enhAnced Mobile BiomEtRics

DELIVERABLE: D6.5

Towards a Protection Profile for User-Centric and Self-Determined Privacy Management in Biometrics

Contract number:	675087
Project acronym:	AMBER
Project title:	Enhanced Mobile Biometrics
Project duration:	1 January 2017 – 31 December 2020
Coordinator:	Richard Guest, University of Kent, Canterbury, UK

Deliverable Number:	D6.5
Type:	Academic Paper
Dissemination level	PU
Expected submission date	January 2018
Date submitted:	January 2018

Authors / contributors	Salatiel Ezennaya-Gomez, Claus Vielhauery and Jana Dittmann
Contributing partners	OVGU

RESEARCH & INNOVATION
Marie Skłodowska-Curie actions

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 675087

Towards a Protection Profile for User-Centric and Self-Determined Privacy Management in Biometrics

Salatiel Ezennaya-Gomez*, Claus Vielhauer*† and Jana Dittmann*
*Multimedia and Security Lab (AMSL)
Otto-von-Guericke-University Magdeburg
Email: {*salatiel.ezennaya / jana.dittmann*} *ovgu.de*
†Brandenburg University of Applied Sciences
Email: *claus.vielhauer*@{*ovgu.de / th-brandenburg.de*}

***Abstract*—While new concepts of data analysis bring new opportunities for technological and societal evolution, they also present challenges with respect to privacy. Misconduct on personal data usage, particularly of biometric data, may lead to expose it to identity thieves or unfair practices. It is necessary to define limits to the usage of personal data, involving the user actively in the process of defining and controlling their own data as it is gathered in the EU data regulation (GDPR). It includes the right for the user to be informed about the actual use of the data, as it is called notice and choice. In recent decades, security and privacy design aspects were analysed and incorporated as building blocks for IT systems, and now some aspects are mandatory in standardisation and certification procedures. As a first step towards a Protection Profile in biometrics meeting GDPR requirements, in this paper we propose new privacy enforcement concepts and essential privacy requirements to achieve the goal of designing user-centric and self-determined privacy management in mobile biometrics.**

Keywords–GDPR; privacy; biometric data; sensible data; informed consent; transparency.

I. INTRODUCTION

After data breach public scandals, such as Cambridge Analytica and Facebook, or the mainstream adoption of Home Voice Assistants [1], [2], [3], there is increasing social alarm concerning uncontrolled acquisition of personal data. Concerns about privacy rose some time ago, since social and individual liberties are attached to sensitive data, such as biometric data, as Lane, Stodden, Bender and Nissenbaum (2014) clearly expose about informational data and privacy [4].

The European General Data Protection Regulation (GDPR) [5] undermines practices carried out by organisations regarding the use of personal data and sets rules on informational privacy. This regulation defines the rights of the owner of the data, as well as the obligations for organisations responsible for the acquisition, processing and maintenance of the data. Regarding the treatment of sensitive data, the regulation is very strict and precise with the rights that the user has over them. For instance, processing personal data in categories, such as political opinions, religious beliefs, and ethnicity is prohibited. Moreover, GDPR includes the right to control the data, so individuals have the right to object to the processing of their data, unless the organisations demonstrate the contrary for legitimate reasons [6] and [7]. This implies that individuals must be informed about the use of their data and the organisations must provide the means for the identification of the data once they are in storage. This regulation presents concepts on data protection, e.g., purpose binding, data minimisation, transparency, information security and individual's rights by means of consent [7] and [5].

Some aforementioned principles are gathered in the Fair Information Practice Principles (FIPPs) introduced in the 70s by the U.S. government, as well as in several previous data protection laws of European countries. However, the terms are inefficient in providing users power over their personal data.

In the case of GDPR, one can claim that the term Consent will be a building block in the development of IT systems for years to come. The regulation obligates mandatory demonstrable consent for certain purposes, and it can be withdrawn at any time [5]. In short, the user has the right to access, delete, customise and choose which personal data are shared without the current tedious bureaucratic process, or simply having no option to carry out these actions after having given consent. Moreover, the regulation sets the user's right to obtain a copy of the data (Data Portability), to be informed, and to object if he/she does not agree with the use of his/her data. In summary, GDPR is crucial for personal data processing, thus having an economic impact on companies' procedures. It should be mentioned that there are guidelines and methodologies of data protection models embracing GDPR from a legal point of view, such as the Standard Data Protection Model published by the German data protection authorities (DPAs) [8].

With respect to the research agenda, on biometric data protection and for data holders, it can be summarised in the following domains: biometric devices, extraction and representation of biometric data, privacy, design of trusted systems [9]. However, for the sake of our scope, we focus our attention on the last two domains. The former refers to limiting risks of privacy and civil liberties, whilst offering policies to enable robust biometric systems. The latter refers to design of transparent and fair systems for user acceptance accomplishing social norms. Thereby, new technical mechanisms to limit personal data usage, and likewise, guidelines in technical implementation of informed consent are urgently to be developed to translate data accountability into an increasing volume of businesses.

Biometric data pose key privacy questions as are summarised by Bustard (2015) [6], e.g., what biometric data are being gathered and by whom? Are data being used solely for the purpose for which it was gathered? Misuse of biometric data is extremely dangerous to user privacy. Biometric systems can reveal health conditions of users, and uniquely identify users by means of de-anonymising or linking information, among other examples of hazards.

 ISBN: 978-1-61208-661-3

For this reason, research communities across different disciplines have discussed the privacy issue for several years. Proposals of Artificial Intelligence (AI) governance models for AI frameworks or standardisation of ethics in AI are under development [10] and [11]. Additionally, solutions to improve IT systems, privacy-enhancing technologies, and mechanisms to embed GDPR requirements, are all being studied in several European research projects. Technologies on Identity Management or Access Control are covered in European projects, e.g., PaaSword [12] or CREDENTIAL [13]. In the specific case of Biometrics, there is ReCRED which seeks to improve access control solutions relying on the uniqueness of biometrics [14] and AMBER (enhAnced Mobile BiomEtRics) [15], which addresses current issues facing biometric solutions on mobile devices. This includes new methods for user data privacy protection, to provide data anonymity and usage transparency with user-centric data management, and to implement informed consent by organisational and technical means.

In a large part of published documents in standardisation, security requirements are limited to evaluate risks in aspects, such as Confidentiality, Integrity, Authenticity, Availability and the latest added design aspect: Privacy-by-Design. For the aforementioned reasons on the relationship between privacy and biometric data, privacy-preserving design aspects besides those well-known (Anonymity, Unlinkability, Unobservability), namely Transparency and Intervenability [8], should be taken into account in system design that intends to process biometric data.

In this document, we briefly review some Protection Profiles (PP) existing in biometrics, and what privacy requirements should be considered, in addition to security aspects, which already meet some standards. Finally, we focus on the definition of protection profiles that are the guidelines for certification of security systems. A set of preliminary concepts of transparency requirements are proposed, which may be included in a forward protection profile on transparency for biometric systems environments. These must be centred on user privacy management to achieve the goal of implementation of Informed Consent. We analyse potential threats for privacy, and we propose informal functional requirements for a transparent biometric system. Note that the present work does not intend to define a protection profile to cover all types of systems, but to be a step to study the inclusion of terms and requirements defined in GDPR.

The paper is divided as follows: In Section II, background in protection profiles and standards related to biometric are briefly described, as well as work done in research and other disciplines as recommendations for evaluation of biometric systems. In Section III, we propose the essential privacy requirements that a biometric system should present for its performance according to GDPR requirements. In Sections IV and V, discussion and conclusions are presented along with future work.

II. Background in Protection Profiles and Standards

In order to have a secure privacy-preserving biometric system, it must comply with six basic security design aspects or protection goals, as they are required by any computer system: Confidentiality, Integrity of the data, Authenticity, Non-repudiation, Availability, and Privacy-by-Design. Regarding privacy, there are precise privacy aspects for privacy-preserving technology that are: Anonymity, Pseudonyms, Unlinkability and Unobservability [16].

With the upcoming future changes, new protection goals are essential to be included during the IT system design stage to achieve transparent secure privacy-preserving systems, they are *Transparency* and *Intervenability*. Transparency brings the right of notification, and information of data subjects or users. Intervenability is a term adopted in [8], which refers to the right of deletion, correction, and objection by data subjects, as they are gathered in GDPR, that is, to implement self-determination into systems. To achieve these two essential aspects, a possible and logical solution would be to seek *Informed Consent* of the user by technical means.

Once the protection goals are defined, there is a question to be asked: Are these protection goals collected in published technical standards or in any protection profile in biometrics?

The Common Criteria (CC) is an international standard (ISO/IEC 15408) that sets security requirements for the evaluation of IT products or systems [17]. Under the CC, PP documents are published for the certification of an IT security product. These define an implementation-independent set of security requirements, across different categories such as: access control devices, databases, and data protection (e.g., cryptographic modules) among others. According to the current requirements of the latest version of CC (version 3.1), biometric systems may perform either enrolment or verification under the authentication framework. So far, there are published PPs for biometrics on verification mechanisms and fingerprint spoof detection. However, PPs span different categories which enforce security aspects, such as confidentiality, integrity of data in IT products, thus suitable for biometric systems. Some of those PPs are for Access Control devices, Encryption Systems for data protection, Smart Cards (ePassport) or Trusted Computing. Current PPs, relevant for this paper, under the CC version 3.1 are:

- BSI-CC-PP-0043-2008 Biometric Verification Mechanisms Protection Profile: Describes the functionality of a biometric verification system, defining its functional and assurance requirements [18].
- BSI-CC-PP-0062-2009 Fingerprint Spoof Detection Protection Profile: The scope of this Protection Profile is to describe the functionality of a biometric spoof detection system in terms of CC [19].

Currently, a CC working group is developing the Essential Security Requirements (ESR) for biometric products in an upcoming PP, within which the security requirements do not depend on biometric characteristics [20].

Other technical standards on IT security techniques have been published by ISO or ANSI (American National Standards Institute). Concretely, the Joint Technical Committee SC37 of ISO is responsible for development of technical standards in biometrics. This is divided into working groups, each which works on a different topic, such as: harmonised vocabulary, biometric technical interfaces, data interchanges formats, and technical implementations among others.

An example of standards in biometrics that might be interesting to systems that process biometric data, is the ISO/IEC 24745. It provides guidance for protection of biometric information during transfer and storage, providing confidentiality,

 ISBN: 978-1-61208-661-3

integrity and revocability as well as providing guidelines on the protection of user privacy while processing biometric data. Also, standards that cover data formats for interoperability which depend on the biometric modality, or for biometric presentation attack detection are defined in ISO/IEC 19794-1:2011 and ISO/IEC 30107-2, respectively [21].

We highlight the standard ISO/IEC 30136:2018 published recently which provides evaluation of accuracy, as well as the privacy of biometric templates, establishing definitions to evaluate the biometric template scheme performance [22].

In the literature, technical mechanisms and protocols to achieve user-centric management have been proposed in several works [23], [24], [25] for different frameworks (e.g., identity management in the cloud). The work is based on information exchange security isolating personal information. In the context of IoT and Smart cities, Martinez, Hernandez, Beltran, Skarmeta and Ruiz (2017) presented an IoT attribute-based access control platform which empowers the user to decide which energy data is shared with other entities defining XACML-based privacy policies [26]. In the context of biometrics, the efforts are focused on different areas of authentication, such as proposing more robust storage mechanisms, improving biometric authentication using cryptographic schemes, or biometric template protection systems. In the latter area, Gomez-Barrero, Rathgeb, Galbally, Busch, and Fierrez (2017) work on providing unlinkability and irreversibility in biometric templates [27]. Besides, the so-called biometric-system-on-cards (BSoC) or smartcards (considered in ISO/IEC 17839) are proposed for user-centric privacy in biometrics, [28]. In this case, the user has physically his/her biometric templates stored in a smartcard. The capture device, signal processing, feature extraction and comparison are embedded in a smartcard. In addition, in regulation and standardisation, proposals on PP for biometric systems under specific standards of the ISO, and protection profiles and evaluations of biometric system performance under the CC have been published [29].

Current standards and protection profiles in data protection neither include data subject preferences in relation to data sharing, nor consent to process his biometric data, both threats related to transparency or unfair use of personal data. Therefore, besides security design aspects, privacy-by-design requirements must be gathered in future PPs in biometrics.

III. Essential Privacy Requirements for Biometric Products

Data breaches or misuse of personal data, in the specific case of biometric data, can lead to the invasion of privacy of the individual, identity impersonation, or other hazards. These risk the disastrous consequence of the loss of user's trust to biometrics and its advantages. Therefore, a first step in the definition of the security problem is the risk analysis, wherein risks, to which a biometric system is exposed, are evaluated.

The following threats are applicable in many architectures, though we focus our attention on systems based on Cloud-as-a-Service (CaaS). These systems use biometric data to offer a service, such as voice-assistants including Alexa of Amazon [30], since voice templates are not solely used for authentication.

TABLE I. Threats: Unfair Use of Personal Data

Threat	*Description*
Profiling or discovering patterns	The application of machine learning techniques for profiling or predictive consumer scores, which also can lead to a re-identification of the subject. Data holders can learn from biometric data. Processing personal data, such as political opinions, religious beliefs, sexual orientation etc. to profile individuals into categories is now prohibited according to GDPR.
No-policy-transparency	No clear comprehensible communication regarding data management.
Violation of the principle of proportionality	Biometric data are not only used for what has been originally intended, but for other purposes [33].
Monetisation of information	Pricing data exchanges between agents which manages a user's personal data [34]
Processing children's biometric data	To process children's data, such as voice or faces, without parental authorisation or consent.
Second-hand data leakage	Private data are revealed (unintentionally) by a person who has any kind of relation with another person. Also named by Barocas, Solon and Nissembaum (2014) [35], the tyranny of minority
Cross-border data transfer	The effect of the transfer data to third countries which do not respect individuals privacy [8].

A. Risk Analysis for Privacy

Attacks or threats, regardless of biometric modality, can be identified based on where, what and how they are produced. In the literature, there are some taxonomies wherein threats of IT systems are identified, such as the CERT taxonomy or ENISA Taxonomy [31] and [32]. Protection profiles, as well as standards, collect complete lists of threats, such as eavesdropping/hijacking (communication channels), failures (physical or logical), outages, nefarious activity (malware, etc.), which affect different parts and elements of the architecture of a general IT system [32]. Specific threats related to biometric systems are high level threats as discussed in [33], and can be summarised as follow:

- Spoofing, coercion, mimicry or denial of service attacks can compromise the capture device.
- Pre-processing and feature extraction modules could be compromised by impostor data, or malware (in both enrolment and verification stages). This could happen in the matching and decision modules with attacks, such as reply, component replacement, or hill climbing.
- A reference database, i.e., where data are processed and stored, could be attacked by reading or modifying templates, or changing links between biometric templates and a user's ID.

Besides the aforementioned hazards, there are threats to privacy regarding the misuse of the biometric data. We evaluate the following threats in Table I as risks of *unfair* use of data, therefore, risks for privacy.

B. Informal Privacy Requirements for a Fair and Transparent System

Following with the exercise of the definition of the security problem, in this subsection, the informal privacy objectives

are described. The goal of a user-centric and self-determined system is to provide a tool to inform, manage and make decisions concerning outsourced biometric data. In order to achieve the protection goals listed in [8], a transparent system must be designed to perform the specific functionalities for transparency and intervenability (in Table II), besides those that provide anonymity, unlinkability, pseudonym and unobservability. This is summarised as follows:

- Reduce collected attributes of the data subject (data minimisation principle): Attributes in the context of biometrics certainly include all kinds of features extracted for a specific classification task, such as language, race, gender and age determination, childhood, and health conditions, [36].
- Protect sensitive information-flow by means of security mechanisms already developed (e.g., access control, language-based techniques, among others), relying on existing PPs, and provide security and privacy to biometric data in order to address threats. Including the aforementioned threats to privacy (e.g., BSI-CC-PP-0043-2008 and Standard ISO24174).
- Provide biometric data stored in the system which is complete, legible, auditable, and understandable to the user. Moreover, the biometric data should be portable, which means, in case the user will copy the biometric data for any reason, it should be in a standardised data format (e.g., ISO/IEC 19785-1).
- Audit changes on biometric data and provide logs of any action performed on the data.

An practical example of a system that processes biometric data (user's utterances) with no biometric authentication purpose, is an intelligent voice assistant, (e.g., Amazon Alexa). Biometric data are processed in the cloud to perform the service. Note that these type of systems can be considered HbC (Honest-but-Curious), that is, it provides a service while it tries to retrieve information from the user's data.

A first step, before data disclosure, is the informed consent negotiation. The user must be notified about the points listed in Table II. According to his/her privacy preferences, the user must have control over those points. These preferences must be written in a profile (or a privacy certificate written in XML-based language, for instance) and shared with the system in the cloud. Note that the privacy profile should be updated periodically with user's preferences. The cloud must check the procedures that it will apply to the data, such as algorithms, outsourcing, purpose, retention time, etc. Later, it should inform the client which options it is able to fulfil. The client receives the server's options and checks the conditions. Sequentially, once the handshake is performed, the client is ready to share the biometric data, previously processed (i.e., applying anonymisation or marking algorithms, such as speech watermarking). Once these steps are performed, the data are sent to the cloud and stored following security requirements for sensitive data. In case that the negotiations ended in a deadlock, the user should able to decide to share the data with the best conditions that the server offers to preserve privacy, otherwise decline the use of his/her biometric data. In case of consent revocation, the system should look into the database, identify the user's data, and erase them.

TABLE II. SYSTEM DESIGN FUNCTIONALITIES

Privacy Design Aspects	*System Functionalities*
Transparency	Inform the user about: – Purpose of data collection. – Retention period of the data in data holder's servers. – Associated privacy risks. – Data collection periodicity. – Location of storage servers of data holder. – If decision making is done or not.
Intervenability	System must give options to: – Accept or decline the purpose of data collection. – Accept or decline data sharing with third-parties. – Revoke complete consent for processing. – Revoke partial consent, such as data sharing. – Erase data stored in data holder's servers. – Allow or deny decision making over user's data.

IV. DISCUSSION

GDPR pays attention to biometrics in Art. 9 Paragraph 1 which says: *"(...) the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited."* Following a list of exceptions is specified, where the first exception is described in Paragraph 2.a: *"the data subject has given explicit consent to the processing of those personal data for one or more specified purposes (...)"*. It may seem that the prohibition is in vague terms. Since once given the consent, it may give rise to continue with the misuse practices, with the difference that now the user is supposedly informed. This point is related to the user's behaviour at the time of reading the privacy policies. It has been observed that the user is aware of the importance of disclosure of sensitive data. In an experiment conducted by Naeini et al. in the context of the IoT, users appreciate being informed about the purpose and periodicity of data acquisition, [37]. Even so, when deciding about it, they tend to have a permissive behaviour. The causes can be diverse and are studied from a psychological point of view. Nonetheless, a reason has been proven to be linked to the prize obtained in exchange for granting the data, as preliminary results were shown by Bock (2018), who concludes that a solution for educating users is needed [38].

To the best of our knowledge, self-determination is impossible to implement with current technical mechanisms. The systems are not designed to allow such configuration. As we briefly reviewed, methods are being developed to incorporate intervenability into systems. A first intuition is to bring into mobile phones the same functional philosophy of smartcards, since they are more powerful computationally than a smartcard. In this case, as Sanchez-Reillo (2017) compels in [28], this option is not feasible, since the smartphones are multipurpose devices, respect for the security constraints of smartcards may be in conflict with other purposes. An example of this statement may be our case of use, voice assistants pre-installed in Android smartphones. They are able to perform more tasks beyond simply to search or send SMS. They can be launched remotely with no user privileges either by the manufacturer or by external attackers, as has been demonstrated by Alepis and Patsakis (2017), [39]. In such

 ISBN: 978-1-61208-661-3

situations, current mechanisms of access control, encryption, or anonymisation are insufficient.

For these reasons, GDPR data subjects requirements regarding data management are currently not possible to guarantee. At present, we must rely on user data management platforms in the cloud provided by the data holder. In case of revocation of consent or account deletions, if this information has been disclosed to third parties previously, it is impossible to trace, and therefore to erase. For this reason, it is urgent to define protocols and common criteria security certificates with a thorough list of functional privacy and security requirements, as discussed in the paper.

V. Conclusion and Future Work

In order to create biometric systems respectful of user privacy while fulfilling GDPR requirements, new concepts in the design and implementation of privacy are needed. As stated earlier, along with the essential security requirements, privacy concepts and aspects (Unlinkability, Anonymity, Pseudonyms, Unobsevability) are defined in standards for IT systems. Nevertheless, two more aspects must be added to the list to accomplish users privacy expectations in sensible data processing: Transparency and Intervenability.

Since the use of biometrics in industry must provide accountability towards customers and data regulators, their systems should enforce the standards for biometrics. In this paper, we presented the outlook for biometric systems to embed the GDPR requirements, within which new privacy aspects are defined besides the well-known security aspects. We reviewed standards regarding biometric systems. With the idea to contribute to the analysis of further protection profiles for biometric systems, we presented the essential privacy requirements a biometric system should meet with focus on Transparency and Intervenability. For that purpose, potential threats of the unfair use of sensitive data were included in the list of threats related to biometric systems that are met in standard documentation. Some of those are profiling, no-policy-transparency, violation of the principle of proportionality, and cross-border data transfer. Regarding informal requirements, we consider it essential to reduce collected attributes of data subjects, apply user privacy preferences on data processing, and provide management permissions to the user allowing revocable consent.

For setting up PPs, basic aspects of transparency are necessary to be depicted in the CC. The current version 3.1 of CC lacks a family of the aforementioned essential privacy aspects, i.e., Transparency and Intervenability. Our contribution can be a first step to include in current version of the current CC. These two new families in the Functional Privacy Class (FPR) may be called (following the standard naming convention) FPR_TRP and FPR_INV, Transparency and Intervenability families, respectively.

Our future work continues with transparency, by means of the implementation of informed consent into protocols for user-centred systems.

Acknowledgment

The work presented has been supported in part by the European Commission through the MSCA-ITN-ETN - European Training Networks Programme under Project ID: 675087 ("AMBER - enhAnced Mobile BiomEtRics"). We would like to thank Nicholas Whiskerd for his formulations in developing this work. The information in this document is provided as is, and no guarantee or warranty is given or implied that the information is fit for any particular purpose. The user thereof uses the information at one's sole risk and liability.

References

[1] C. Cadwalladr and E. Graham-Harrison, "Revealed: 50 million facebook profiles harvested for cambridge analytica in major data breach," 2018, URL: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election, [accessed: 2018-07-16].

[2] H. Chung, M. Iorga, J. Voas, and S. Lee, "Alexa, can I trust you?" Computer, IEEE, vol. 50, no. 9, 2017, ISSN:0018-9162.

[3] J. Hubaux and A. Juels, "Privacy is dead, long live privacy," Communications of the ACM, vol. 59, no. 6, 2016, pp. 39–41, ISSN:0001-0782.

[4] J. Lane, V. Stodden, S. Bender, and H. Nissenbaum, Privacy, Big Data, and the Public Good: Frameworks for Engagement. Cambridge University Press, 2014, doi:10.1017/CBO9781107590205.

[5] "Regulation (EU) 2016/679 of the european parliament and of the council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/ec (general data protection regulation) (text with eea relevance)," 2016, URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679, [accessed: 2018-07-16].

[6] J. Bustard, "The impact of EU privacy legislation on biometric system deployment: Protecting citizens but constraining applications," Signal Processing Magazine, IEEE, vol. 32, no. 5, 2015, pp. 101–108, ISSN:1053-5888.

[7] G. Danezis, J. Domingo-Ferrer, M. Hansen, J. Hoepman, D. Metayer, R. Tirtea, and S. Schiffner, "Privacy and data protection by design-from policy to engineering," Tech. Rep., 2015, ISSN: 978-92-9204-108-3, URL:https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design, [accessed: 2018-07-16].

[8] K. Bock, W. Ernestus, M. Kamp, L. Konzelmann, T. Naumann, U. Robra, M. Rost, G. Schulz, J. Stoll, U. Vollmer, and M. Wilms, "The standard data protection model a concept for inspection and consultation on the basis of unified protection goals, version 1.1 (pdf)," 2018, URL: https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/SDM-Methode_V_1_1.pdf (in German), [accessed: 2018-07-16].

[9] N. R. Council, Biometric Recognition: Challenges and Opportunities. Washington, DC: The National Academies Press, 2010, ISBN= 978-0-309-14207-6. [Online]. Available: https://www.nap.edu/catalog/12720/biometric-recognition-challenges-and-opportunities

[10] U. Gasser and V. Almeida, "A layered model for AI governance," IEEE Internet Computing, vol. 21, no. 6, 2017, pp. 58–62.

[11] J. Havens, "Ethically aligned standards - a model for the future," 2017, URL: https://www.standardsuniversity.org/e-magazine/march-2017/ethically-aligned-standards-a-model-for-the-future/, [accessed: 2018-07-16].

[12] "European project: Paasword - a holistic data privacy and security by design platform-as-a-service framework introducing distributed encrypted persistence in cloud-based applications," 2015-2017, URL:https://cordis.europa.eu/project/rcn/194247/_en.html, [accessed: 2018-07-16].

[13] "European project: Credential - secure cloud identity wallet," 2018, URL: https://credential.eu/, [accessed: 2018-07-16].

[14] "European project: From real-world identities to privacy-preserving and attribute-based credentials for device-centric access control," 2015-2018, URL: https://cordis.europa.eu/project/rcn/194863/_en.html, [accessed: 2018-07-16].

[15] "European project: Amber - enhanced mobile biometrics," 2017, URL: https://www.amber-biometrics.eu/, [accessed: 2018-07-16].

[16] C. Vielhauer, J. Dittmann, and S. Katzenbeisser, "Design aspects of secure biometric systems and biometrics in the encrypted domain," in Security and Privacy in Biometrics. Springer, 2013, pp. 25–43.

 ISBN: 978-1-61208-661-3

[17] N. Mead, "The common criteria," 2013, URL: https://www.us-cert.gov/bsi/articles/best-practices/requirements-engineering/the-common-criteria, [accessed: 2018-07-16].

[18] T. Nils and L. Boris, "Biometric verification mechanisms protection profile bvmpp,v1.3," Bundesamt für Sicherheit in der Informationstechnik Common Criteria, Protection Profile, 2008, URL: https://www.commoncriteriaportal.org/files/ppfiles/pp0043b.pdf, [accessed: 2018-07-16].

[19] N. T. Boris Leidner, "Fingerprint spoof detection protection profile based on organisational security policies fsdpp_osp v1.7," Bundesamt für Sicherheit in der Informationstechnik Common Criteria, Protection Profile, 2010, URL: https://www.commoncriteriaportal.org/files/ppfiles/pp0062b_pdf.pdf, [accessed: 2018-07-16].

[20] C. W. G. for Biometric Product Security, "Biometric Product Essential Security Requirements," Common Criteria, Protection Profile, Nov. 2016, URL: https://www.commoncriteriaportal.org/communities/bio-esr.pdf, [accessed: 2018-07-16].

[21] C. Tilton and M. Young, Standards for Biometric Data Protection. Springer London, 2013, pp. 297–310, ISBN = 978-1-4471-5230-9.

[22] "ISO/IEC 30136:2018 Information technology – Performance testing of biometric template protection schemes," International Organization for Standardization, Standard, Mar. 2018.

[23] P. Dash, C. Rabensteiner, F. Hrandner, and S. Roth, "Towards privacy-preserving and user-centric identity management as a service," in Open Identity Summit 2017, L. Fritsch, H. Ronagel, and D. Hhnlein, Eds. Gesellschaft fr Informatik, Bonn, Oct. 2017, pp. 105–116.

[24] H. Gunasinghe and E. Bertino, "Privacy preserving biometrics-based and user centric authentication protocol," in Network and System Security. Springer International Publishing, 2014, pp. 389–408.

[25] S. Wohlgemuth, "Adaptive user-centered security," in Availability, Reliability, and Security in Information Systems. Springer International Publishing, 2014, pp. 94–109, ISBN = 978-3-319-10975-6.

[26] J. Martínez, J. Hernández-Ramos, V. Beltrán, A. Skarmeta, and P. Ruiz, "A user-centric internet of things platform to empower users for managing security and privacy concerns in the internet of energy," International Journal of Distributed Sensor Networks, vol. 13, no. 8, 2017, doi:10.1177/1550147717727974.

[27] M. Gomez-Barrero, J. Galbally, C. Rathgeb, and C. Busch, "General framework to evaluate unlinkability in biometric template protection systems," IEEE Transactions on Information Forensics and Security, vol. 13, no. 6, June 2018, pp. 1406–1420, ISSN: 1556-6013.

[28] R. Sanchez-Reillo, Biometric systems in unsupervised environments and smart cards: conceptual advances on privacy and security, ser. Security. Institution of Engineering and Technology, 2017, pp. 97–122, Chapter 5, URL: http://digital-library.theiet.org/content/books/10.1049/pbse004e_ch5.

[29] B. Fernandez-Saavedra, R. Sanchez-Reillo, J. Liu-Jimenez, and O. Miguel-Hurtado, "Evaluation of biometric system performance in the context of common criteria," Information Sciences, vol. 245, 2013, pp. 240 – 254, ISSN:0020-0255.

[30] A. D. S. LLC, "Alexa terms of use - amazon privacy notice," 2018, URL: https://www.amazon.com/gp/help/customer/display.html?nodeId=201909010, [accessed: 2018-07-16].

[31] C. James and Y. Lisa, "A taxonomy of operational cyber security risks," Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, Tech. Rep. CMU/SEI-2010-TN-028, 2010, URL: http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=9395, [accessed: 2018-07-16].

[32] L. Marinos, "Enisa threat taxonomy: A tool for structuring threat information initial version, 1.0," ENISA, Heraklion, Tech. Rep., 2016, URL: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/etl2015/enisa-threat-taxonomy-a-tool-for-structuring-threat-information/view, [accessed: 2018-07-16].

[33] P. Campisi, Security and Privacy in Biometrics: Towards a Holistic Approach. London: Springer London, 2013, pp. 1–23, Chapter 1, ISBN= 978-1-4471-5230-9.

[34] L. Kugler, "The war over the value of personal data," Commun. ACM, vol. 61, no. 2, 2018, pp. 17–19, ISSN:0001-0782.

[35] S. Barocas and H. Nissenbaum, "Big data's end run around procedural privacy protections," Communications of the ACM, vol. 57, no. 11, 2014, pp. 31–33.

[36] N. Whiskerd, J. Dittmann, and C. Vielhauer, "A requirement analysis for privacy preserving biometrics in view of universal human rights and data protection regulation," 2018, to appear in Proc. EUSIPCO 2018.

[37] P. Naeini, S. Bhagavatula, H. Habib, M. Degeling, L. Bauer, L. Cranor, and N. Sadeh, "Privacy expectations and preferences in an iot world," in Proceedings of the 13th Symposium on Usable Privacy and Security (SOUPS), JUL 2017, pp. 399–412.

[38] S. Bock, "My data is mine - users' handling of personal data in everyday life," in Sicherheit 2018, Beiträge der 9. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.V. (GI), Konstanz., Apr. 2018, pp. 261–266, URL:https://dblp.org/rec/bib/conf/sicherheit/Bock18.

[39] E. Alepis and C. Patsakis, "Monkey says, monkey does: Security and privacy on voice assistants," IEEE Access, vol. 5, 2017, pp. 17 841–17 851, doi:10.1109/ACCESS.2017.2747626.

 ISBN: 978-1-61208-661-3