How to do it right: A framework for biometrics supported border control

Mohamed Abomhara[1], Sule Yildirim Yayilgan[1], Anne Hilde Nymoen[1], Marina Shalaginova[1], Zoltán Székely[2], and Ogerta Elezaj[1]

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

Abstract. Complying with the European Union (EU) perspective on human rights goes or should go together with handling ethical, social and legal challenges raising due to the use of biometrics technologies as border control technologies. While there is no doubt that the biometric technologies at European borders is a valuable element of border control systems, these technologies lead to issues of fundamental rights and personal privacy, among others. This paper discusses various ethical, social and legal challenges arising due to the use of biometric technologies in border control. First, we identify a set of specific challenges and values affected and then provide generic considerations related to mitigation of these issues within a framework. The framework is expected to meet the emergent need for supplying interoperability among multiple information systems used for border control.

Keywords: Biometrics · Border Control · Ethical challenges · Legal challenges · Social challenges.

1 Introduction

Biometrics technologies [17,19] refer to automated methods of identification and verification of the identity of individuals based on their physiological or behavioral attributes. Examples of biometrics include fingerprints, facial features, iris scans, etc. They are used to support the border police on making decisions by providing automated identification, verification and cross-checking of individuals based on their biological and behavioral traits [5]. Identification is a process to associate a person with an identity (who are you?). Verification is a process to determine whether someone is who he/she claims to be (are you who you claim to be?). Cross-checking is a process of verifying information by using an alternative European Union (EU) information systems. Biometric technology is increasingly being used by countries worldwide and is a highly adopted technology at the EU borders [12, 31]. Its aim is to help achieving an automated,

rapid and highly secure border clearance process, such that increasing passenger throughput does not compromise border control reliability.

On the one hand, biometric technologies have been proven to be cost-effective in enhancing border security, detecting fraud and help to improve border crossing efficiency as well as facilitate an effective migration control and enforcement. On the other hand, biometric technologies can lead to some challenges and conflicts with fundamental human rights and can be a cause of ethical, social and legal challenges [11, 31]. The key challenge is related to individual rights, such as respect for personal privacy [36, 37], human dignity [15], bodily integrity [25], equity and personal liberty [30, 35]. Personal data protection is also an issue, especially when biometric information is stored in centralized databases [8, 28].

Another major concern with biometrics technologies is the seemingly immutable link between biometric traits and persistent personal information storage about individuals [9]. The tight link between personal records and biometrics can have both positive and negative consequences for individuals and the society overall. Recent research [10] on biometrics data shows that it can reveal personal information, such as gender, age, ethnicity and even critical health problems like diabetes, vision problems, Alzheimer's disease, etc. Such confidential information might be used for example to discriminate among individuals when it comes to border crossing enforcement.

People have the right to choose to what extent and how to engage with the systems and devices (e.g., biometric sensors and readers). For example, some people may refuse to having their photographs taken by a face recognition system due to the concerns about the purpose of the use of the images [9]. Moreover, others may refuse to or feel uncomfortable about undergoing iris scans or providing fingerprints due to permanent or temporary disability. For example, a study of biometric enrollment and verification in the United Kingdom showed that 0.62% of the sample group of people with disabilities were unable to enroll any of the three biometrics tested: fingerprints, facial scans, and iris scans [24]. Such concerns may impact people belonging to different groups with varying cultural beliefs, values and specific behaviors on how they interpret the requirements of being exposed to biometrics technologies. In general, a range of complex and interconnected issues must be addressed while deciding on the use of biometrics as a technology for border control [29]. Also, ethics guideline and a regulatory framework must be formulated for using biometrics technologies in border control in order to avoid any harmful may impact on the society while allowing for the continuous development of this technology to benefit the society [11].

In this paper, section 2 discusses the potential benefits of using biometrics in EU borders and the ethical theories around it. Section 3 investigates on the key ethical, social and legal challenges of using biometrics technologies and demonstrates vulnerabilities and risks related to these challenge categories, followed by a discussion of moral considerations with regards to human rights, right to privacy, right to data protection etc. Section 4 presents a discussion on ethical reasoning and decision making. Section 5 concludes the study.

2 Background

This section provides a background of benefits of biometrics in EU borders and a discussion on moral, ethics and ethical theories.

2.1 Potential benefits of using biometrics in EU borders

Freedom of movement is restricted by closed or controlled borders in order to protect other fundamental rights such as security or health, national or regional political, societal, cultural or economic interests of the political entities within that bordered area. The Schengen Border Code (SBC) (Regulation (EU) 2016/399) and its amendment (Regulation (EU) 2017/458) set out the rules governing the movement of people across EU's internal and external borders. The main aim of border checks is to ensure that the persons and goods crossing the border are entering or leaving the area with the permission (authorization) of the political entity of SBC. This permission for travel is currently manifesting in a travel document having a physical form as well as a record on the authorization in the national travel document database.

Identification and verification procedures at the border are to ensure that entry-to or exit-from a country will be granted to the right person. In recent years, Member States have seen an increased use of biometric identification and authentication systems at EU's borders including airports and land borders [2, 23]. More significantly, the large-scale EU information systems such as Visa Information System (VIS), Second-generation Schengen Information System (SIS II), European Asylum Dactyloscopy Database (EURODAC) and Entry Exit System (EES) etc. [21] employ biometrics for migration and border control and management. Such systems involve several highly complex processes, leading to a number of ethics and privacy challenges [11, 30]. The integration of biometric at border control provides benefits for travelers, political entities (states), authorities responsible for border control as well as individual border guards. The most important benefits include accuracy, integrity, robustness and efficiency.

- **Accuracy:** Accuracy of travelers identification and verification means the ability to recognize genies person and reject imposters person correctly [16]. During manual border checks, border guards seeks to gain knowledge about the subject (traveler) and associate it with his/her identity. For example, the border guard looks at the traveler, then to the picture on the travel document (on bio-data page) and determines if the person standing in front of him/her is the same which is pictured in the travel document. However, the accuracy of identification and verification depends on lighting, age of the picture, perception capabilities, tiredness, make-up etc. In addition, nowadays spreading culture of having aesthetic surgery poses a further challenge to manual identification. Moreover, a human border guard is usually very efficient shortly after the start of its shift, then diminishing appears as the officer gets tired. In this case, biometrics can enhance and support these practices.

A selective and differentiated application of multimodal biometrics identification results in a higher average accuracy during the whole shift as well as facilitates cross-checking of personal data with greater accuracy [16].

- **Integrity:** Integrity of the identification is the ability to confirm that the collected data and its components (e.g., passport picture and passport information) have not been altered from that created by the issuing State or organization [16]. Use of biometrics enhances reducing fraud identity (e.g., fake IDs and passports) impersonation as the identification and verification processes do not rely on the human agent. For example, with a relevant literature containing claims such as no system can be completely fraud- or error-proof [9], there is lack of evidence as to how biometric would help to reduce fraud and if the fraud is happening by the impersonators or the border gourds. To the best of our knowledge, a reduction in fraud means an increase in accuracy. Therefore, using biometrics eliminates a quite considerable integrity threat that the border guards face and benefits the authority responsible for border control.
- **Robustness:** Biometric systems are easy to operate, maintain, update, replace, redeploy or decommission compared to border control units/booths consisting of human agents only. Long years to achieve full competence and repetitive training is not required and experience is not lost with a single unit. From the traveler's view, utilizing multimodal biometrics allows the traveler to (theoretically) decide which biometric modality (e.g., fingerprints, face, iris) will be used for identification based on his/her preferences.
- **Efficiency:** The processing capacity of Automated Border Control (ABC) gates is sustained over time as ABCs don't get tired. Additionally, ABCs conduct an objective repeatable set of checks to complete identity and document verification can be more accurate and quicker to complete than similar checks conducted by humans [16]. This results in higher number of low-risk travelers throughput without losing accuracy or integrity and allows human resources to be focused on potentially higher-risk travelers.

As those benefits are all potential, the actual benefit highly depends on how biometric systems are integrated into the border management and how control systems help facilitate the correct identification and verification of persons and contribute to fighting identity fraud.

2.2 Moral, ethics and code of ethics

Morals are the general views, thoughts and convictions of people in making judgments about what is right or wrong. According to Kizza [22], morality is defined as "a set of rules (code) of conduct that governs human behavior in matters of right and wrong, good and bad." Ethics, on the other hand, concerns the way we can come to moral judgments of what is right and wrong for individuals and society. The ethical judgment of what is good or bad and right or wrong is often based on a set of shared rules, principles, and duties applicable to all in a group or society and this is called code of ethics. A code of ethics is a written set of

ethical principles and guidelines that govern decisions and behaviors in an organization (e.g., border management authorities) according to its primary values and ethical standards and theories [3, 6].

There are many ethical theories, each of which emphasizes different points, such as predicting an outcome and carrying out one's duties to others to reach an ethically correct decision. Consequentialism theory (result-based ethics) emphasizes the consequences of human actions, whether good or bad, right or wrong. Deontological ethics does not concern the consequences of an action but rather it considers the will and the motivation for undertaking an action [20, 22, 27]. It is sometimes described as duty-based or rule-based ethics. Even though the distinction between deontological and consequentialism is often clear, they are fundamentally different. They are both normative, and as a result, code of ethics are formulated as guidelines rather than prescriptions and prohibitions. The aim of the code of ethics is to provide a moral basis for emerging professional choices and provide adequate protection for all those who act in a statutory manner, and to recognize the unworthy practices associated with the police profession. Following are examples of the ethical principles for border guards which provide moral guidance during service shifts and out of service shifts.

1. **Respect of dignity and rights**: Respecting the rights of every person and avoid the use of torture, inhuman or degrading treatment.
2. **Fairness**: Treating of persons must be equal and having no preference, bias or prejudices based on race, background, ethnicity, gender, religion, personal and social status or property status etc.
3. **Duty of confidentiality**: Respecting for privacy and guaranteeing the security of the data and the information obtained.
4. **Responsibility**: Taking responsibility for actions and decisions in legal and moral terms. If misconduct takes place, take steps to ensure it is not repeated.

3 The "how to do it right" framework

In this section, we present a framework (Figure 1) which helps us to point out the types of challenges, the specific vulnerabilities and risks which the stated concerns/challenges lead to and the generic considerations for handling these challenges raising due to the use of biometric technologies. The focus on ethical, social and legal challenges and they constitute the topmost layer of the framework. The next layer of the framework is the values affected due to the presence or uprising of the challenges. The third layer from the top is the impact assessment layer. That is, what is the consequence of a value being affected? What vulnerabilities and risks arise correspondingly and what are the mitigation plans? Then, the bottom most layer lists the corresponding considerations that the border control police is expected to comply with. The framework provides a what to do and how to do it right guideline for border control police when various challenges are met by providing a link from the challenge, to the value(s) affected and an impact assessment on the values affected as well as pointing out

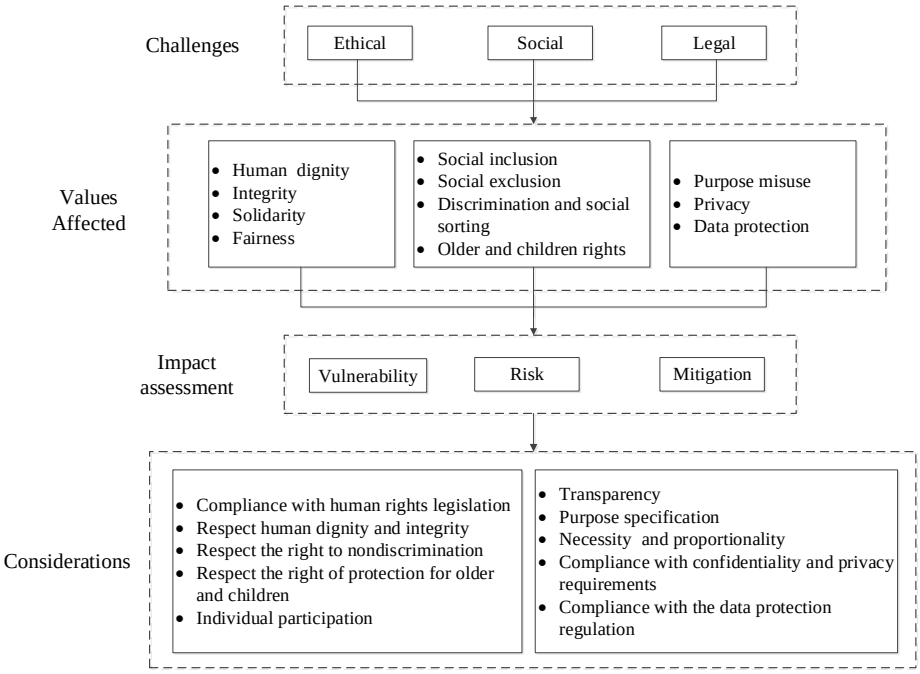

Fig. 1: The proposed framework for specifying biometric technologies related challenges and the considerations

the considerations that must be in place. Below, we provide examples of which values maybe affected under varying challenges and how.

3.1 Challenges level

Biometrics technology is acknowledged to potentially raise critical ethical, social and legal challenges. Ethical challenges is a situation that requires a person or organization to choose between alternatives that must be evaluated as right (ethical) or wrong (unethical). Social challenges are problems that engaging in normal social behaviors which may influence a large number of individuals within a society. Legal challenges refer to a formal questioning of the legality of an act and whether or not the act is being taken in accordance with the law.

Challenges layer provides information to help border officer or border authorities think through basic ethical, social and legal concepts and considerations. It will not provide specific answers for the specific challenges but will help bring to conscious awareness some understandings that help in thinking through these issues.

3.2 Values level and examples of how values are affected by ethics, social and legal challenges

Below, we give examples of how several values may be affected due to the arisen of such challenges.

(I) **Human dignity:** The capability to verify travelers' identities is extremely important and regards human dignity [15,22,30]. People may feel uncomfortable (or humiliated to some extent) when authorities like the border police are recording body features algorithmically. Many factors, for example physical work or physical incapacity (e.g., physical disabilities, sight impairment and mental health problems), can make it hard for some people to provide biometrics or they may simply be unwilling to do so. For instance, damaged fingers due to manual work can impact the way people are treated when providing fingerprint data [13]. In these cases, challenges with collecting biometrics data and remaining respectful of human dignity may emerge. People who cannot provide fingerprints or other biometrics data sometimes face a greater risk of negative consequences than people who can [24].
Biometrics data collection from vulnerable persons including those with disabilities requires particular attention. Human dignity is evidently a complex notion of the individual and biometrics data is strictly linked to the human body, whose integrity (physical and psychological) constitutes a key element of human dignity.

(II) **Social inclusion/exclusion and risk of discrimination:** The introduction of biometrics to improve identity verification at land borders raises serious objections to the potential to facilitate discriminatory social profiling [35]. For example, the biometrics enrollment of injured and disabled travelers could lead to higher false rejection rates than average. Moreover, senior citizens and children who have particular problems with using biometrics enrollment devices (e.g., fingerprint scanner, iris recognition reader) may face enrollment difficulties. Although discrimination of vulnerable individuals might be involuntary and unintentional, it may deeply affect them and impact the principle of equity. Furthermore, religious aspects (e.g., beard, headscarf) or interpersonal contact (e.g., photographs, touching, exposing parts of the body) may render a biometrics system an unacceptable intrusion. For example, those of faith who wear head or face coverings have difficulties with enrolling facial biometrics. Verification of such biometrics in public (e.g., at the border crossing points) may lead to embarrassment or offense, causing avoidance of situations where this is necessary. Therefore, mandatory encouraged use of such system may undermine religious authority and create de facto discrimination against certain groups whose members are not allowed to travel freely or obtain certain services without violating their religious beliefs and privacy. In positive terms, respecting a person's intrinsic worth requires recognizing that the person is always entitled to participate in social and community life regardless of age, beliefs, disability, health, etc.

(III) **Children rights:** Biometric technology also present several ethical questions regarding children's rights. These include the right to information, the

right to privacy, security and the right to no discrimination, etc. With respect to children and biometric technology, the main concern is that children will not fully know or understand the implications of the accessibility to, and subsequent use of the data collected. While children (and indeed their parents) may be aware of basic privacy settings and risks, even sophisticated users face great difficulties. Moreover, child identification introduces the requirement for greater levels of care. The problem is that there are several reasons why not all biometrics can be used for child identification and biometric recognition of toddlers. For example, a study by Basak et al. [4] found that "capturing fingerprints for children less than three years is hard due to very small fingerprint area, smooth skin, and thin fingers." Therefore, very young kids with small fingerprints might not be identified efficiently.
Furthermore, children are particularly entitled to effective privacy protection. This is because children cannot develop privacy expectations for reasonable legal protection. Moreover, biometric match accuracy diminishes as children grow. Fingerprinting young children affects the quality and reliability of future matches to the initial fingerprints [18]. The risk of a wrong match increases when the fingerprints or facial images are compared more than five years after the initial collection.

(IV) **Purpose misuse:** Function or purpose creep occurs when the biometrics 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 the European Dactyloscopy (EURODAC) fingerprint database. The original purpose of this EURODAC was to compare fingerprints for the effective application of the Dublin convention. It 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. Similar concerns may also arise in the case of other large-scale, centralized EU national and international databases, such as SIS II, VIS and EES. Biometrics 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.

(V) **Right to privacy and data protection:** Every individual has the right to privacy protection and personal data protection when his/her data is collected and shared. The use of biometrics technology as a border control tools introduces problems with maintaining individuals' privacy and protection of their personal data. Such a technology will probably increase the risk of available information misuse as a result of unethical and/or illegal practices if personal data are not protected adequately.
The main concerns include unnecessary and unauthorized collection of biometrics data for traveler identification and verification [8, 37]. GDPR [34], among other legislation, state that to best preserve an individual's privacy and right for data protection, the amount of personal data collected should always be kept to a minimum. Moreover, personal data like biometrics data should only be used when individuals or authorities will benefit from the

collection. Cameras, for instance, are now widely used to monitor our everyday life. People often benefit from such monitoring, especially at borders to control people flows and detect suspicious activities (e.g., illegal border crossing). However, extensive data collection and analysis can also lead to privacy violations.
Information linkage and compromise of anonymity is another concern [37]. Various kinds of information about individuals stored in a range of databases (e.g., SIS II and VIS) have the potential to become yet another means through which information can be linked to purposes ranging from commercial marketing to law enforcement. Recent research [10] explores the possibility of extracting supplementary information from primary biometric traits, face, fingerprints, hand geometry and the iris. Such information includes personal attributes like gender, age, ethnicity, hair color, height, weight and so on.
Despite all the benefits of using biometrics technology in border control, privacy concerns have become widespread because each time a person's biometric data is checked, a trace is left that could reveal personal and confidential information. Biometric data should essentially be well-protected against unnecessary and unauthorized collection, access and disclosure etc..

3.3 Impact assessment level

Table 1 summarizes values that may be affected and maps them to vulnerabilities, risks and possible mitigation measures in comparison to the current systems authorized in EU border control and other solutions already on the market.

Table 1: Values and the corresponding vulnerabilities, risks and mitigation measures.

Values	**Vulnerability**	**Risk**	**Potential mitigation measure**
Respect to human dignity	Current systems do not afford individual a choice of what biometrics data they prefer to enroll or use.	Violation of right to human dignity, cultural or religious customs etc.	Border control biometrics must provide information about what and why biometrics used as well as allow choice policies and procedures, unless choice is inapplicable.
Right to the person integrity	Current systems do not adapt or lack informed consent policies.	Violation of the right to integrity.	Border control biometrics must ensures a collection of free and informed consent form individuals according to rules laid down by regulations such as GDPR.

Right to person liberty	Current systems may lack of policy, procedures and ethical guidelines for data collection and processing or may allow unauthorized processing of individuals data; e.g., use of force to collect biometrics data.	Violation of the right to liberty of an individuals.	Border control biometrics must apply policy to restrict the procedures of data collection and processing, balancing between lawful interest and personal liberty.
Respect for private and family life	Current systems do not adapt an adequate family related consent and procedures.	Violation of right to respect for private and family life.	Border control biometrics must adopt appropriate measures for family consent and procedures.
Right of protection for children	Current systems does not address/deal with children vulnerability and special needs	Violation of the children rights which may lead to high levels of discrimination due to children lack of knowledge about the systems.	Border control biometrics must envisages adoption of devices and procedures to ensure children' needs. Also, the biometric data of children should be treated with enormous care and the procedures need to comply with data protection legislation such as GDPR [34]. Parents must always be notified when their children's biometric data is to be collected or used, and written consent must be obtained in advance.

Right to no discrimination	Current systems may be discriminated based on sex, race, ethnic or social origin, genetic features, religion or belief, political opinion, disability, age or sexual orientation etc.	Discrimination, social inclusion/exclusion and social sorting of individuals.	Border control biometrics must ensure nondiscrimination policy that comply with human rights legislation.
Right to no information tracking	Current systems lack of notices and information about tracking of individuals.	Violation of personal right and legitimate purpose requirements leading to surveillance of individuals and/or other members of the family.	If within the purpose and the law, surveillance should be authorized and consistent with EU and national laws.
Right to personal data protection	Current systems may allow personal data to fall into the wrong hands or/and shared across organizations.	Violation of right to security principles such as confidentiality, integrity, and availability.	Border control biometrics must ensure Security by Design to guarantee the ongoing confidentiality, integrity, availability and resilience of processing systems and services.
Right to privacy and confidentiality	Current systems may breach confidentiality, allowing unauthorized disclosure of personal information.	Violation of personal privacy.	Border control biometrics must ensures implementation of privacy-enhancing technologies to protect data in accordance with the law.

3.4 Considerations Level

This section presnets ethical, social and legal considerations.

1. **Ethical considerations for human rights:** According to Article 7, Regulation (EU) 2016/399 (amended in Regulation (EU) 2017/458), competent authorities should ensure that the human dignity and integrity of persons whose data are requested are respected and should not discriminate against persons on grounds of sex,religion, disability, age etc. Thus, biometric platform at border should be designed to support human right-compliant systems, related to technological, ethical and sociological aspects. For biometric

technologies to be successful with its use and actual implementation, they should not only consider the security and privacy of personal data, but it also need to guarantee that the users can interact with the systems and make the user experience acceptable. To do so, system designers and policy makers must consider all challenges, vulnerabilities and risks (Table 1) related to the system design. Moreover, border control biometrics platforms must pay particular attention to minors, whether traveling accompanied or unaccompanied and must respect the specific needs of children and their interests must be protected in ways supplementary to the general treatment of adult subjects.

2. **Considerations for travelers with physical or mental impairment:** As mentioned above, EU Regulation (EU) 2016/399 specifies equal rights for border crossing. Therefore, border control biometrics platforms should consider travelers with special needs/categories including individuals who physically or mentally impaired etc. An extra attention should be given to, among many others:
   (a) People with temporary injuries who might have difficulties to provide biometric sample due to temporary wound (e.g., injured face and/or broken arm/fingers) [24]. In this case, Border control biometrics platforms should not discriminate against such people and shall use biometric devices (e.g., fingerprints scanner) which perform acquisition in a greater number of situations.
   (b) People with total permanent disability whom have difficulties to freely move their limbs due to sensory damage and/or muscle damage. For example, in case of fingerprints verification, travelers with a hand disability may lack the ability to place the required finger and keep it steady for a sufficient time on the fingerprints scanner. Moreover, in case of face recognition/iris scanning, people with neck disabilities may have difficulties in correctly placing their face near the iris scanning device/face recognition camera. Thus, border control biometrics devices should be able to work in off-axis acquisitions and be adjustable to support such people with biometrics recognition and make it more comfort.
   (c) People with technological illiteracy, for example, elderly people and children who lack knowledge of using technology/tools (e.g., automated border control gates) would have a difficulty to use and interact with devices. In this case, border control biometrics devices should design an interface that taking into consideration elder's and kids' needs.
3. **Considerations for privacy and data protection:** As mentioned earlier, biometric data can be used to recognize individuals automatically with greater accuracy. On the other hand, a misuse of such biometric data can have dangerous consequences which pose several security and privacy challenges such data destruction and/or unauthorized disclosure of, or access to personal data, to name a few. Thus, border control biometrics platforms should be designed to support privacy-compliant biometric systems. Perceived risks are related to how people view the biometric technology, whether they trust it, and whether they like to use it. With respect to this, EU regu-

lation (e.g., GDPR [34]) prohibit the use of special categories personal data such as biometric data without the user's awareness and permission. Also, prohibit the use of the biometric data different from the purpose of the system (purpose misuse issue discussed in section 3.2). For example, biometric data stored in e-passports can only be used for issuing electronic documents and verification of document holder (Regulation (EC) 444/2009).
Border control biometrics platforms should consider several privacy aspects for protecting the privacy of personal data. These aspects include:

(a) The purpose of biometric data: The legitimate purpose of biometric data collection and processing used only for verifying the identity of the individual during the border crossing procedure. Article. 13 (1) of the GDPR stipulates that "information to be provided to data subject where personal data are collected from the data subject." This information shall include, purpose of the system, the enrolment and verification processes, and the methods used for data protection, among other.
(b) People control of their personal data: According to Article. 32 (2) of the GDPR [34], the data subject has the right to ask for removal or erasure of biometric data in electronic documents. Also, the data subject should have the possibility to decide when he/she no longer be authenticated and verified using the biometrics system and choice to proceed with manual checks (when applicable).
(c) Data protection measures: Article. 32 (2) of the GDPR stipulates that *"the controller and processor must implement appropriate technical and organizational measures to protect personal data against destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed and against all other unlawful forms of processing."* Therefore, border control biometrics system shall deploy a privacy enhancing technologies and secure access control techniques to avoid any misuse of personal data.
(d) Reuse of data for law-enforcement purposes: According to Regulation (EU) 2016/399 and its amendment Regulation (EU) 2017/458, citizens should be checked in criminal databases such as SIS II and SLTD on a systematic and non-systematic basis. As the majority of these travelers are presumably innocent individuals. Therefore, saving and cross checking their data on a systematic basis with law-enforcement databases would be disproportionate. Any reuse of personal data done for the purpose of law enforcement should be done in accordance with Directive (EU) 2016/680 [1], which aims to ensure more consistent and higher level of protection of the personal data of natural persons in the areas of criminal matters and public security.

4 Discussion on ethical reasoning and decision making

In view of the ethical theories (discussed in section 2.2) and the open dilemma of what is right and what is wrong, it is clear that the situation is similar, particularly surrounding the use of biometric technology. On the one hand, one group

of people (travelers, border officers etc.) may see biometrics technology used in border control as a liberator, believing in the power of technology to bring convenience (e.g., avoid queues) and efficiency (e.g., cut costs) and increase mobility (e.g., convenient border-crossing for citizens). This group may also welcome more powerful surveillance to improve border security (e.g., monitor migration, combat identity theft and fraud etc). We may agree with this group. First and foremost, the border control biometrics system used to improve security at the borders, however besides this main goal, it will maximize the benefits for the society (e.g., travelers) and minimize the human workload (e.g., border police officers) while improving security and detecting fraud (discussed in section 2.1). With respect to the consequentialism theory (discussed in section 2.2), every society member (travelers, border police officers etc.) benefit the same and it is not specific to any individual. Furthermore, the reason one individual must promote the overall good is the same reason why anyone else has to promote the good. Hence, it can be said that the ethics of the border control biometrics is related to consequentialism. The consequentialism theory places a group's interest and happiness above those of an individual for the good of many.

On the other hand, other groups of people may object and perceive biometrics technology as a threat to their personal life and privacy. Such groups might believe that surveillance technology is untrustworthy and destructive to liberty, dignity and privacy. For example, collecting biometric data such as iris scanning from veiled Muslim women [26] in stressful situations (e.g., inappropriate police behavior due to exhaustion or stress) may undermine the dignity of the women being scanned. An FRA report "Under watchful eyes: Biometrics, EU IT systems and fundamental rights" [14] showed that disproportionate force has been used when fingerprinting asylum seekers and migrants in irregular situations. Considering deontological ethics (duty-based or rule-based ethics discussed in section 2.2) and given the vulnerability of the people concerned as well as the obligation to use the least invasive means, it is difficult to justify the use of physical or psychological force solely to obtain biometrics for the purpose of identification and verification. When it comes to border control and border rules, ethical theories might change according to circumstance. Border officers have a duty to do the right thing (verify the identity of a traveler before entering/exiting the border etc.) even if it produces an undesirable outcome. In the case of veiled Muslim women or any other cases, it would be difficult to judge the action of an officer based on the outcome.

From the review, it could be concluded that ethics are not absolute, and clearly, views on biometrics technology vary according to the differing needs of people and institutions. However, different perceptions of biometrics technology reflect the diverse value judgments as influenced by many factors: age, gender, cultural beliefs, education, moral imagination etc. Remarks over the use of biometrics technology for large populations, especially if the consequences lead to social exclusion, either as a result of the individual being unable to reliably enroll or verify their data, or simply not having confidence in the system and avoiding having to interact with it. Certainly, when it comes to border control and

the use of biometrics technology to increase border security, monitor migration and combat identity theft and fraud etc., the argument is essentially utilitarian (consequentialism theory) where the collective right of a group (group interest) is balanced against the rights of the individual. It makes the individual simply a means to the ends of the majority. However, this could be a wrong argument. Wickins in [35] and Townend in [33] argue that public interest must be judged by considering the balance between individuals, i.e. the rights of single individuals must be balanced against other single individuals if individuals are not to be used instrumentally.

5 Conclusions

An important conclusion to this paper is that we are not attempting to provide an answer to what is ethical and what is not, or what is right and what is not. We see biometrics technology usage in border control with two sides. One side is the main intention and aim of biometrics technology to improve border control management and enhance people flow etc. The other side represents the risk of violating personal rights. As said, conflicts with decisions based on what to choose (e.g., privacy versus security, autonomy versus solidarity) make it difficult to have a broad and consistent position in favor of, or against expanding or restricting biometric technologies.

Individual acceptance of biometrics technology should be actively promoted through ensuring transparency of decision-making, clear policy regarding the purpose of biometric technology and how it is used, as well as increased measures dedicated to preserve personal rights and personal data protection. Since greater use of personal data impacts upon human rights, there needs to be an honest and assertive study of what the risks are to personal rights and privacy as well as how these risks are mitigated. Border control biometrics should comply with human rights legislation to encourage respect for fundamental rights in the implementation of biometrics technologies. Also, they should respect human dignity and protect personal integrity, preserve individual freedom and self-determination (i.e., choice and consent with respect to which biometrics data he/she prefers to use), respect privacy and family life, and safeguard against harm and unreasonable force for data processing. Moreover, border control biometrics should comply with security requirements and data protection legislation to ensure data confidentiality, integrity and availability when collecting and processing personal related data.

In the future, we shall investigate the use of ontologies for knowledge representation and enhancement of knowledge discovering using machine learning techniques. Ontologies provide a formal, explicit specification of a shared conceptualization of a domain that can be communicated between people and heterogeneous and widely spread application systems [32]. We aim to propose a semantic based framework for biometrics integration in border control systems relying on ontologies and machine learning techniques [7] to tackle ethical, social and legal challenges.

ACKNOWLEDGEMENTS

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

References

1. Directive (eu) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing council framework decision 2008/977/jh. Official Journal of the European Union (2016), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680&from=EN
2. Anand, A., Labati, R.D., Genovese, A., Munoz, E., Piuri, V., Scotti, F., Sforza, G.: Enhancing the performance of multimodal automated border control systems. In: 2016 International Conference of the Biometrics Special Interest Group (BIOSIG). pp. 1–5. IEEE (2016)
3. Banks, C.: Criminal justice ethics: Theory and practice. Sage Publications (2018)
4. Basak, P., De, S., Agarwal, M., Malhotra, A., Vatsa, M., Singh, R.: Multimodal biometric recognition for toddlers and pre-school children. In: 2017 IEEE International Joint Conference on Biometrics (IJCB). pp. 627–633. IEEE (2017)
5. Bhatia, R.: Biometrics and face recognition techniques. International Journal of Advanced Research in Computer Science and Software Engineering **3**(5) (2013)
6. Boddington, P.: Towards a code of ethics for artificial intelligence. Springer (2017)
7. Buitelaar, P., Cimiano, P., Magnini, B.: Ontology learning from text: methods, evaluation and applications, vol. 123. IOS press (2005)
8. Campisi, P.: Security and privacy in biometrics, vol. 24. Springer (2013)
9. Council, N.R., Committee, W.B., et al.: Biometric recognition: challenges and opportunities. National Academies Press (2010)
10. 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 (2015)
11. De Hert, P.: Biometrics and the challenge to human rights in europe. need for regulation and regulatory distinctions. In: Security and privacy in biometrics, pp. 369–413. Springer (2013)
12. Díaz, V.: Legal challenges of biometric immigration control systems. Mexican law review **7**(1), 3–30 (2014)
13. Drahansky, M., Dolezel, M., Urbanek, J., Brezinova, E., Kim, T.h.: Influence of skin diseases on fingerprint recognition. BioMed Research International **2012** (2012)
14. European Union Agency for Fundamental Rights: Under watchful eyes – biometrics, eu it-systems and fundamental rights (2018), https://fra.europa.eu/en/publication/2018/biometrics-rights-protection
15. Floridi, L.: On human dignity as a foundation for the right to privacy. Philosophy & Technology **29**(4), 307–312 (2016)
16. 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

17. Jain, A., Hong, L., Pankanti, S.: Biometric identification. Communications of the ACM **43**(2), 90–98 (2000)
18. Jain, A.K., Arora, S.S., Cao, K., Best-Rowden, L., Bhatnagar, A.: Fingerprint recognition of young children. IEEE Transactions on Information Forensics and Security **12**(7), 1501–1514 (2017)
19. Jain, A.K., Ross, A., Prabhakar, S., et al.: An introduction to biometric recognition. IEEE Transactions on circuits and systems for video technology **14**(1) (2004)
20. Kagan, S.: Normative ethics. Routledge (2018)
21. Kenk, V.S., Križaj, J., Štruc, V., Dobrišek, S.: Smart surveillance technologies in border control. European Journal of Law and Technology **4**(2) (2013)
22. Kizza, J.M., et al.: Ethical and social issues in the information age, vol. 999. Springer (2007)
23. Labati, R.D., Genovese, A., Muñoz, E., Piuri, V., Scotti, F., Sforza, G.: Biometric recognition in automated border control: a survey. ACM Computing Surveys (CSUR) **49**(2), 24 (2016)
24. Lee, T.: Biometrics and disability rights: legal compliance in biometric identification programs. Journal of Technology Law & Policy p. 209 (2016)
25. Van der Ploeg, I.: Genetics, biometrics and the informatization of the body. Annali-Istituto Superiore di Sanita **43**(1), 44 (2007)
26. Rahman, Z., Verhaert, P., Nyst, C.: Biometrics in the humanitarian sector (2018)
27. Ronzoni, M.: Teleology, deontology, and the priority of the right: on some unappreciated distinctions. Ethical theory and moral practice **13**(4), 453–472 (2010)
28. Sprokkereef, A.: Data protection and the use of biometric data in the eu. In: IFIP International Summer School on the Future of Identity in the Information Society. pp. 277–284. Springer (2007)
29. Sprokkereef, A., De Hert, P.: Ethical practice in the use of biometric identifiers within the eu. Law Science and Policy **3**(2), 177 (2007)
30. Sutrop, M.: Ethical issues in governing biometric technologies. In: International Conference on Ethics and Policy of Biometrics. pp. 102–114. Springer (2010)
31. Tanwar, S., Tyagi, S., Kumar, N., Obaidat, M.S.: Ethical, legal, and social implications of biometric technologies. In: Biometric-Based Physical and Cybersecurity Systems, pp. 535–569. Springer (2019)
32. Taye, M.M.: Understanding semantic web and ontologies: Theory and applications. Journal of Computing, **2**(6) (2010)
33. Townend, D.: Overriding data subjects' rights in the public interest. In: The Data Protection Directive and Medical Research Across Europe, pp. 89–102. Routledge (2017)
34. Voigt, P., Von dem Bussche, A.: The eu general data protection regulation (gdpr). A Practical Guide, 1st Ed., Cham: Springer International Publishing (2017)
35. Wickins, J.: The ethics of biometrics: the risk of social exclusion from the widespread use of electronic identification. Science and Engineering Ethics **13**(1), 45–54 (2007)
36. Yu, S.: Big privacy: Challenges and opportunities of privacy study in the age of big data. IEEE access **4**, 2751–2763 (2016)
37. Zeadally, S., Badra, M.: Privacy in a Digital, Networked World: Technologies, Implications and Solutions. Springer (2015)