 2). In principle, the proposed Regulation serves as *lex generalis* subject to the *lex specialis* requirements under other EU secondary legislation and national law (cf. Recital 41 PAIA, COM (2021) 206 final, p. 12). The proposed Regulation is as such not directed at a specific sector or class of individual (e.g., a consumer or employee) per se, and thus to be viewed in conjunction with sectoral legislation.

The proposed approach is risk-based, with 'unacceptable risks', 'high risks', and 'low or minimal risks' forming the framework (COM (2021) 206 final, p. 12). Determining the risk category requires a sector-by-sector and case-by-case evaluation in light of the impact on rights and safety. At its core, the proposed Regulation adopts a cautious approach vis-à-vis risks. Particular 'unacceptable risks' are prohibited outright, whereas mandatory requirements and systems for placing on the market or putting into service AI systems in the EU apply in order to mitigate the risks involved (cf., Recital 43 PAIA). Most of the PAIA provisions concern high-risk AI systems, namely those systems that have 'a significant harmful impact on the health, safety and fundamental rights of persons' (Recital 27 PAIA), for which the proposal provides criteria (Article 6 PAIA) and a list of high-risk systems (Annex III). In principle, such high-risk systems must conform to the diverse legislative requirements (Articles 8 et seq. PAIA) in order for a high-risk system to be lawfully placed on the market or put into service. The Regulation does not contain a specific sub-category or rules particular to low-risk AI systems, e.g., AI for predictive text messaging or the AI used in computer games.

For emotions, the proposal includes 'emotion recognition systems' as part of its risk-based framework. This is an important step as the scope of protection afforded to emotions within such proposed system offers insights into the degree to which emotions are considered worthy of protection.

3.2. Emotion Recognition Systems

The Commission's proposal for an Artificial Intelligence Act adopts a 'technology neutral' approach to an artificial intelligence system ('AI System') in order to adapt to the rapid developments in this field (COM (2021) 206 final, p. 12). Article 3 No. 1 PAIA defines an AI system as 'software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with. Pursuant to Article 3 No. 34 PAIA, however, 'Emotion Recognition Systems' constitute a particular type of AI system.

3.2.1. Definition

Article 3 No. 34 PAIA defines an emotion recognition system as 'an AI system for the purpose of identifying or inferring emotions or intentions of natural persons on the basis of their biometric data'. Emotion recognition systems therefore centre on the use of biometric data for this purpose. Such focus on biometric data is problematic as there is not only a lack of reference to other types of data that may be relevant in determining the emotional state but, moreover, the proposed rules will not apply if data are used which do not allow a person to be identified [22]. The intended consistency with the GDPR is therefore maintained (Recital 7 PAIA), as insights into a natural person's emotional state are without adequate legal protection where the individual is not identifiable.

3.2.2. Risk-Based Approach

The risk-based approach adopted by the PAIA centres around the classification of AI systems as an 'unacceptable risk', 'high risk', or 'low or minimal risk' based in particular on the extent of the risks to the health and safety or fundamental rights of persons. In the absence of *lex specialis* provisions, the lawful use of the AI system pursuant to the PAIA will therefore depend on the particular category.

Fundamental Rights

For emotions, the fundamental rights to respect for private and family life, and protection of personal data under Articles 7 and 8 of the EU Charter of Fundamental Rights are especially at stake in allowing AI systems to use data to draw inferences on an individual's state of mind [23]. Whereas privacy centres on upholding the core values of 'individuality, autonomy, integrity and dignity' by protecting the individual against outside intrusions, data protection protects the individual's control over her personal data and thus the 'selective presentation' of the different facets of her personality [17,20].

The example applications of AI listed above not only require data in order to function, but the nature of the function may require a continuous data flow, i.e., constant monitoring of the emotional state. Increasing the accuracy may also require gathering data from multiple sources or pressing the user to reveal more data. The AI system in place may therefore require on further data in order to function effectively. Detecting the emotion will also depend greatly on the context—after all, a smile does not always signify happiness. Further information on the individual's whereabouts and behaviour may therefore be necessary, perhaps requiring data to be communicated from tracking technologies installed on smartphones or other wearable devices [3]. In other words, the individual is subject to varying degrees of surveillance. This may potentially result in the harmful effects of behavioural changes and self-censorship [24].

Despite the harmful effects of infringements on privacy and data protection, such rights are not absolute. Moreover, the European Court of Justice has held that an interference with the right to privacy does not depend on the sensitivity of the information or the inconvenience caused (Joined Cases C-465/00, C-138/01 and C-139/01 *Österreichischer Rundfunk*, para. 75; Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland*, para. 33). Permitted incursions require an express legal basis, in particular the consent of the individual. In this respect, the lack of clarity in relation to the status of emotions under the GDPR and the application of the measures therein drive concerns about the standing of consent and transparency in relation to the collection and processing of the data.

Unacceptable Risk

Emotion recognition can be used to respond to the individual's emotional state of mind by provoking the technology to take a particular course of action. On the other hand, the system has the potential to influence decisions made by or concerning the individual. As mentioned, emotions are a driving force in the decision-making process. As the past discussions surrounding the role of AI have highlighted, the technology can greatly influence decisions made not only by an individual herself, but also in relation to an individual opening the door to discrimination. Such capability is especially concerning whereby the technology exploits or provokes particular emotions and 'nudges' the individual towards or subjects her to detrimental decisions, for example by encouraging 'retail therapy' where inferences point towards sadness [10,25–27].

The PAIA attempts to heed such concerns insofar as prohibiting AI systems that, for example, cause or are likely to cause physical or psychological harm through subliminal techniques beyond a person's consciousness in order to materially distort her behaviour or to exploit particular vulnerabilities (Article 5(1)(a), (b) PAIA). Moreover, Article 5(1)(c) prohibits the evaluation or classification of the trustworthiness of natural persons based, inter alia, on known or predicted personal of personality characteristics, which leads to certain types of detrimental or unfavourable treatment. The prohibitions thus acknowledge the potential to use AI to achieve a power asymmetry in relation to an individual with the effect of manipulating their autonomy, thereby impacting on core values such as human dignity as well as the right to privacy and data protection (cf. Recital 15 PAIA).

However, the proposed provisions have received sharp criticism, with consumer organisations arguing that the protection is limited or even non-existent when applied in practice [22]. In particular, the prohibition under Article 5(1)(c) only applies to public authorities and thus does not protect consumers from the evaluation or classification of trustworthiness by a private enterprise, in particular through the use of emotion recognition systems [22].

From the perspective of emotions, the Article 5(1)(a) and (b) PAIA is to be especially criticised as the wording 'in order to' presupposes an intention to materially distort and does not take into account the potential effect [22]. As McStay notes, the use of emotion AI in children's toys may inadvertently impact on the child's emotional development [10].

Moreover, such prohibitions thus only apply where harm may or does result. Accordingly, the prohibition does not apply if an AI system uses subliminal techniques to materially distort behaviour in order to avert the risk of harm, thereby raising questions around the degree to which it is acceptable to manipulate of an individual's emotional state for such purpose.

Closer reading of the provision also reveals an apparent gap in its scope of protection: economic harm is not covered. For the consumer at least, the EU Unfair Commercial Practices Directive 2005/29/EC ('UCPD') plugs the gap insofar as prohibiting a range of commercial practices which are contrary to the requirements of professional diligence and materially distort or are likely to distort the consumer's economic behaviour (Article 5(2) UCPD). Although 'any algorithmic exploitation of consumer behaviour in violation of existing rules shall be not permitted and violations shall be accordingly punished' (COM (2020) 65 final, p. 14), Article 5 PAIA nonetheless ought to make express reference to economic harm to better complement the UCPD [22,27].

From the perspective of emotions, criticism is due with regard to vulnerability. Article 5(1)(b) makes express reference to age and physical or mental disability as categories implying vulnerability. This list is not only exhaustive but also narrower than the UCPD which includes credulity alongside mental or physical infirmity and age as vulnerabilities (Article 5(3) UCPD). In contrast to the PAIA, Recital 19 UCPD clarifies that the list is not exhaustive. Moreover, a 2016 study by the European Commission adopts a more personalised definition of vulnerability, referring to the individual's 'socio-demographic characteristics, behavioural characteristics, personal situation, or market environment' [28]. In light of the advent of such high degrees of personalisation and the technological capabilities to ascertain and respond to real time, the potential exists to exploit transient vulnerabilities such as the emotional state of mind and therefore it is astonishing that a more individualised understanding of vulnerability is lacking for prohibiting certain practices in general.

High Risk

The majority of the provisions in the PAIA concern the compliance requirements for 'high risk systems' (Articles 6–51 PAIA). In essence, the classification as high risk centres around the intended purpose of the AI system, in line with product safety legislation: high risk depends on the function performed as well as the system's purpose and modes of use (COM (2021) 206 final, p. 13).

High-risk AI systems are divided into two main categories: 'systems that are intended to be used as a safety component that are subject to third party ex ante conformity assessment' and 'other stand-alone AI systems with mainly fundamental rights implications' (COM (2021) 206 final, p. 13). For the former, ERS could be considered high risk if used as a safety component of a product or is itself a product (Article 6(1)(a) PAIA). However, this aspect is not applicable to all products, but only to those listed in Annex II (e.g., toys), and for which a third-party conformity assessment is required. For the latter category, Annex III to the PAIA provides an explicit list of high-risk AI systems with fundamental rights implications. According to this list, an AI system that is used by law enforcement (Annex III 6(b)) or by public authorities in relation to migration, asylum, and border control management (Annex III 7(a)) to detect the emotional state of a person is a high risk AI system. The use is not prohibited in such contexts, but subject to the strict requirements set out in the PAIA.

The list of high-risk AI systems in Annex III therefore makes little express reference to scenarios in which the use of an AI system will be considered high risk where the natural person is a consumer. Annex III 5(b) merely only refers to the use of AI systems for the purposes of evaluating the credit worthiness of natural persons and does not make express reference to emotions. Here, the lack of a reference to insurance—especially where AI systems are used as polygraphs—may astonish, however the use in such scenarios may require sector specific legislation regarding the application. (For example, the use of emotion recognition in the insurance sector to determine whether an individual is lying when making a claim or to calculate premiums is contentious, with calls to ban the use of emotion AI for such purposes, at least insofar as facial detection is used [29]. Moreover, connected devices with AI embedded (e.g., virtual assistants) are not considered high-risk systems under the PAIA [22].

'Limited' Risk

Article 52 PAIA provides for certain transparency obligations for certain AI systems, irrespective of their status as high risk or otherwise. The designation 'transparency' is an exaggeration as ultimately, the obligations merely require the provision of information to a natural person that she is interacting with an AI system. Under Article 51(1), this disclosure obligation does not apply where it is obvious from the circumstances and the context.

For emotion recognition systems, Article 52(2) provides that natural persons exposed to an emotion recognition system are informed of the operation of the system. How the natural persons are to be informed will depend on the circumstances and context, but disclosure is mandatory. Despite the elevation to mandatory status, the disclosure obligation seemingly only applies where the emotion recognition system satisfies the definition in Article 3 No. 34 PAIA. In other words, the disclosure is only mandatory if the system utilises biometric data. As has been stated above, this excludes the application of other types of data that could be used to detect emotions and thereby circumvent the disclosure obligation [22].

In addition, the provision lacks details as to the scope or the type of biometric data that is collected. The individual may be aware that emotion recognition software is in operation, but not of its functionality, e.g., whether gait analysis or gaze detection is in operation. When read in conjunction with the grey areas in the GDPR, the provision casts doubt on whether such obligation is proportionate to the understanding of emotions as 'highly sensitive information'.

4. Transparency via Consumer Law

The above description of the approach proposed for an Artificial Intelligence Act shows that there are fundamental flaws that are to be addressed over the legislative process. It is clear from the outset that the proposed general approach needs to become more general in scope, but equally needs to be supplemented by sector-specific changes. This will take time and in the meantime, the technology will continue to develop and be applied subject to the law as it stands as well as non-binding codes of conduct, etc.

Moreover, the development is taking place at an age in which concerns for data protection and privacy are no longer an afterthought for consumers, but are a contributing factor in contracting, reflected also in recent industry efforts to provide technical and self-regulatory approaches to tackle dubious practices, especially tracking [30]. The role to be played by consumer law in this context is especially critical not only due to the potential to manipulate consumer behaviour on a new level but to allow consumers to assess and keep abreast of the capabilities and implications of new technologies. Emotions are not merely a factor driving decisions by and concerning consumers, but as emotion recognition becomes a feature of consumer goods, increased transparency at the pre-contractual stage is also necessary. Pre-contractual information plays a central role within EU consumer law *acquis*, with diverse areas of consumer law relying on the pre-contractual disclosure of information as an instrument to counter the information asymmetry existing between the consumer and trader.

As the above examples of applications show, the technology may form part of a range of consumer goods either as the primary or secondary feature. Here, the Commission has already emphasised that the requirement of transparency requires consumers to 'receive clear information on the use, features, and properties of AI-enabled products' [16], highlighting the importance to 'adequately communicate the AI system's capabilities and limitations to the different stakeholders involved in a manner appropriate to the use case at hand' [16]. However, according to Art. 13(3)(b) PAIA, such information on the capabilities and limitations, as well as the characteristics and performance, only apply in the context of high-risk AI systems. More fundamentally, this only applies to 'users' as defined in Article 3 No. 4 PAIA, which does not include the consumer [22].

At first glance, the dearth of particular AI information duties vis-á-vis consumers is concerning, not least in light of the emphasis on transparency. However, here the UCPD and the Consumer Rights Directive 2011/83/EU provide a potential framework for addressing general transparency aspects surrounding emotion recognition in consumer goods, irrespective of the level of risk associated with the AI system.

Under the Consumer Rights Directive, the trader is to inform the consumer in a clear and comprehensible manner of the main characteristics of the goods, digital content, and digital service. Understanding the scope of main characteristics requires recourse to Art. 6(1)(b) and Art. 7(4) UCPD, which contain non-exhaustive lists of material information that the average consumer needs to take an informed transactional decision. In light of the information requirements under the PAIA, it is worthwhile considering whether the function and scope of material information under the UCPD—not least the invasive nature of emotion recognition—will require the disclosure of certain information, such as on the accuracy of the system or its limitations.

A further notable information obligation under the Consumer Rights Directive concerns the 'functionality' of the consumer product. According to the Guidance document accompanying the Directive, recital 43 Digital Content Directive 2019/770, and recital 27 Sale of Goods Directive 2019/771, the notion of functionality refers to the ways in which the product can perform their functions having regard to their purpose. This may include information on the conditions for using the product, such as tracking of consumer behaviour and/or personalisation [28]. As a fluid concept, it may also comprise the disclosure of information on the application of emotion recognition, including whether emotion detection is essential for the functionality of the product.

Whereas the collection of the data ultimately depends on the necessary hardware, emotion detection through analysis of the data can be achieved through software development. Per the definition, AI is software (Article 3 No. PAIA). In the digital age, therefore, modifications to the software can improve or enhance the digital element of goods, extend the functionalities, and adapt them to technical developments after purchase (Recital 28 Sale of Goods Directive). Should emotion detection become a new feature (e.g., voice assistants), Art. 19(1)(c) Digital Content Directive provides that the consumer is to receive clear and comprehensible information about the modification.

For goods utilising emotion recognition, 'on the box notification' has been highlighted as an important means to communicate information on the types and methods of data collection, allowing for decisions to be made about the privacy and data protection implications before purchasing the device and either reinforcing the consent to the collection of the necessary data or the awareness that the data are necessary for the performance of the contract [10]. Viewed more generally, the performance of the obligations to provide information on the main characteristics and functionality could nonetheless be sufficiently flexible to cover functions and the methods of data collection needed in relation to emotions, irrespective of the type of data collected. To some degree, this may contribute to offsetting some of the transparency deficits in the PAIA, but it involves the application of an approach that is already flawed. As has been noted, the pre-contractual information duties on 'main characteristics' and 'functionality' are in essence tucked away amongst the vast catalogue of information duties, creating the paradox that efforts towards enhancing transparency ultimately result in opacity [31]. It therefore raises the question whether the nature of emotions as 'highly sensitive information' warrants a 'highly sensitive approach' in ensuring transparency beyond mere general information obligations.

5. Conclusions

This paper illustrated that although existing approaches in consumer law may make a limited contribution, ultimately greater clarity and certainty about the status of emotions in the legal framework are needed to provide a robust system of protection to the consumer where her emotions are at stake. This is because the assessment of the current and proposed legal framework highlights several fundamental inadequacies concerning the appropriate protection and safeguards for emotions, justifying the sharp criticisms drawn by consumer organisations in relation to the proposed Artificial Intelligence Act. At their core, the current and proposed frameworks are not proportionate to the perception that emotions are highly sensitive. Such deficiencies, especially in the PAIA, may stem from the understanding of and focus on biometric data and the relationship to inferring emotions. The need to create a robust legal framework to protect consumers from possible exploitation is clear, yet consumers must have the choice whether they wish to interact 'emotionally' with technology. This requires not only improvements to the proposal itself but clarification in other areas of law as to the scope of pre-existing systems and protections.

Author Contributions: Conceptualization, M.D. and J.W., writing—original draft preparation, M.D. and J.W.; writing—review and editing, M.D. and J.W. All authors have read and agreed to the published version of the manuscript.

Funding: This work is part of / contributes to the larger work undertaken by the author at the National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online (REPHRAIN).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Picard, R. *Affective Computing*; MIT Media Laboratory Perceptual Computing Section Technical Report No. 21; 1995; pp. 1–4. Available online: https://hd.media.mit.edu/tech-reports/TR-321.pdf (accessed on 9 November 2021).
2. Bundestag. Bericht der Enquete-Kommission Künstliche Intelligenz–Gesellschaftliche Verantwortung und Wirtschaftliche, Soziale und Ökologische Potenziale BT-Drs 19/23700; 2020. Available online: https://www.btg-bestellservice.de/pdf/20089800.pdf (accessed on 9 November 2021).
3. McStay, A.; Bakir, V.; Urquhart, L. *Briefing Paper: All Party Parliamentary Group on Artificial Intelligence–Emotion Recognition: Trends, Social Feeling, Policy*; Emotional AI: London, UK, 2020.
4. Barrett, L.F.; Adolphs, R.; Marsella, S.; Martinez, A.M.; Pollak, S.D. Emotional expressions reconsidered: Challenges to inferring emotion from human facial movements. *Psychol. Sci. Public Interest* **2019**, *20*, 1–68. [CrossRef] [PubMed]
5. EPRS. Artificial Intelligence at EU Borders; 2021. Available online: https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_IDA(2021)690706 (accessed on 9 November 2021).
6. Kröger, J.L.; Raschke, P.; Bhuiyan, T.R. Privacy implications of accelerometer data: A review of possible inferences. In Proceedings of the 3rd International Conference on Cryptography, Security and Privacy, Kuala Lumpur, Malaysia, 19–21 January 2019; pp. 81–87.
7. Kröger, J.L.; Lutz OH, M.; Raschke, P. Privacy Implications of Voice and Speech Analysis–Information Disclosure by Inference. In *Privacy and Identity Management*; Friedewald, M., Ed.; Springer: Basel, Switzerland, 2020; pp. 242–258.

8. Kröger, J.L.; Lutz OH, M.; Müller, F. What Does Your Gaze Reveal About You? On the Privacy Implications of Eye Tracking. In *Privacy and Identity Management*; Friedewald, M., Ed.; Springer: Basel, Switzerland, 2020; pp. 226–241.
9. Kröger, J. Unexpected Inferences from Sensor Data: A Hidden Privacy Threat in the Internet of Things. In *Internet of Things. Information Processing in an Increasingly Connected World*; Strous, L.A.M., Cerf, V., Eds.; Springer: Basel, Switzerland, 2018; pp. 147–159.
10. McStay, A.; Rosner, G. Emotional artificial intelligence in children's toys and devices: Ethics, governance and practical remedies. *Big Data Soc.* **2021**, *8*, 2053951721994877. [CrossRef]
11. Xu, S.; Fang, J.; Hu, X.; Ngai, E.; Guo, Y.; Leung, V. Emotion Recognition from Gait Analyses: Current Research and Future Directions. 2020. Available online: https://arxiv.org/abs/2003.11461 (accessed on 9 November 2021).
12. Šucha, V.; Gammel, J.-P. *Humans and Societies in the Age of Artificial Intelligence*; EU Publications: Luxembourg, 2021.
13. Voss, C.; Schwartz, J.; Daniels, J.; Kline, A.; Haber, N.; Tariq, Q.; Robinson, T.; Desai, M.; Phillips, J.; Feinstein, C.; et al. Effect of Wearable Digital Intervention for Improving Socialization in Children with Autism Spectrum Disorder: A Randomized Clinical Trial. *J. Am. Med. Assoc. Pediatrics* **2019**, *173*, 446–454. [CrossRef] [PubMed]
14. Lerner, J.S.; Li, Y.; Valdesolo, P.; Kassam, K.S. Emotion and Decision-Making. *Annu. Rev. Psychol.* **2015**, *66*, 799–823. [CrossRef] [PubMed]
15. Matz, S.C.; Netzer, O. Using Big Data as a window into consumers' psychology. *Curr. Opin. Behav. Sci.* **2017**, *18*, 7–12. [CrossRef]
16. Article 29 WP. *Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679*; European Commission: Brussels, Belgium, 2018.
17. Wachter, S.; Mittelstadt, B. A right to reasonable inferences: Re-thinking data protection law in the age of big data and AI. *Columbia Bus. Law Rev.* **2019**, *2*, 1–130.
18. Galič, M.; Gellert, R. Data protection law beyond identifiability? Atmospheric profiles, nudging and the Stratumseind Living Lab. *Comput. Law Secur. Rev.* **2021**, *40*, 105486. [CrossRef]
19. Article 29 WP. *Opinion 4/2007 on the Concept of Personal Data*; European Commission: Brussels, Belgium, 2007.
20. Lynsky, O. Deconstructing data protection: The "added-value" of a right to data protection in the EU legal order. *Int. Comp. Law Q.* **2014**, *63*, 569–597. [CrossRef]
21. Clifford, D. The Legal Limits to the Monetisation of Online Emotions. Ph.D. Thesis, KU, Leuven, Belgium, 2019.
22. BEUC. *Regulating AI to Protect the Consumer*; BEUC: Brussels, Belgium, 2021.
23. Michalowski, S. Critical Reflections on the Need for a Right to Mental Self-Determination. In *The Cambridge Handbook of New Human Rights*; von Arnauld, A., von der Decken, K., Susi, M., Eds.; Cambridge University Press: Cambridge, UK, 2020; pp. 404–412.
24. Solove, D. A Taxonomy of Privacy. *Univ. Pa. Law Rev.* **2006**, *154*, 477–560. [CrossRef]
25. Article 29 WP. *Annex—Health Data in Apps and Devices, to the Letter to European Commission dated 5 February 2015*; European Commission: Brussels, Belgium, 2015.
26. Holkar, M.; Lees, C. *Convenience at a Cost*; Money and Mental Health Policy Institute: London, UK, 2020.
27. VZBV. *Artificial Intelligence Needs Real World Regulation*; VZBV: Berlin, Germany, 2021.
28. European Commission. *Consumer Vulnerability across Key Markets in the European Union*; EU Publications: Luxembourg, 2016.
29. European Commission. DG Justice Guidance Document concerning Directive 2011/83/EU; 2014. Available online: https://ec.europa.eu/info/sites/default/files/crd_guidance_en_0.pdf (accessed on 9 November 2021).
30. CISCO. *Data Privacy Benchmark Study*; Cisco: San Jose, CA, USA, 2021.
31. Wendehorst, C. Consumer Contracts and the Internet of Things. In *Digital Revolution: Challenges for Contract Law in Practice*; Schulze, R., Staudenmayer, D., Eds.; Nomos: Baden-Baden, Germany, 2016; pp. 189–223.