Border Control and Use of Biometrics: Reasons Why the Right to Privacy Can Not Be Absolute

Mohamed Abomhara, Sule Yildirim Yayilgan, Marina Shalaginova, Zoltán Székely

Border Control and Use of Biometrics: Reasons Why the Right to Privacy can not be Absolute*

Mohamed Abomhara[1], Sule Yildirim Yayilgan[1], Marina Shalaginova[1], and Zoltán Székely[2]

[1] Department of Information Security and Communication Technology, Norwegian University of Science and Technology, Gjøvik, Norway
{mohamed.abomhara, sule.yildirim, marina.shalaginova}@ntnu.no
[2] National University of Public Service, Faculty of Law Enforcement, Hungary
dr.szekely.zoltan@gmail.com

Abstract. This paper discusses concerns pertaining to the absoluteness of the right to privacy regarding the use of biometric data for border control. The discussion explains why privacy cannot be absolute from different points of view, including privacy versus national security, privacy properties conflicting with border risk analysis, and Privacy by Design (PbD) and engineering design challenges.

Keywords: Biometrics · Biometric technology · Border control · Data privacy · Right to privacy.

1 Introduction

Biometric technologies are automated methods of recognizing and verifying the identity of individuals based on physiological or behavioral attributes [11]. They are used progressively more and are highly adopted at European borders [20,21]. Strengthening border security, improving border crossing efficiency and facilitating effective migration control and enforcement are among the main grounds for utilizing biometric technologies [26]. Despite the many advantages of biometrics, there are some limitations. The integration of biometric information systems employed for border control leads to increased surveillance that involves collecting and storing personal data such as fingerprints as individuals cross borders, apply for visas or request asylum. According to the General Data Protection Regulation (GDPR) [49], personal information falls in a number of general categories, such as identity number and financial information (Article 4(1) GDPR) as well as special categories, for instance, biometric data, sexual orientation, medical information, personal activities, etc. (Article 9(1) GDPR). Such information is a valuable asset because it is crucial for all individuals to be able to keep it to themselves. On one hand, biometric technology has been proven to be cost-effective

*This work is carried out as part of the EU-funded project SMart mobILity at the European land borders (SMILE) (Project ID: 740931), [H2020-DS-2016-2017] SEC-14-BES- 2016 towards reducing the cost of technologies in land border security applications.

in enhancing border security, detecting fraud, helping improve border crossing efficiency as well as enabling effective migration control and enforcement [9]. On the other hand, biometric technology has serious impacts on privacy and data protection [33].

Major concerns with the use of biometric technology relate to individuals' privacy reduction and the immutable link between biometric traits and persistent information storage about a person. The tight link between personal information and biometrics can have both positive and negative consequences for individuals' privacy. Recent research [17] explores the possibility of extracting supplementary information from primary biometric traits, e.g. face, fingerprints and iris. These traits denote personal attributes like gender, age, ethnicity, hair color, height, weight and so on. However, a breach (unauthorized acquisition, access, use or disclosure) of such confidential information would violate the principle of the right to privacy for those consenting to cross a border, even if the breach involved innocuous information that would not result in any social, economic, legal, or any other harm.

The right to privacy is described as the right of the individual to be let alone and to decide how, when, with whom and to what degree their personal data should be shared and communicated [30, 51]. However, unlike absolute fundamental rights as "the right to life or the prohibition of torture and inhuman or degrading treatment or the right to be free from slavery," which admit of no restriction (judgment of Court of Justice of the European Union (CJEU) of 12 June 2003, Schmidberger, Case C-112/00, paragraph 80 [5]), the right to privacy is not an absolute right and hence can be limited by law [27,35] – for example in time of public emergency that threatens the life of a nation. The arguments made in this paper pertain to why privacy cannot be absolute from different points of view: (1) privacy versus national security; (2) privacy properties conflicting with border risk analysis; and (3) Privacy by Design (PbD) and engineering design challenges.

The remaining part of this paper is organized as follows. Section 2 briefly discusses the use of biometrics for border control and the right to privacy principle. Section 3 investigates and argues why privacy cannot be absolute. Section 4 concludes the paper.

2 Background

2.1 The use of biometrics for border control

The dramatic advances in biometric technologies have opened doors to unprecedented opportunities in the field of border control. The challenge of border security is to identify with assurance who is crossing the border and decide if the person is authorized to cross or not. Unassisted by technology, a border staff member cannot maintain this degree of swift, assured identification. Border authorities are equipped with biometric technologies to facilitate more efficient checks at borders and contribute to preventing and combating illegal migration,

etc. [26]. Biometrics enable accurate identification since each person has their own unique physical characteristics. Moreover, the use of multimodal biometrics [29, 37] offers even better results with higher accuracy by combining several biometrics [34]. Multimodal biometrics-integrated border management benefits all stakeholders, including governments concerned with securing national territory, immigration authorities managing controls at ever more crowded borders, and simply travelers who want to enjoy the journey to their destination [21].

European Union (EU)-wide border biometric information management systems [20], including the European Asylum Dactyloscopy Database (EURODAC), Visa Information System (VIS) and Second-generation Schengen Information System (SIS II) have an increasingly important role in the identity establishment process by storing biographic and biometric data of third-country nationals [12, 39]. In addition, the centralized Entry/Exit System (EES) of border control is expected to be fully implemented by 2020 in compliance with Regulations (EU) 2017/2225 [2] and (EU) 2017/2226 [3]. Interoperability will allow the EU information systems to complement each other, help facilitate the correct identification of persons, contribute to fighting identity fraud and ease information sharing. Accordingly, the SMart mobILity at the European land borders (SMILE)[1] interoperability with other border information systems is greatly promising in terms of enhancing the speed, efficiency and flow of border crossing mobility as well as border security.

As a border control tool, SMILE encourages the propensity to collect, use and process sensitive biometrics like fingerprints, face and iris data, etc. to improve traveler flow and boost border security. On the one hand, SMILE technologies are intended to enhance security levels and make the traveler identification and authentication procedures easy, fast and convenient. On the other hand, similar to other biometric technologies, SMILE technologies have raised new threats to fundamental rights, data protection and privacy.

2.2 Right to privacy

Every individual has the right to the privacy protection of their personal information when it is collected and shared. Generally, legal documents on data protection and privacy such as GDPR [49] refer to personal information protection throughout all steps from collection to storage and dissemination. Moreover, provisions of the European Convention of Human Rights (ECHR) constitute the basis for challenging inequitable decisions of public authorities [15, 27, 50]. Article 8 ECHR ensures everyone's right to have their private and family life, home and correspondence respected without public authority interference. The aforementioned right is mirrored in Article 7 of the Charter of Fundamental Rights (CFR). Moreover, Article 8 of the Charter enshrines the right of everyone to the protection of their personal data. Individuals (data subjects) have the right to exercise control over their personal data (Article 12-23 GDPR [49]). Protection

[1] http://smile-h2020.eu/smile/

of privacy is frequently seen as a line drawn for how far society can intrude into a person's private affairs [35].

However, these rights can be overruled if a legal basis is laid down for collecting, processing, storing or retaining personal data to achieve a legitimate goal [13]. According to Article 52(1) CFR, "subject to the principle of proportionality, limitations of rights to privacy may be made only if they are necessary and genuinely meet objectives of general interest recognized by the Union or the need to protect the rights and freedoms of others." Moreover, Recital 4 GDPR acknowledges that the right to data protection (as well as the right to privacy) is not an absolute right. Ruling the Eifert case [6], the CJEU holds that "the right to the protection of personal data is not an absolute right, but must be considered in relation to its function in society." Furthermore, the rights to privacy must be proportionately balanced with other fundamental rights. According to the Opinion of Advocate General Jääskinen in the Google Spain Case [7], the fundamental rights to privacy and to the protection of personal data are not absolute and may be limited provided there is a justification acceptable in view of the conditions set out in Article 52(1) of the Charter.

3 Viewpoints of privacy: Why it can not be absolute

This section discusses the contradictory interests of privacy versus national security, privacy properties conflicting with border risk analysis and Privacy by Design (PbD) and engineering design challenges.

3.1 Privacy versus national security

The Schengen Borders Code (SBC) (Regulation (EU) 2016/399) [1] and its amendment (Regulation (EU) 2017/458) [4] set out the rules governing the movement of people across EU's internal and external borders. Internal borders means (a) the common land borders, including river and lake borders, of the Member States; (b) the airports of the Member States for internal flights; (c) sea, river and lake ports of the Member States for regular internal ferry connections. External borders means the Member States' land borders, including river and lake borders, sea borders and their airports, river ports, sea ports and lake ports, provided that they are not internal borders. SBC also defines the rules for the border checks of persons crossing external Schengen borders (border checks on persons). Cross-border movement at external borders shall be subject to minimum and thorough checks by border guards (Article 8 of Regulation (EU) 2016/399). The main objectives of the minimum and thorough checks are to ensure that the persons in question do not represent a threat to public order, internal security or public health, and to improve the security of the EU Member States and their citizens. Therefore, the key issue in question is how to achieve a trade-off between border check requirements (Regulation (EU) 2016/399) to ensure border security and meeting the need for flexible border crossing without compromising individuals' privacy.

According to a survey and interviews carried out for the SMILE project with land border guards (refer to the SMILE public deliverables), the majority of guards claim that the use of biometric authentication and verification at land borders is justified and necessary to improve border security measures and better protect the public interest. Biometrics are believed to help improve the accuracy of traveler identification and verification, meaning the ability to correctly recognize a genuine person and reject an imposter. Moreover, utilizing biometrics promotes the reduction of identity fraud (e.g., fake IDs and passports) as the identification and verification processes do not rely on the human agent. To the best of our knowledge, fraud reduction signifies accuracy increase. Therefore, using biometrics eliminates a considerable integrity threat that border guards face and benefits the authority responsible for border control. As a consequence, biometrics would result in a higher throughput of low-risk travelers without losing accuracy or integrity and allow human resources to focus on potentially higher-risk travelers.

The right of people to be respected for their private and family life, home, etc. (Article 8 of the ECHR) and also protected against unreasonable biometric searches (e.g., unreasonable biometric authentication and verification at the border) shall not be violated. For border authorities to be reasonable with using biometrics, traveler authentication and verification using biometrics must be as limited in its intrusiveness as it is consistent with satisfying the administrative need that justifies it [32]. It is important to argue on the one hand whether the introduction of biometrics for border control can be regarded as being in accordance with the law and if the biometrics satisfy a legitimate aim (public safety, crime prevention, etc.), proportionality and the necessity principles pursuant to Article 8 of ECHR. On the other hand, it is arguable whether breaching the right to privacy is also considered proportionate to the threats that biometric technologies are supposed to prevent. As for necessity and effectiveness, many discussions address whether biometrics actually add value to serving border control interests, including but not limited to, providing the safe, secure, efficient and unobtrusive, on-the-move security control of travelers, fighting terrorism and serious crime, and ensuring high internal security levels.

If national security has greater priority, should individual privacy yield? Besides, would it be ethically justifiable to sacrifice some privacy interests to achieve the highest national security gains possible? Moreover, if a traveler faces the dilemma of either providing biometrics or not being allowed to cross the border (in case no other alternative is provided), the person's right to freedom of movement may be restricted [35]. Our conclusion is not yet sufficiently clear to answer these questions. Even if it is accepted that using biometrics at borders is necessary and proportionate, serious concerns about whether the intrusion is in accordance with the law still remains a question. It may be said that conflicts arising between border security (Regulation (EU) 2016/399) interests and individual privacy cannot be weighed because they are not measurable by the same standards [31]. While acknowledging there could be legitimate aims for the invasion of privacy, the effectiveness of biometrics is still questionable. Therefore, a

sensible trade-off is necessary between individual interests (individual privacy) and the legitimate concerns of the Member States such as preventing and investigating crime [40, 48]. An appropriate trade-off would involve retaining the benefits of biometric technologies to extend the border control ability to support high border security and reliability while maintaining individual privacy.

3.2 Privacy properties conflicting with border risk analysis

Border risk analysis is a governance tool to normalize border and migration risks. It is based on an automated analysis of lager databases (SIS II, etc.) to extract useful information about people and their activities in order to identify behavioral patterns that may point to suspicious activity. Although border risk analysis is useful in decision-making, it can also lead to serious privacy concerns.

The key issue is in the contradictory interests of the principle of data minimization (Article 5 GDPR) that limits personal data collection, use and disclosure and the benefit of the capability to process personal data for performing border risk analysis. The main concerns include the unnecessary and unauthorized collection of biometric data for traveler identification and verification [14, 51]. For one, the data minimization principle and strong privacy properties (i.e., unlinkability, anonymity, undetectability) [19] restrict personal data collection and use for further analysis. However, border risk analysis requires the use of personal data for the investigation and/or monitoring of actions/activities of one or more individuals. In other words, the more personal data border authorities, for instance, can obtain about individuals, the better the risk prediction and thus overall risk analysis results will be. There has certainly been considerable progress in privacy preserving techniques for data analytics [38, 41]. Nonetheless, even with such privacy-friendly techniques, border risk analysis is prone to privacy violations.

Another major concern is related to the potential for function/purpose creep. Purpose creep occurs when personal data is collected for one specific purpose and subsequently used for another unintended or unauthorized purpose without the user's consent. A famous example of a large-scale biometric function creep is related to the European Dactyloscopy (EURODAC) fingerprint database (Regulation (EC) 2725/2000). The original purpose of the EURODAC database was to compare fingerprints for the effective application of the Dublin convention (Regulation (EU) 603/2013) [51]. EURODAC enables EU countries to identify asylum applicants as well as illegal immigrants within the EU. However, soon after the database was established, other police and law enforcement agencies were also granted access. There are many other large-scale, centralized EU national and international databases, such as SIS II and VIS with the same risks. Similar concerns also arise in the case of border control risk analysis [9]. Hard and soft biometrics [8, 18, 52] are likely to strengthen the potential for function creep due to the very sensitive nature of the data collected and the possibility to use centrally stored biometric data for purposes other than the original purpose (border crossing). Moreover, such databases offer more attractive targets for outsider attacks and insider misuse.

Therefore, the purpose specification principle (Article 5(1)(b) of GDPR), which is among the main principles of EU data protection legislation, has a key role. According to Article 5(1)(b) of GDPR, personal data must be collected for specified, explicit and legitimate purposes and not be further processed in a way incompatible with those purposes. However, GDPR provides exemptions in Article 23, which stipulates that Member States' laws may restrict the scope of the principles mentioned in Article 5 of GDPR when such restriction constitutes a necessary measure to safeguard national security and public security, to prevent, investigate, detect or prosecute criminal offences or execute criminal penalties, to protect the data subject or the rights and freedoms of others, etc. In our view, the indication of "a necessary measure" means that exemptions are restricted to specific investigations, case-by-case requests, and not to cases where personal data processing is systematic as foreseen by the use of biometrics for border control. As mentioned earlier, the processing of biometric data is questionable even when considering that an exemption might be applicable. Therefore, the problems of function creep and purpose misuse are not to be underestimated. Nonetheless, they can be curbed by stricter laws, particularly by limiting the use of specific biometric data for certain purposes. It can thus be concluded that the clarity of purpose regarding the intention of biometric data collection is paramount. It is important to be clear about the necessity for biometrics and how biometrics will help fulfill specified needs.

3.3 Privacy by Design (PbD) and engineering design

Privacy by design (PbD) is a policy measure that guides software developers to apply inherent solutions to achieve better privacy protection [23]. For privacy to be embedded in the system development lifecycle and hence in organizational processes, system developers and policy makers must be ready to embrace and understand the domain [47].

Recent studies [23,36,43,44] reveal that most software developers lack formal knowledge and understanding of the concept of informational privacy. Besides, most have insufficient knowledge of how to develop privacy practices such as PbD [23]. Software developers additionally find it difficult to understand privacy requirements by themselves [44] and require significant effort to estimate privacy risks from a user perspective in order to relate privacy requirements to privacy techniques [36]. Moreover, software developers have trouble evaluating whether they have successfully embedded PbD strategies into the system design.

Privacy design frameworks serve as potential bridges between users, software developers and policy makers. Several studies like [22, 24, 28, 46] discuss privacy design frameworks to assist software developers with addressing privacy during the system development process. However, to the best of our knowledge, it is still unclear how effective these design frameworks are and what the possible limitations for their utilization in everyday privacy engineering practices are. The key elements of PbD are intended to limit the collection, use and disclosure of personal data, to involve individuals in the data lifecycle, and to apply appropriate

safeguards in a continuous manner [31]. This means separating personal identifiers, using pseudonyms and anonymization as well as deleting personal data when no longer needed [42]. However, as argued by Leese [31], such practices are undeniably suitable in economic and organizational contexts. But as discussed in Sections 3.1 and 3.2, border checks and border risk analysis derive decisions exactly through the collection and processing of data, which could ultimately be connected to possible criminal activities, in order to control any risk. On the contrary, essentially PbD principles radically exclude the possibilities that come with advanced data analytics in border control contexts. Thus, the contradictory interests of PbD principles and the benefit of the ability to process biometrics data for border control cannot simply be resolved by technical means.

Thus, if PbD is ever to become a viable practice, a considerable change must be made to prepare the field for the wide implementation of this policy. Privacy implementation guidelines should be provided to help software developers and policy makers embed privacy into the system design. Moreover, an evaluation and demonstration of privacy assurance – as recommended by the ENISA[2] guidelines for privacy and data protection [16] – is required to provide software developers with feedback to verify whether they have successfully followed the guidelines. This would reduce software developers' personal opinions on privacy practices and ease how privacy is embedded into the system. Moreover, the development method (Agile Software Development [10], Security Development Lifecycle [25, 45], etc.) used within the organization must be taken into account in order to apply the concepts of privacy throughout the entire system development process. This will enable development teams, policy makers, etc. to take appropriate measures in the relevant phases. Finally, upon design completion, the organization must adopt and monitor it throughout its lifetime.

Alongside the PbD issue is the Privacy by Default obligation. Under this obligation, data controllers must implement appropriate measures on both technical and organization levels to ensure that personal data collected is only used for specific purposes. Essentially, only the minimum amount of personal data required should be collected and stored, while data subjects should be allowed data accessibility and controllability. Ensuring privacy through every phase of the data lifecycle (collection, use, retention, storage, disposal or destruction) has also become crucial to avoiding legal liability, maintaining regulatory compliance, and so on. Therefore, integrating the Data Protection Impact Assessment (DPIA) with the Ethical Impact Assessment (EIA) and Privacy Impact Assessment (PIA) in the earlier stages of any system development would aid with the early identification of ethical and privacy problems and risks. Ideally, a full and detailed description of the processing along with its necessity and proportionality would help manage the risks to the rights and freedoms of natural persons resulting from personal data processing. Furthermore, taking PbD strategies into consideration should precede system design to ensure that ethical and privacy principles are taken into account. As a result, data controllers will be more able

[2]European Union Agency for Network and Information Security (www.enisa.europa.eu).

to comply with the legal requirements of data protection and demonstrate taking appropriate measures where DPIA is used to check compliance against data protection regulations.

4 Conclusions

Border control systems raise the tendency to collect, use and process personal data (e.g. alphanumeric data like names and birth dates; biographic information; biometric data like fingerprints) to optimize and monitor the flow of people at land borders as well as enhance security and detect fraud. However, evidence demonstrates that personal data collection and processing pose several privacy challenges. Privacy is a fundamental human right in EU countries and is controlled by legislation that responds and adapts to data subjects' privacy needs. Moreover, the obligations of the Member States pertaining to personal data collection and processing along with the exchange of personal data among Member States are stated in various EU laws and regulations. It is therefore essential for border authorities to consider the legal consequences of developing and deploying biometric identification and authentication methods.

Personal data flows and ripples are in some ways difficult to predict. Despite all attempts to provide anonymity, biometric data still penetrates a person's physical, psychological and social identity. Biometric technology enables revealing personal information, such as gender, age, ethnicity and even critical health problems like diabetes, vision problems, Alzheimer's disease, etc. Members of particular groups including disabled, transgender and older people, religious groups, and others, can encounter additional negative effects on privacy. Although numerous proposals, recommendations and legal considerations are in place as safeguards, it is unclear how they can ultimately be put in practice. For example, even a well-conceived, general and sustainable data protection and privacy regulation like GDPR is strained by the effort to ensure superior effectiveness with respect to privacy.

It is quite obvious that biometric technology exposes travelers to significant loss of privacy and limitations of other rights and freedoms. This paper discussed concerns with the absoluteness of the right to privacy regarding the use of biometric data for border control. In accordance with Article 8(2) ECHR, "there shall be no interference by a public authority with the exercise of the right to privacy except such as is in accordance with the law." The exemption clause contains two conditions: (1) the necessity for a democratic society that should be proportional to the purposes of the law and (2) exceptions in accordance with the law. These conditions require a specific legal rule that authorizes the interference and sufficient access of individuals to the specific law, and that the law must be precisely formulated in order to ensure that individuals are capable of foreseeing the conditions of its applicability.

In future, the authors plan to investigate the effect of using biometrics for border control on individuals' privacy. Unfortunately, there is still too little knowledge about the real effects on individuals and a system's reputation when

privacy breaches occur. This is because on the one hand, very little knowledge exists about the tangible and intangible benefits of personal data collection in EU information systems. On the other hand, it is not clear to what extent people have the right to choose what information about themselves to share and how to engage with border systems and devices such as biometric sensors and readers.

References

1. Regulation (EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code). Official Journal of the European Union 2017, L 77/1, https://eur-lex.europa.eu/eli/reg/2016/399/oj
2. Regulation (EU) 2017/2225 of the European Parliament and of the Council of 30 November 2017 amending Regulation (EU) 2016/399 as regards the use of the Entry/Exit System. Official Journal of the European Union 2017, L 327/1, https://eur-lex.europa.eu/eli/reg/2017/2225/oj
3. Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011. Official Journal of the European Union 2017, L 327/20, https://eur-lex.europa.eu/eli/reg/2017/2226/oj
4. Regulation (EU) 2017/458 of the European Parliament and of the Council of 15 March 2017 amending Regulation (EU) 2016/399 as regards the reinforcement of checks against relevant databases at external borders. Official Journal of the European Union 2017, L 74/1, https://eur-lex.europa.eu/eli/reg/2017/458/oj
5. Court of Justice of the European Union, C-112/00, Eugen Schmidberger, Internationale Transporte und Planzüge v Republik Österreich (2003)
6. Court of Justice of the European Union, Joined Cases C-92/09 and C-93/09, Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen (2010)
7. Court of Justice of the European Union, Case C-131/12, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González (2014)
8. Abdelwhab, A., Viriri, S.: A survey on soft biometrics for human identification. Machine Learning and Biometrics p. 37 (2018)
9. Abomhara, M., Yildirim Yayilgan, S., Elezaj, a., Székely, Z., Elezaj, O.: How to do it right: A framework for biometrics supported border control. In Proceedings of the 8th International Conference on e-Democracy 2019, CCIS 1111, pp. 1–16, 2020 (12 2019)
10. Abrahamsson, P., Salo, O., Ronkainen, J., Warsta, J.: Agile software development methods: Review and analysis. VTT Technical Research Centre of Finland, VTT Publications 478 (2017)
11. Bhatia, R.: Biometrics and face recognition techniques. International Journal of Advanced Research in Computer Science and Software Engineering **3**(5) (2013)
12. Boehm, F.: Information sharing and data protection in the area of freedom, security and justice: Towards harmonised data protection principles for information exchange at EU-level. Springer Science & Business Media (2011)

13. Bonnici, J.P.M.: Exploring the non-absolute nature of the right to data protection. International Review of Law, Computers & Technology **28**(2), 131–143 (2014)
14. Campisi, P.: Security and privacy in biometrics, vol. 24. Springer (2013)
15. Çinar, Ö.H.: The right to privacy in international human rights law. Journal of Information Systems & Operations Management **13**(1), 33–44 (2019)
16. Danezis, G., Domingo-Ferrer, J., Hansen, M., Hoepman, J.H., Metayer, D.L., Tirtea, R., Schiffner, S.: Privacy and data protection by design-from policy to engineering (2014), https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design
17. Dantcheva, A., Elia, P., Ross, A.: What else does your biometric data reveal? a survey on soft biometrics. IEEE Transactions on Information Forensics and Security **11**(3), 441–467 (2016)
18. Dantcheva, A., Velardo, C., D'angelo, A., Dugelay, J.L.: Bag of soft biometrics for person identification. Multimedia Tools and Applications **51**(2), 739–777 (2011)
19. Deng, M., Wuyts, K., Scandariato, R., Preneel, B., Joosen, W.: A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements. Requirements Engineering **16**(1), 3–32 (2011)
20. eu-LISA: Biometrics in large-scale it: Recent trends, current performance capabilities, recommendations for the near future. European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA) (2018), https://www.eulisa.europa.eu/Publications/Reports/Biometrics%20in%20Large-Scale%20IT.pdf
21. European Commission: Biometrics technologies: a key enabler for future digital services. Digital Transformation Monitor (2018)
22. Gürses, S., Troncoso, C., Diaz, C.: Engineering privacy by design. Computers, Privacy & Data Protection **14**(3), 25 (2011)
23. Hadar, I., Hasson, T., Ayalon, O., Toch, E., Birnhack, M., Sherman, S., Balissa, A.: Privacy by designers: software developers' privacy mindset. Empirical Software Engineering **23**(1), 259–289 (2018)
24. Hoepman, J.H.: Privacy design strategies. In: IFIP International Information Security Conference. pp. 446–459. Springer (2014)
25. Howard, M., Lipner, S.: The security development lifecycle, vol. 8. Microsoft Press Redmond (2006)
26. International Civil Aviation Organization (ICAO): Icao tyou rip guide on border control management (2017), https://www.icao.int/Meetings/TRIP-Jamaica-2017/Documents/ICAO%20TRIP%20Guide%20on%20BCM-For%20validation-16-11-2017.pdf
27. Jonsson Cornell, A.: The right to privacy. Oxford University Press (2016), https://oxcon.ouplaw.com/view/10.1093/law:mpeccol/law-mpeccol-e156
28. Kalloniatis, C., Kavakli, E., Gritzalis, S.: Addressing privacy requirements in system design: the pris method. Requirements Engineering **13**(3), 241–255 (2008)
29. Khoo, Y.H., Goi, B.M., Chai, T.Y., Lai, Y.L., Jin, Z.: Multimodal biometrics system using feature-level fusion of iris and fingerprint. In: Proceedings of the 2nd International Conference on Advances in Image Processing. pp. 6–10. ACM (2018)
30. Kizza, J.M., et al.: Ethical and social issues in the information age, vol. 999. Springer (2013)
31. Leese, M.: Privacy and security–on the evolution of a european conflict. In: Reforming European Data Protection Law, pp. 271–289. Springer (2015)

32. Lind, N.S., Rankin, E.T.: Privacy in the Digital Age: 21st-Century Challenges to the Fourth Amendment: 21st-Century Challenges to the Fourth Amendment, vol. 2. ABC-CLIO (2015)
33. Liu, N.Y.: Bio-privacy: Privacy regulations and the challenge of biometrics. Routledge (2013)
34. Lumini, A., Nanni, L.: Overview of the combination of biometric matchers. Information Fusion **33**, 71–85 (2017)
35. Mironenko, O.: Body scanners versus privacy and data protection. Computer Law & Security Review **27**(3), 232–244 (2011)
36. Oetzel, M.C., Spiekermann, S.: A systematic methodology for privacy impact assessments: a design science approach. European Journal of Information Systems **23**(2), 126–150 (2014)
37. Parkavi, R., Babu, K.C., Kumar, J.A.: Multimodal biometrics for user authentication. In: 2017 11th International Conference on Intelligent Systems and Control (ISCO). pp. 501–505. IEEE (2017)
38. Rao, P.R.M., Krishna, S.M., Kumar, A.S.: Privacy preservation techniques in big data analytics: a survey. Journal of Big Data **5**(1), 33 (2018)
39. Robinson, N., Gaspers, J.: Information security and data protection legal and policy frameworks applicable to european union institutions and agencies (2014)
40. Rung, S., van Lieshout, M., Friedewald, M., Ooms, M., van den Broek, T.: Privacy and security: Citizens' desires for an equal footing. In: Surveillance, Privacy and Security, pp. 15–35. Routledge (2017)
41. Saranya, K., Premalatha, K., Rajasekar, S.: A survey on privacy preserving data mining. In: 2015 2nd International Conference on Electronics and Communication Systems (ICECS). pp. 1740–1744. IEEE (2015)
42. Schaar, P.: Privacy by design. Identity in the Information Society **3**(2), 267–274 (2010)
43. Senarath, A., Arachchilage, N.A.: Why developers cannot embed privacy into software systems?: An empirical investigation. In: Proceedings of the 22nd International Conference on Evaluation and Assessment in Software Engineering 2018. pp. 211–216. ACM (2018)
44. Sheth, S., Kaiser, G., Maalej, W.: Us and them: a study of privacy requirements across north america, asia, and europe. In: Proceedings of the 36th International Conference on Software Engineering. pp. 859–870. ACM (2014)
45. Shostack, A.: Threat modeling: Designing for security. John Wiley & Sons (2014)
46. Spiekermann, S., Cranor, L.F.: Engineering privacy. IEEE Transactions on software engineering **35**(1), 67–82 (2008)
47. Spiekermann-Hoff, S.: The challenges of privacy by design. Communications of the ACM (CACM) **55**(7), 34–37 (2012)
48. Valkenburg, G.: Privacy versus security: Problems and possibilities for the trade-off model. In: Reforming European Data Protection Law, pp. 253–269. Springer (2015)
49. Voigt, P., Von dem Bussche, A.: The eu general data protection regulation (gdpr). A Practical Guide, 1st Ed., Cham: Springer International Publishing (2017)
50. Warren, S., Brandeis, L.: The right to privacy. Litres (2019)
51. Zeadally, S., Badra, M.: Privacy in a Digital, Networked World: Technologies, Implications and Solutions. Springer (2015)
52. Zewail, R., Elsafi, A., Saeb, M., Hamdy, N.: Soft and hard biometrics fusion for improved identity verification. In: The 2004 47th Midwest Symposium on Circuits and Systems, 2004. MWSCAS'04. vol. 1, pp. I–225. IEEE (2004)