A Requirement Analysis for Privacy Preserving Biometrics in View of Universal Human Rights and Data Protection Regulation

Nicholas Whiskerd, Jana Dittmann
Multimedia and Security Lab (AMSL)
Otto von Guericke University Magdeburg
Germany
{nicholas.whiskerd|jana.dittmann}@ovgu.de

Claus Vielhauer
Brandenburg University of Applied Sciences &
Otto von Guericke University Magdeburg
Germany
claus.vielhauer@{th-brandenburg.de|ovgu.de}

***Abstract*—Data Protection (DP) and Universal Human Rights are extremely relevant to biometrics, where inherently private data is used for authentication purposes. In this context this paper stresses that there are significant challenges beyond biometric authentication. For example, it has been shown in the existing literature that medical information of a skin disease from a fingerprint, symptoms of diabetes on the retina, or diseases affecting one's walk can be extracted from biometric recordings. We address the derived privacy challenges in biometrics by a careful review of relevant aspects of the universal human rights from UN documents and the EU General Data Protection Regulation (GDPR) with a first identification and enumeration of relevant attributes. From the derived privacy sensitive attributes and respective requirements, de-identification approaches to protection of soft biometrics in face and fingerprints are explored. In consideration of these techniques, there is the question of what constitutes legal and moral biometric signal processing presently in the state-of-the-art, as well as motivation for further work towards fulfilling the criteria.**

Keywords—privacy; soft biometrics; data protection; human rights; GDPR

I. INTRODUCTION

The vast majority of the world has achieved consensus on fundamental universal human rights such as declared by the United Nations. Amongst these rights, privacy rights have been substantiated already in the Universal Declaration of Human Rights [1] (UDHR), primarily by Article 12 with the phrase:

"(…) No one shall be subjected to arbitrary interference with his privacy (...)"

The UN position on rights was clearly defined in 1949 with the UDHR, and serves as the foundation for the conventions built upon it, notably the International Covenant on Civil and Political Rights [2] (CCPR) and International Covenant on Economic, Social and Cultural Rights [3] (CESC).

In July 2014, the UN affirmed that the rights to privacy people are treated to offline should equally apply to the online sphere [4]. In acknowledgement of these universal rights, countries and groups of nations have been implementing legislation on data protection of personal data, e.g. the EU General Data Protection Regulation [5] (GDPR), which defines framework conditions for such data processing, including sensitive biometric signal processing.

Of course, Data Protection (DP) is extremely relevant to biometrics, where inherently private data is used for authentication purposes. However, due to their nature, biometric measurements may disclose further properties of their owners, which can be determined by means of classification, and may well still be very sensitive, private information. Examples for such sensitive information include: medical information of a skin disease from a fingerprint [6], symptoms of diabetes on the retina [7], or a disease affecting one's walk [8]. Emotions are captured too, as one would expect through facial images, yet also wearables and mobile phones [9] are capturing information passively which could suggest stress, excitement or any emotional response that triggers bodily reactions.

This paper will address such non-identification privacy challenges for biometrics by a careful review of relevant aspects of the universal human rights and GDPR, with a first identification and enumeration of relevant attributes. These attributes are discussed with regards to technical approaches that may work towards privacy protection, in particular those within the works from [18] and [20], which have also identified the challenge, for gender, age, race and ethnicity,

The relevant attributes identified in the paper are presented in Table 1, to be used as the basis for discussion of selected exemplary modalities. The specifically highlighted modalities of face and fingerprints are selected for later discussion in protection measures.

ISBN 978-90-827970-1-5

TABLE 1: Derived attributes. Abbreviations U and C refer to UDHR and CCPR respectively. Appended numbers refer to the Articles within the documents. Sources [1][2][3].

Attribute	Origin	Biometric Modalities
Race	U2, C2	Eye, **face**, **fingerprints**
Gender	U2, C2	Body, **face**, **fingerprints**, gait, gestures, hand, handwriting, speech
Language	U2, C2	Handwriting, speech
Freedom of Thought	U2, U18, U19, C2, C18, C19	Eye, **face**, gait, speech, wearable sensors
Nationality	U2, U15, C2, C24	**Face**, **fingerprints**, handwriting, speech
Age	U2, C2	Body, **face**, gait, gestures, handwriting, speech
Childhood	GDPR 8	Body, **face**, gait, gestures, handwriting, speech
Health	GDPR 9	Body, eye, **face**, **fingerprints**, gait, gestures, hand, handwriting, speech, wearable sensors
Sexual Orientation	GDPR 9	Eye, **face**

In view of the identified set of requirements for biometric data, the paper will further focus on the specific modalities of face and fingerprints, and review those technical mechanisms from the state-of-the-art [18], which appear adequate to address the requirements. While the original publication [18] can be seen as a best effort approach to identify today's methods and limitations of face and fingerprint de-identification, the goal of this paper will be to elaborate on a list of explicit proposals, which of the technologies may be utilised for specific DP aspects in future.

The further paper is structured as follows: in the upcoming Section II, further explanations and justifications for the identified attributes as summarised in Table 1 are given. Section III will then consider de-identification approaches as DP methods for the discussed sensitive data, and conclusions of our findings are summarised in the last section.

II. Summary of Potential Relevant Attributes

The goal of this section is to provide a brief insight into articles from UN rights documents and DP regulation that have a direct impact to processing of biometric data from individuals. From these, we derive a set of attributes (i.e. protection aspects) and data processing requirements, which are introduced by real world biometric signal processing examples and linked to the corresponding articles in the declarations. The summary of findings is pre-summarised in Table 1.

There are many works for each of these attributes, however, for conciseness only one reference to an example is given for each.

A. Attributes derived from UN Rights

Under both CCPR and UDHR Article 2, the UN rights enumerate all that which is not grounds for discrimination: "race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status" and "political, jurisdictional or international status". Primarily we derive attributes from this root:

Firstly, the attribute **Race** we summarise from "race" and "colour". More subtle indicators may be visible in fingerprint and iris, however, using the many aspects of the face is the more studied approach [10].

The **Gender** attribute is stated as "sex". Much work has been done in determining gender from across various modalities, such as face [11].

Language as an attribute is naturally disclosed in speech recognition and handwriting. Identification of language in speech is the tougher ongoing challenge [12].

Freedom of Thought is summarised from the rights to "religion, political or other opinion", as well as elaborations in further articles. CCPR/UDHR Article 18 states "freedom of thought, conscience and religion", and CCPR/UDHR Article 19 provides "freedom of opinion and expression", noting the freedom to "hold opinions without interference and to seek, receive and impart information". Capture devices could assess reactions to religious, political or other material, and derive agreement, disagreement, or nuanced reactions. While many modalities provide insight, as the natural human method for communicating emotion, there is much work in determining affect from the face [13].

Nationality as an attribute is derived from both "national or social origin" and "political, jurisdictional or international status". Furthermore CCPR Article 24 and UDHR Article 15 state "No one shall be arbitrarily deprived of his nationality nor denied the right to change his nationality". Nationality is a free aspect of identity distinctly apart from the physical attributes, however, nationality can be estimated either from **Language** or from **Race**.

Age is an attribute derived from impartiality of conditions of "birth", regardless of era. Assigning age demographics from face images has proven effective [14].

These attributes are beholden to certain restrictions and requirements of broader rights, we can derive the requirements for their use.

Fundamentally the substantiation of privacy is made clear in CCPR Article 17 (similarly to UDHR Article 12) which states "No one shall be subjected to arbitrary or unlawful interference with his privacy (...)". Privacy is a right like any other which deserves protection in the eyes of the law. In interpreting the article, there is an issue with deciding what is arbitrary. Consider when data is held long-term for potential developments, or used in machine learning without understanding of the underlying logic generated.

In employment, CESC/UDHR Article 23 highlights the importance of no discrimination: "Everyone, without any discrimination, has the right to equal pay for equal work." With technology such as machine learning models and sorting based on a huge amount of features, there exists the risk of concealed immoral discriminating factors [15].

ISBN 978-90-827970-1-5 © EURASIP 2018

B. *Attributes and Requirements derived from GDPR*

Within the GDPR, further attributes which directly relate to biometric data processing, are derived.

The attribute of **Childhood** is substantiated by Article 8: "Additional protection for children under 16: Processing of personal information from children under 16 is only allowed with consent given or authorised by the holder of parental responsibility over the child (...)". Consequently, in biometric systems, groups of minors need to be robustly identified for control over their processing. However, conventional methods of agreement have trouble verifying a user's age, especially where biometrics in public environments are passively captured. It is a challenge to identify children to selectively exclude them from processing, while restricted from processing their data [16].

Health as an attribute is derived from Article 9 which states "data concerning health (...) shall be prohibited." This is overridden in the case of explicit consent, however clearly remains a requirement for passive capture. Health information can be captured widely across many modalities, from distant cameras to close wearables. Diabetes is visible in vein patterns of hand and retina, skin conditions and pigmentation in fingerprint and face, and diseases in movement of gait and gestures [6].

Additionally from Article 9, **Sexual Orientation** is derived from "data concerning a natural person's sex life or sexual orientation shall be prohibited". Sexual Orientation can be divulged in reactions of pupil dilation in the eye, and exploratory works exist in identifying orientation from face images [17]. Whether the systems are truly feasible or not, the lawfulness of such implementations would be questionable, regardless of effectiveness.

In addition, and essentially as one of the key purposes of DP regulation, is the provided regulation on basic operating principles in the processing of private information. Since these are obviously relevant for biometric data processing, they are summarised in requirements in Table 2 with reference to each corresponding article.

TABLE 2: Summary of processing requirements by GDPR, in particular regard to biometrics. Source [5].

Article	Summary
Chapter II – Principles	
5	Principles relating to processing of personal data • Processed within the bounds of the law • Fairness and transparency • Purpose limitation • Data minimisation • Accuracy • Storage limitations • Integrity and confidentiality • Data controller accountability
9	Processing of biometric data for unique identification of a person is generally prohibited. Processing of biometric data without unambiguous, rigorous consent is forbidden. Exceptions are in cases of extreme public interest in legal or medical scenarios, or the information is public by nature.
Chapter III – Rights of the data subject	
12/13	The following knowledge must be provided where personal data are collected for a new purpose: • The responsible parties who are using the data • The identity of the data controller • How long the data will be stored • The right to request access, rectification and erasure
15	Personal data accessibility
16	Rectification
17	Erasure (right to be forgotten)
20	Data portability
22	Not to be subject to a decision based solely on automated processing (which may include profiling)
Chapter IV – Controller and processor	
24	The data controller is responsible for technical and organisational accordance with the law
25	Data protection by design
32	Security of processing
33/34	Notification of breaches to both supervisory authority and subjects
35	Data protection impact assessment

From the derived attributes and requirements, we have identified many areas of biometric data under threat. Evaluated technical countermeasures for some selected scenarios are thus explored in the following section.

III. De-identification Methods

De-identification is a method of personal DP through hiding a captured subject's identity. Ideally it obscures a subject's identity without compromising the action or disturbing the remaining context of the source material. However, such perfect and simultaneously feasible solutions are not yet in existence and a subject of current research.

Upon successful de-identification, even if methods are implemented such that not all the privacy sensitive attributes are hidden in the final data, the hiding of identity naturally absolutely protects privacy. Any remaining attributes left attached would not be attachable to any individual. Further to this, de-identification serves as protection of the sensitive information which may be contained in data which is not yet discernible and/or extractable with present technology.

As described in [18], de-identification can be both reversible and irreversible. Irreversible methods are more robust protection in effective hiding of data, however, they are naturally destructive in the process, massively hindering data utility. Reversible methods are ideal for DP by default, with reversibility upon authority request. These methods are not destructive of the source data but involve additional information for future extraction of the original de-identified material, such as by method of a held private key.

There is damage to data naturalness and intelligibility in many if not all cases by the very manner of information removal or replacement of that which is natural. Naive approaches are either highly damaging to data naturalness (e.g.

ISBN 978-90-827970-1-5 © EURASIP 2018

by black boxes over faces), or, in the case of simple methods like basic blurring, may be vulnerable to parrot attacks.

As an example in captured video, full de-identification of the human silhouette can hide the body, face and gait. And thus by extension, any of the sensitive attributes potentially revealed by those modalities. One such method is **body silhouette transform domain scrambling** [19]. It can be applied for full de-identification of a whole moving body, and is reversible with the secret encryption key upon necessity. It is fitting for live video situations, as the method is demonstrated to be efficient and easy to implement. The naturalness of video is lost, but localised to the subjects' bodies and not affecting of the full picture.

Since as stated already, full de-identification naturally removes identity, we consider the sub-category of methods re-purposing de-identification methods for hiding captured soft biometrics: human characteristics which may be shared among multiple subjects or are only temporary. This is an opposite approach to de-identification in the sense that the goal is not to remove identity. Instead identity can be preserved, however, soft biometrics alone are to be effectively removed. There is at present little work in the area, as noted in [18]. There are gaps in the available technology to achieve this goal. Therefore, if the soft biometrics cannot be hidden in a selective manner, on the basis of the derived requirements, barring explicit consent there is justification for total de-identification even with the sacrifice of data loss.

TABLE 3: Identified solutions in the literature of derived attribute protections by selective de-identification.

Biometric Modality	Attribute	Solutions (None/Partial/Complete)
Face	Race / Nationality	Partial
	Gender	Complete
	Freedom of Thought	None
	Age / Childhood	None
	Health	Partial
	Sexual Orientation	None
Fingerprint	Race / Nationality	None
	Gender	Complete
	Health	None

Within the ridge patterns of fingerprints, there are indicators of both **Gender** and **Race**. Additionally the presentation of the skin of the thumb will divulge **Health** attributes such as skin conditions and diseases, to the extent that recognition can often fail.

Gender hiding in fingerprints can be accomplished by shifting the frequency distributions as shown in [20]. This achieves successful obscuration of the attribute of gender in stored templates, while still preserving a system within which identification attempts succeed.

The subject of face de-identification methods involves both the easier problem of static images, and the greater challenge of video especially given real-time demands. However, this is clearly an area of interest considering existing established widespread video surveillance. Much is disclosed in the face of an individual, including **Age**, **Gender**, **Race** and **Health** and potentially **Freedom of Thought**. **Race** is one example with a well-known effect on facial recognition and their common biases. Such an attribute is commonly disclosed.

Race, and thus to an extent **Nationality**, hiding in video is mentioned in [21] as an achievable challenge by masking the skin colour as a relevant race indicator. However this is achieved by merely involving the step of RGB and hue-space transformations and compromises data naturalness. This is only a basic approach which may fool systems not trained for it, but even to a human eye (in the case of adequate resolution) this is not sufficient as other distinct racial features are not obscured.

Transformations on skin colour may intend to hide **Race**, however such methods are additionally a step towards preventing exposure of **Health**. In [22], skin carotenoid colouration is shown to be both affected by diet, and an indicator visible to other humans of apparent health.

Furthermore in obscuring soft biometrics, some work exists not applicable to the attributes derived in Section II. Notably this includes coverage of hairstyles and clothing. However, the clothing colour methods in [24] could be applied to skin colour, again achieving a similar step towards DP of **Race**, **Nationality** and **Health**.

In the example for **Gender** [20], data naturalness is not significantly compromised and identification is still demonstrated as successful. With only two classes, it is more straightforward to shift the distribution. This is not applicable for other attributes such as **Health** and **Race** which have many more variables, and levels of each. Hiding of soft biometric features wherein classes cannot all be blended together can be overall ruinous to data naturalness. Where such damage is considered unwanted, less jarring results are desirable.

If all subtleties can be identified eventually, therefore they can equally be selectively de-identified. However, it may not be feasible in real-time systems to process each individual subject with such scrutiny. A common blanket approach for all captured subjects may thus be a more reasonable solution.

The advantage of selectively hiding sensitive secondary information for protection of privacy without sacrificing data utility is clear: free, privacy-preserving biometric identification. However, there remain many challenges in finding and hiding that which is sensitive. Presently full de-identification approaches remain the only established effective methods for completely satisfactory DP. However, we acknowledge that de-identification remains a domain of active research, where numerous approaches beyond the above mentioned are to be expected. This may include additional modalities, not yet considered such as handwriting, or alternative approaches, e.g. those based on the variety of cryptographic building blocks.

ISBN 978-90-827970-1-5 © EURASIP 2018

IV. Conclusion

In this paper, we derived privacy-sensitive attributes in biometric data from UN rights and GDPR, and present threats to the privacy of people's captured biometric data. From studying current capabilities in identifying additional features beyond the purposes of identification or verification, there is potential for vast personal information disclosure.

From review of existing methods in de-identification, we conclude that selective DP methods for all the attributes and modalities are incomplete. This is justification for full de-identification of captured data where privacy is necessary, while further development of selective approaches continues.

A proposed solution to investigate is addition of overlaid features rather than transformation or subtraction of the existing features. Further activities in soft biometrics protection could investigate group de-anonymisation [25], whereby the novelty lies in the data sets being intentionally equipped with such features, that will classify them into one single, common category. This enables exposure of individual soft biometrics from a single subject, yet makes each individual indistinguishable within this particular group. To any observer, all data subjects would exhibit all health conditions, ethnicities, emotions etc. and discriminatory judgements based on displays of attributes would therefore be impossible.

Acknowledgements

The work presented has been supported in part by the European Commission through the MSCA-ITN-ETN - European Training Networks under Project ID: 675087 ("AMBER - enhAnced Mobile BiomEtRics"). This project has received funding from the European Union's Horizon 2020 research and innovation programme. The information in this document is provided as is, and no guarantee or warranty that the information is fit for any particular purpose is given or implied. The user thereof uses the information at one's own sole risk and liability.

References

[1] United Nations General Assembly, "The Universal Declaration of Human Rights (General Assembly resolution 217 A)", Paris, 1948

[2] UN General Assembly, International Covenant on Civil and Political Rights, 16 December 1966, United Nations, Treaty Series, vol. 999, p. 171

[3] UN General Assembly, International Covenant on Economic, Social and Cultural Rights, 16 December 1966, United Nations, Treaty Series, vol. 993, p. 3

[4] United Nations General Assembly, The Right to Privacy in the Digital Age, http://www.ohchr.org/Documents/Issues/DigitalAge/A-HRC-27-37_en.doc, 30 June 2014

[5] The European Parliament and The Council, General Data Protection Regulation, http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf, 27 April 2016

[6] Martin Drahansky, Michal Dolezel, Jaroslav Urbanek, Eva Brezinova, and Tai-hoon Kim, "Influence of Skin Diseases on Fingerprint Recognition," Journal of Biomedicine and Biotechnology, vol. 2012, Article ID 626148, 14 pages, 2012

[7] Prabhu, Srikanth and Chakraborty, Chandan and Banerjee, R N and Ray, A K (2012) Study of Retinal Biometrics with Respect to Peripheral Degeneration with Clinically Significant Features. Special Issue of International Journal of Computer Applications. pp. 29-34. ISSN 0975 – 8887

[8] Li, Q., Wang, Y., Sharf, A. et al. Vis Comput (2016), Classification of gait anomalies from kinect

[9] Eugenia Politou, Efthimios Alepis, Constantinos Patsakis, A survey on mobile affective computing, In Computer Science Review, Volume 25, 2017, Pages 79-100, ISSN 1574-0137

[10] Lu, Xiaoguang & K. Jain, Anil. (2004). Ethnicity Identification from Face Images. Proc SPIE. 5404

[11] Azzopardi G., Greco A., Vento M. (2016) Gender Recognition from Face Images Using a Fusion of SVM Classifiers. In: Campilho A., Karray F. (eds) Image Analysis and Recognition. ICIAR 2016. Lecture Notes in Computer Science, vol 9730. Springer, Cham

[12] A. Ghoshal, P. Swietojanski and S. Renals, "Multilingual training of deep neural networks," 2013 IEEE International Conference on Acoustics, Speech and Signal Processing, Vancouver, BC, 2013, pp. 7319-7323

[13] H. Meng and N. Bianchi-Berthouze, "Affective State Level Recognition in Naturalistic Facial and Vocal Expressions," in IEEE Transactions on Cybernetics, vol. 44, no. 3, pp. 315-328, March 2014

[14] H. Han, C. Otto, X. Liu and A. K. Jain, "Demographic Estimation from Face Images: Human vs. Machine Performance", IEEE Trans. PAMI, Vol. 37, No. 6, pp. 1148-1161, June 2015

[15] Moritz Hardt, How big data is unfair, https://medium.com/@mrtz/how-big-data-is-unfair-9aa544d739de, website request 26.1.2018

[16] Jain, A. K., Cao, K., & Arora, S. S. (2014). Recognizing infants and toddlers using fingerprints: Increasing the vaccination coverage, IJCB 2014 - 2014 IEEE/IAPR International Joint Conference on Biometrics [6996252] Institute of Electrical and Electronics Engineers Inc.

[17] Wang, Y., & Kosinski, M. (2018). Deep neural networks are more accurate than humans at detecting sexual orientation from facial images. Journal of Personality and Social Psychology, 114(2), 246-257

[18] Ribaric, Slobodan; Ariyaeeinia, Aladdin; Pavesic, Nikola, "De-identification for privacy protection in multimedia content: A survey", Signal Processing: Image Communication. 47: 131–151

[19] F. Dufaux, T. Ebrahimi, Scrambling for privacy protection in video surveillance systems, IEEE Trans. Circuits Syst. Video Technol. 18 (8) (2008) 1168–1174

[20] L. Lugini, E. Marasco, B. Cukic, J. Dawson, Removing gender signature from fingerprints, Proc. Spec. Sess. Biom., Forensics, De.-identifications Priv. Prot. (BiForD) (2014) 63–67

[21] P. Agrawal, P.J. Narayanan, Person de-identification in videos, IEEE Trans. Circuits Syst. Video Technol. 21 (3) (2011) 299–310

[22] Ian D. Stephen, Vinet Coetzee, David I. Perrett, Carotenoid and melanin pigment coloration affect perceived human health, Evolution and Human Behavior, Volume 32, Issue 3, 2011, Pages 216-227, ISSN 1090-5138

[23] Li, Chao & Li, Daniel & Miklau, Gerome & Suciu, Dan. (2012), A Theory of Pricing Private Data. ACM Transactions on Database Systems

[24] Karla Brkic, Tomislav Hrkac, Zoran Kalafatic, Ivan Sikiric, "Face, Hairstyle and Clothing De-Identification in Video Sequences", 2017

[25] Chertov, Oleg & Tavrov, Dan, "Group Anonymity", In: "Information Processing and Management of Uncertainty in Knowledge-Based Systems. Applications", Volume 81, Part 6, Part 9, 592-601), Springer, 2010