Chapter 20
Promises, Social, and Ethical Challenges with Biometrics in Remote Identity Onboarding

Katrin Laas-Mikko, Tarmo Kalvet, Robert Derevski, and Marek Tiits

Abstract Issuance of identity documents has commonly relied on face-to-face customer onboarding. Checking a person's physical presence and appearance has been an essential part of identity enrolling procedures to avoid the risk of identity forgery. Yet, several weaknesses, including face morphing attacks, have been identified in document issuing processes. In the context of the COVID-19 pandemic, increasing international mobility, and a greater focus on user convenience, established onboarding rules and procedures have been disrupted. Solutions are being sought which would eliminate the barriers that stem from physical distance while offering at least equal or even better onboarding processes than in-person identity verification. Recently, novel remote onboarding solutions have appeared on the market. They vary from human-assisted video identification procedures to biometric-based automated verification procedures. The main social and ethical issues with biometrics in remote identity onboarding are (1) the risk of harming integrity of personal identity and misuse of it; (2) the risk of privacy invasion and function creep; (3) ethical issues that are raising from algorithmically driven actions and decisions; and (4) public perception and social acceptance of technology. These non-technical requirements need to be addressed in developing identity verification technologies based on biometrical algorithms and security techniques.

K. Laas-Mikko
SK ID Solutions AS, Pärnu mnt 141, Tallinn, Estonia
e-mail: katrin.laas-mikko@skidsolutions.eu

T. Kalvet (✉) · R. Derevski · M. Tiits
Institute of Baltic Studies, Lai 30, 51005 Tartu, Estonia
e-mail: tarmo@ibs.ee; tarmo.kalvet@taltech.ee

R. Derevski
e-mail: robert@ibs.ee

M. Tiits
e-mail: marek@ibs.ee; marek.tiits@taltech.ee

T. Kalvet · M. Tiits
Department of Business Administration, Tallinn University of Technology (TalTech), Ehitajate tee 5, 19086 Tallinn, Estonia

C. Rathgeb et al. (eds.), *Handbook of Digital Face Manipulation and Detection*,
Advances in Computer Vision and Pattern Recognition,
https://doi.org/10.1007/978-3-030-87664-7_20

20.1 Introduction

Information and the concept of the "digital society" is the driving force for change in the twenty-first century. Throughout this process, the advancement of technology is a fundamental part of it and serves as a catalyst to enable a wide spectrum of new and unique opportunities. Digitalisation is ubiquitous and takes a prominent role in our daily lives. It can even be described as a "post-digital world" where digital solutions are entirely bound up with our everyday lives and becomes inseparable [1]. In an unprecedented "fourth revolution" of automation and digitalisation, which includes the rise of such spheres as artificial intelligence (AI), virtual reality, the Internet of Things (IoT) or big data analytics [2, 3], things that seemed to be as something from science fiction just some decades ago (smartphones, internet or virtual reality) are normal and essential part of our daily life today [1].

The advancement of technology promises enormous changes in the future. For instance, in the field of communication "we are rapidly reaching a point where computational algorithms can create nearly any form of human communication that is, for all intents and purposes, indistinguishable from reality" [4]. Some scholars even go as far as to state that soon, hundreds of billions of devices might be communicating with the internet [3], which is many times more than the entire human population. Technology has also redefined what is considered possible and what the boundaries are between physical and digital. Let us take digital nomads, for instance, who embark on various forms of remoteness and use digital opportunities as a mediator between technology and infrastructure [1, 5]. This digital lifestyle demonstrates that it has never been easier to travel and work; where one could find themselves working from a laptop in a coffee shop today and from a co-working space in another country a week later [5].

With the increasing availability of different tools, forgery has also become massive and widespread. As Boneh et al. have argued "the barrier to entry for manipulating content has been lowering for centuries. Progress in machine learning is simply accelerating the process" [4]. With the development of digital technology, the ability to forge or manipulate data—including biometrics technology and its realism—develops as well. In fact, there are hundreds of different technologies and programmes available to forge or manipulate data. These can be spoofing attacks, adversarial attacks or digital manipulation attacks [6]. Similarly, the topics of digital security have become the cornerstone for further development of the information society. Identity theft has become a significant concern for individuals, organizations, and businesses and has directed all relevant stakeholders to work on secure digital identity solutions.

Until recently, government-issued identity documents, including strong electronic identity which serves as a means for authentication or electronic signature, have been exclusively issued as a part of a face-to-face customer onboarding process. Checking a person's physical presence has been an essential part of identity enrolling procedures to avoid the risk of identity forgery. Yet, several weaknesses, including face morphing attacks (digital image alterations), have been identified in document

issuing processes. With synthetic media and artificial intelligence generated, like 'deep fakes', it is becoming increasingly difficult to identify a true identity from a fake one. Various approaches are being applied to tackle this, including taking the identity document photo in the application office, i.e., live enrolment. Even this is a break with tradition for many countries and entails a sizeable overhaul in the public sector, which can be reluctant to change and often lacks the necessary formal methods that ensure a smooth transition. Behind the successful implementation of live enrolment is proper risk management: covering technological, political, and organizational risks, but also understanding cultural differences, potential ethical challenges and addressing them [7].

It has also been suggested that in improving identity management and identity documents, the focus should be primarily on breeder documents that generally lack standardised and security features and are generally considered to be a weak link in the government-issued identity documents chain. The introduction of biometric data to the breeder documents or introduction of centralized biometric identity databases would be technically feasible for establishing a stronger link between the birth certificate and the respective document holder. As another solution, it has also been suggested to issue identity cards instead of birth certificates to newborns immediately from birth. This can be implemented relatively quickly, avoiding the costs of development, international standardization and introduction of a completely new (breeder) document. Again, the collection and processing of biometric data are clearly subject to ethical and societal concerns, especially when the collection and use of infants' biometric data is concerned [8].

Furthermore, increasing international mobility, the COVID-19 pandemic, and a greater priority on user convenience poses a significant challenge to the established onboarding rules and procedures. This is especially true when it comes to issuing a national electronic identity or opening bank accounts internationally. A silver bullet is being sought—the remote customer onboarding and identity verification solutions—which would eliminate the barriers that stem from a physical distance while offering at least equal or better onboarding processes than face-to-face identity verification with the physical presence of a person.

In this chapter, we research the requirements of the different use-cases of remote identity verification solutions for identity onboarding, including the main risks and challenges from ethical, societal and privacy perspectives. We hypothesise that automated identity verification technologies based on biometric algorithms that ensure a person's presence and vital state, while also protecting one's identity through advanced security techniques, are key elements for a secure and reliable remote solution. However, next to developing technically superior solutions, there are also non-technical requirements to ensure the accuracy of the claimed identity presented during the identity onboarding process, such as the user's context-awareness of the person who is enrolled via the remote solution, the trustworthiness of identity provider, and the social and ethical issues.

After the current introductory section, the chapter will establish the need for remote identity verification based on the rapid spread of identity theft and people's expectations. In section three, the emergence of remote biometric identity verification

technologies is discussed, and use cases are introduced. These are then discussed from the perspectives of ethics, privacy and societal acceptability in section four. The chapter concludes with the discussion and conclusions.

20.2 Identity Theft and the Emerging Need for Remote Identity Verification

20.2.1 Risks and Societal Implications of Identity Theft

Obtaining someone else's personal information or identity document (ID), such as an identity card or passport, is where identity fraud begins, and it is becoming increasingly popular [9, 10]. With a stolen identity, the fraudster can effectively become someone else, allowing them to access the victim's financial or other accounts, access communications, set up new contracts, or present false information to the authorities. This is not only a violation of privacy but may bring about substantial financial and/or legal consequences to the victim. Evidence is also available on the associated major social and psychological impacts [9, 11].

In our earlier research [11, 12], it has been concluded that roughly 25–30% of the population of Austria, France, Germany, Italy, Spain, and United Kingdom have experienced some form of attempted or confirmed misuse of personal information over the period of 2013–2015. Only 10% of these cases were detected before personal information was actually taken. Thus, around 100 million citizens were forced to take extra steps to protect their identity during a 3-year period in the EU. Almost half of them had to do so more than once, as they experienced multiple incidents. As a result of the misuse of personal information, close to 40 million EU citizens have experienced significant personal consequences, such as debt collectors contacting them, problems with their family or friends, being denied a new service, having to face legal problems, etc.

The total value of the money, goods or services obtained by criminals from 2013 to 2015 was roughly 12–16 billion euros in the EU. This is, however, only the "consumer side". From the misuse of personal information, various institutional actors, e.g., financial or health insurance institutions, are likely to have incurred additional financial losses that are unknown to the individuals and, therefore, not reflected in this study [11, 12]. For instance, in the United States of America, Internal Revenue Service has estimated that it paid 4 billion euros in fraudulent identity theft refunds in filing season 2013, while preventing fraudulent refunds of 18 billion euros (based on what they could detect) [13]. It is within reason than to assume that, given the above example, the rough financial cost of identify in Europe reflects only the tip of the iceberg.

Other studies such as those commissioned and co-operated on by the United States Department of Justice and the Bureau of Justice Statistics [14, 15] have studied identity theft issues in recent years and confirm the scale and growth of the problem.

Javelin's 2020 Identity Fraud Study concludes that total identity fraud reached 15 billion euros in 2019 while criminals are targeting smaller numbers of victims and inflicting damage that is more complex to prevent or remediate. The research states that "the type of identity fraud has drastically changed from counterfeiting credit cards to the high-impact identity fraud of checking and savings account takeover. At a time when consumers are feeling financial stress from the global health and economic crisis, account takeover fraud and scams will increase" [16].

Eurobarometer survey on cyber security from 2020 [17] is also reflecting raising concerns: as compared to the study from 2017 [18], less Europeans feel they can protect themselves sufficiently against cybercrimes (59%, down from 71% in 2017). Three key concerns are related to falling victim to the bank card or online banking fraud (67%), the infection of devices with malicious software or identity theft (both 66%), and 6% of the respondents have actually experienced identity theft 2017–2019 [17].

20.2.2 The Need for Remote Biometric Identity Verification

Based on the increasing sophistication of attacks and the number of actual cases of identity theft, the need for strong electronic identity is especially clear in online services. The following three key arguments are developed: (1) on the importance of the strong electronic identity solutions, (2) on the importance and acceptance of the biometric solutions and (3) on the emerging need for remote identity onboarding methods.

First, earlier research has shown that the public has little trust in the security of popular Internet services, such as e-mail or Facebook [19]. Widespread misuse of Internet accounts, bank accounts and credit cards does not foster trust in these services. However, the personal experience with the attempted abuse or misuse of personal information does not lead to the decline of confidence in government issued identity documents. Confidence in government issued electronic identity cards and passports remains very high [20, 21] and is likely to be because the misuse of government issued identity documents remains infrequent in citizens' view as compared to other forms of identity fraud.

Government issued electronic identity solutions for online transactions are, thus, an obvious choice for bolstering security of Internet services and broadening the use of electronic authentication and signatures both in public and private applications. Furthermore, front-runner countries' experience in the widespread acceptance of electronic identity documents, such as Estonia, shows that mobile ID can serve as a convenient and secure alternative to more traditional electronic identity cards. In fact, the majority of the users of mobile ID seldom turn back to their electronic identity card when online authentication on Internet or electronic signature is required.

Furthermore, people who have experienced misuse of personal information are more likely to prefer identity documents that are more difficult to misuse, e.g., when lost or stolen. Victims of the misuse of personal information are also more likely to

accept modern forms of online authentication, such as electronic identity cards or mobile ID, including in combination with fingerprints or other biometrics.

Second, the importance and acceptance of biometric solutions have increased considerably, and such technologies should be preferred in identification solutions. The direct aim of biometric technology (which includes biometric identifiers like face and fingerprints) is to enhance the reliability of identification. Biometrics is a tool used to identify and reliably confirm an individual's identity based on physiological or behavioural characteristics (or a combination of both) that are unique to a specific human being. Since biometrics provides a close link between the physical person and identity credential, e.g., a government issued identity document, it is considered a strong form of identification technology [21].

Biometric identification can be applied and regarded as part of a more extensive security system for identity management in a restricted security environment or system (e.g., an eBank) to distinguish one person from another and decide whether the specific person has access rights to the environment. It can also be used within broader security systems to ensure legal access to a state or area, such as the Schengen area. Thus, the use of biometrics in border guard solutions can be used to identify illegal immigrants or people who have been blacklisted as international criminals or terrorists.

The use of biometrics has the potential to raise the effectiveness and trust level in transactions, procedures and systems where the verification or identification of a person is necessary. Use of biometric traits, for example fingerprints or faces, ensures with high probability that the person identified is the person he or she claims to be and thus can be reliably related to his or her rights, entitlements, actions and responsibilities. In other words, biometric "data" does not need to be remembered and kept somewhere in secret, as a human's biometric features cannot be forgotten or lost [22, 23]. This, in turn, can create more conventional and more reliable alternative to traditional authentication methods, such as passwords.

However, the reliability of identities and identity documents depends largely on the overall security of the issuing process, from the person's registration in the support system (e.g., information system managing identity issuance) to the overall organisation of the issuance. Every link in this trust chain must be secure. If it emerges, for example, that a passport (including its chip) is technically difficult to forge, criminals will look for more easily exploitable weak spots such as issuance process, corrupt officials or information system weaknesses in order to forge an identity.

Biometrics as a form of identity technology has many advantages over traditional means of identification like personal identification numbers (PIN), passwords or token-based approaches. It is difficult to forge or duplicate a person's biometric trait; as such, it can prevent identity theft or rule out the use of several identities by a single individual. Also, biometric identification is more convenient compared to other identification tools or methods, since biometrics is 'what you are'—and therefore always at hand [24]. But because of this connection there are also considerable risks related to the use of biometrics (see more in section three). Nevertheless, each

biometric characteristic (and the method used to capture it) has strengths and weaknesses regarding their universality, uniqueness, permanence, collectability, performance, acceptability and circumvention [24]. Therefore, often multi-modal biometrical systems are considered. For example, ePassports and some of the electronic identity cards combine face and fingerprints. Also, not every biometric approach is suitable for every implementation context. Some higher security processes would require authoritative identity source against enrolled biometrics to be verified (for example enrolled facial image against some register or reliable identity document). For some biometrics enrolment must take place in a controlled and secure environment using special equipment that is not available for normal user (enrolling fingerprints and sending to service provider, for example, or iris scan). Some biometrics is also under special legal protection, where its enrolment and use are legally restricted (fingerprints in some countries, for example).

Third, we would argue that there is clear need for remote identification methods for identity onboarding. Until recently, government issued electronic identity documents, but also electronic identity means or electronic signature certificates on the highest security level have been exclusively issued based on the physical face-to-face customer onboarding.

However, increasing international mobility and greater priority on user convenience, but also the COVID-19 pandemic, challenge the established onboarding rules and procedures. This is especially true when it comes to issuing electronic identity or opening bank accounts internationally. A silver bullet is being sought (the remote customer onboarding and identity verification solutions), which would eliminate the barriers that stem from physical distance, while offering at least equal or even better onboarding processes in comparison to face-to-face identity verification with physical presence of a person.

Novel remote onboarding processes have recently appeared on the market; they vary from human-assisted video identification procedures to biometric-based automated verification procedures. Earlier research has concluded that a considerable aspect in successful implementation of biometric technology is public trust and acceptability. Generally speaking, distrust among citizens regarding the technology, be it deployment difficulties, inconvenience, false acceptance rates or else, lowers the general trust in that technology among individuals but also state agencies deploying that technology [20, 21].

20.3 Remote Biometric Identity Onboarding Technologies

20.3.1 Emergence of Biometric Remote Identity Onboarding

There are several modalities for issuing identity documents in operation in Europe. In some of the countries, specialised passport offices of the national government provide identity documents to citizens. In other countries, regional or local governments

issue documents. At the more detailed organisational level, there is even more of a variability in enrolment approaches, e.g., whether the enrolment of document data takes place on the site of document issuing authority or remotely, live or not live, under different levels of supervision (attended, semi-attended, automated controlled or uncontrolled), with centralised or decentralised data storage, professional or non-professional acquisition of biometric data, by capturing a single modality or multiple biometric modalities in the same session, with a data processing system developed by the public administration or by a private company.

Traditionally, professional photographers have been put in charge of capturing the facial images, which were then handed as print-out or digital file to the issuer of identity documents. However, this approach is prone to unwanted morphing of facial images. Therefore, live or semi-live by an official or in an official photo-booth that is located in a controlled environment have become preferable. But, there is an increasing need to allow also for completely remote enrolment, including the capture of the facial image and the data from the previously issued identity document.

In 2020, European Union Agency for Cybersecurity (ENISA) conducted a research mapping down identity verification practices used in different European countries for identity onboarding. ENISA concluded that identity onboarding technologies could be divided into several categories: "onsite with the operator, video with the operator, remote automatic, electronic identification means, certificate based and combined" [25]. The first, second, and the final onboarding categories listed above require a real time presence by both the verifier and the applicant, which can be challenging to organise when performing identification procedures on a daily basis (i.e., banking). The remaining three methods—remote automatic, based on the electronic identification means and certificates—are representing solutions that can be used remotely and at the convenience of the person.

Traditional identity checking methods have their obvious shortcomings. Most notably, physical identity checks require that the person checking the identity and the applicant must be present at the same place. This is a requirement that can prove "complicated, time consuming, and given the recent pandemic crisis even dangerous for health-related reasons" [25]. Contrastingly, remote verification solutions like remote verification by AI based on facial biometrics (often labelled "selfie-id"), electronic authentication methods (fingerprint scanners on phones) or certificate-based solutions (electronic signatures) makes it easier to identify the person and prove their physical existence but without any requirement of physical presence at an official enrolment station.

Hence, the significance of remote identity proofing methods for identity onboarding is increasing, especially in cross-border applications in Europe and elsewhere. The ENISA study found that 23 of 30 trust service providers (TSP) surveyed already used remote identity proofing methods as a part of their services in 2020. The most widely used method (used by 11 TSPs) is the remote method with a verifying operator (typically based on synchronous audio–video call) while the second most popular option involves electronic identification means, incl. notified electronic identification schemes. Remote automatic processes based on AI processing of the applicant's picture (selfie) and a picture of ID is recorded for four TSPs. As such,

it demonstrates the wide interest of TSPs and companies in using remote proofing methods and the increasing interest towards this field. This is further illustrated by Fig. 20.1 where it could be seen that remote identity proofing is already allowed and practiced in extensive number of the EU member states. TSPs indicated to extend the number of remote identity proofing methods or introduce new ones; six TSPs plan to offer remote automatic identification based on AI [25].

What is currently missing is a unified approach and common regulatory framework in terms of remote identity verification. The absence of commonly accepted practices has resulted in a situation where different initiatives emerge across countries which share some common elements but also numerous differences that can lead to challenges related to the disjointed nature of remote identification policies. As such, even though the remote identity verification technologies are becoming more popular, the importance of cross-country recognition and legislation together with technical know-how and uniformity in methods and practices across the countries might help to strengthen and advance the development of a synchronized and secure

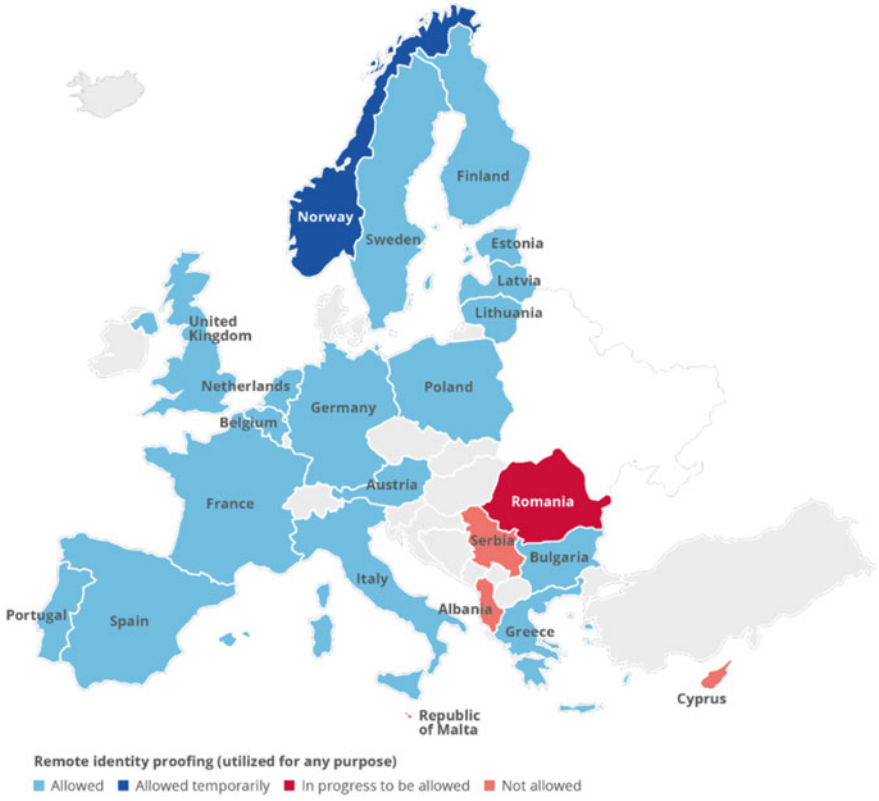

Fig. 20.1 Geographical map of the remote identity proofing practice for any (regulated) purpose [25]

remote identity verification solutions. Key to solving some of these challenges lies not just on public and private sector cooperation, but also on interoperability between governments issued electronic identity systems and private sector electronic identities [26].

Financial sector is generally considered as frontrunner in digital transformation and in the development of electronic services. For example, banks have been historically identified as the 'informal' leaders of the Estonian software industry and have generated overall trust towards ICT due to their successful implementation of internet banking services [27, 28]. Financial sector is also currently one of the prominent fields where cross-border identification solutions are being sought, as the need for having bank accounts in many countries and onboarding international clients in the twenty-first century is growing. A few years ago, financial institutions started to onboard new customers remotely in non-face-to-face processes. This takes place both on the domestic level as well as across the national borders using commercial identity verification solutions. The mobile payment apps, such as Wise, Revolut or Monzo, exemplify a hot arena for remote customer onboarding that builds on (live) facial images and on the government issued identity documents. The biometric identify verification technologies acquired by the financial institutions to help them verify the identity of their customers *en masse* and with a higher accuracy than a human operator could offer. But of course, the challenges that the banks face are broader than just identity checks and include such aspects as credit referencing, address verification, employment checks, income verification etc. Thus, the need for cross-border solutions for remote identity verification solutions makes financial sector one of the main domains where novel technological solutions are pioneered (like using blockchain, decentralised identity networks, "trusted events", non-standard identity sources, etc.) [26].

ETSI, the European standardisation organisation, has ongoing activities regarding standardizing identity proofing for the trust services (issuing e-signature and e-seal certificates). ETSI has prepared new standard for policy and security requirements for trust service components providing identity proofing of trust service objects [29]. There is the expectation that this standard would be of use not only for trust services but also for other means of electronic identity (which are usually issued by state authorities) and for the financial sector, especially for anti-money laundering (AML) and know your customer (KYC) processes. This calls for synchronising identity proofing area more widely, including physical identity verification and remote identification.

Typically, remote identification solutions rely on biometric verification, unless a new identity is based on an already issued electronic identity that can be verified during the onboarding either by the means of on-line authentication or qualified electronic signature. Biometric verification that takes place during the remote enrolment process assumes the existence of an authoritative source that a newly issued (secondary) identity could be based on. In the absence of such possibility, a more thorough process would be required for the identification of the person (analogue of refugee identification process for example), while risk of creating a new double identity cannot be completely avoided.

The almost only biometric characteristic that can be viably used for remote identification is the facial image. It is a universal and accessible means that allows for enrolment of identity in an environment that is not strictly controlled; it is compatible with accessible primary authoritative sources (e.g., travel documents, databases) and is a mature technology with presentation attack detection mechanisms.

Other biometric data, such as fingerprints or eye iris image, are not suitable for enrolment to create the new identity for a person in uncontrolled remote environment, as there is no suitable reference data available from authoritative sources, the access to such sources is restricted by the law or undesirable from ethics and privacy points of view. Thence, other biometric characteristics beyond face images are only usable in multimodal applications, e.g., fingerprints can replace a PIN code as a part of access control.

Last but not the least, putting the biometrics based remote identification solutions into use assumes the existence of high-level presentation attack detection methods and a security system that is in regular re-assessment and improvement in terms of the detection of new attack-vectors and mitigation of emerging risks. In other words, on-going enhancement of the face morphing and other presentation attack detection methods is absolutely crucial.

20.3.2 Biometric Remote Identity Onboarding Technologies

Based on two above-mentioned studies [25, 26], the main methods regarding remote biometric identity verification technologies for identity onboarding could be approached as follows:

First, **human assisted video identity verification** is, for the time being, perhaps the most popular onboarding method. The method is similar to face-to-face onboarding, except that the presence of applicant is not physical, but the communication takes place through a secure audio and video communication channel. In this process, a human operator carries out the person's identity verification in a similar way compared to the physical process, i.e., checks if the national identity document is authentic and valid, reads/copies data from this document, and compares visually, if the facial image from identity document against the face of the applicant. The operator plays the central role and makes decision about verification match and whether to issue a new identity to the applicant.

The main weakness of this method is that operator alone may not be able to detect document forgeries, image, or video forgeries, etc. without the assistance of a specialised software, as advanced presentation attacks are impossible to detect with a "bare human eye". Also, this case physical MRTD-s are used, forged documents detection is easier and document integrity controls are more advanced with eMRTD-s. This can potentially be software assisted where a software is used for checking the authenticity of the document and for verifying whether the person who visible in a live video session is a high-probability match with the facial image in document. In

this way, extra steps can be taken to ensure that the video session is not manipulated and attacked.

The second method for identity verification is **automated remote identity verification solutions** that base their decisions solely on machine-learning systems. The process is conducted and guided by a dedicated software application that carries out automated steps of data collection and comparison without operator's intervention. Usually, the onboarding starts with reading/capturing identity document of applicant, i.e., picture or video of identity document. Thereafter, facial verification takes place by taking a short video of the applicant and comparing the live facial image in a video against the portrait photo in the identity document. On the back end, this includes security checks against a presentation attack by checking liveness of person, etc.

When the validation and security checks are satisfied, an automatic system decides whether to issue a new identity or to cancel the issuance. An automatic system does not mean that there could not be monitoring and alerting system, where if there is suspicious activity or uncertain events the human operator can intervene and decide what to do. Here, the biometrical verification system and supporting presentation attack detection systems play a crucial role as they must ensure that this particular person is the same person as he or she presents. Also, the identity document and its authenticity are very important as it is usually the only trustworthy and widely recognised source against which the identity of the applicant can be compared. But for automated purposes, not every identity document is suitable and sufficiently secure, only documents that comply to ICAO 9303 standard for biometrically enabled Machine-Readable Travel Document (eMRTD) meet such expectations. Usually, eMRTD includes facial image, fingerprint (optionally) and/or iris images and also provides data authenticity and integrity controls (PKI based passive and active authentication).

The weakness of this method lies primarily in whether the solution can be manipulated by attackers (phishing). Therefore, the applicant's awareness is crucial—whether she or he understands the context of transaction and purpose for which his/her data are collected and used. Security measures shall be implemented in such a way that the presentation attack or phishing adversary could not easily assume the context of the transaction and the purpose for which the applicant's data would be used.

Third, **combined video identity verification**. Identity verification tasks are carried out mainly by machine learning systems based on biometrical verification (in development for France and Spain eID-s). Combined method is defined as mixing video session, where the main verification functions are carried out by AI and machine learning systems and assisted by a human operator who interacts where necessary or to make a final decision to issue an identity. The human operator can understand and can check the person's motivation and awareness for this procedure. This method addresses weaknesses from the previous alternatives and is suitable in the context where other measures are not appropriate.

The main objective of combined methods is to bind the applicant's biometric data with the biometric data contained in government-issued identity document (as a trustworthy source) and make sure that the claimed identity and captured live

biometric data match with different security measures. Here, "liveness" of the person participating in the onboarding process and his/her awareness of identity verification context (for which purposes identity verification is carried out) are as important as in previous methods.

The remote identity onboarding solutions require electronic identity solutions that can be handed over remotely (for example mobile phone application and server or cloud-based solutions) or physical carrier of electronic identity can be delivered in secure way so that only rightful person can receive and activate the identity token. For reading eMRTD-s, NFC reader enabled mobile phones are needed. Thus, it means that availability of these kind of remote solutions are limited with certain technical capabilities and enabling technologies.

Remote identity onboarding use-cases where the newly created identity will be used for further transactions and where physical presence of applicant is usually needed are (1) banks issuing authentication means for online banking customers or providing access to e-merchants customers using electronic wallet; (2) public authorities or identity providers for issuing e-identity means (for authentication) in public or private services; and (3) trust service providers for issuing e-signature certificates and/or devices. Use cases for single electronic transactions that need in-person or remote onboarding verification include the opening a bank account (AML and KYC requirements) and signing agreements which would normally require the physical presence of a person.

Today there are professional remote identity onboarding providers which offer video interviews, identity document check (both physical and digital), enrolment of biometric characteristics and biometric verification (with presentation attack measures) services. The largest providers are offering tailor-made customer solutions and/or service packages, concentrating on a specific service, like biometrics enrolment and verification or digital identity document check which will be integrated and orchestrated together within some remote identity verification service solution.

Also, mixed use-cases exist where trust service providers perform remote identity verification and linked to a specific bank customer. The main similarity for these different solutions is the biometric characteristics that are used, like facial biometrics and the recognition task itself. This type of solution is 1:1—meaning one-to-one biometrical verification; matching a biometric sample (video-selfie) with biometric reference data from a trusted source like a digital identity document (eMRTD) to prove a person's claim about his or her identity.

20.4 Ethics, Privacy and Societal Acceptability of Biometric Identity

20.4.1 Risks and Main Ethical Issues

In order to weigh values, assessing and identifying relevant risks (to values) and benefits of technology, defining the context is important [30, 31]. According to [30] and [32], technology can be viewed on different levels of abstraction: as a high-level socio-technical system (for example, technologies like biometrics, cloud computing, affective computing), as an artefact (hardware or smaller scale technical items, for example RFID chip) or at the level of applications of technology. The latter includes the use of technologies (and artefacts) for particular purposes and in specific settings/technical configurations (for example ePassport, specific solutions as for example smart (automated) CCTV for the identification of abnormal behaviour or specific kind of remote identity onboarding solutions). A particular high-level technology or artefact can raise different risks and ethical issues depending on the context and its application [30].

As we have seen from the use-cases above, the main functionality of remote identification solutions is to onboard the new identity for issuing e-identification/authentication means or e-signature devices for transactions to access certain systems (bank systems, specific e-service environments) and e-services or to perform single e-transactions. Identity verification of a person is based on face biometrics or theoretically may be based on other biometrical characteristics such as fingerprints or iris biometrics.

Biometrical characteristics are used mainly either for the purpose of establishing a subject's identity ("who is the person") or for verification/authentication ("is this the person who he claims to be?") in various information systems, but sometimes also to monitor abnormal activities and intentions using behavioural biometrical characteristics to profile a person [33].

Thus, there are two main ways of biometric comparison. The first is biometric *verification,* a one-to-one process in which the face of the authenticator/user is compared to the existing model. The second one is *identification*, which is a one-to-many process of comparing the authenticator's data to many existing samples in the database and seeking for the match [22]. The latter is more complex procedure as it involves not just authenticating the user, but also verifying the identity of the user. In both cases, biometric interaction starts from *enrolment* process when the initial biometric sample is constructed. This serves as a biometric template which is then stored in the database and is taken as a basis for *matching*, which takes place when the user scans biometric data in the future for recognition. This results in a *matching score* which is produced to reflect the level of similarity between the sample and the biometrics of authenticator [22].

So far, remote identity onboarding solutions have focused mainly on linking a person's data to his or her claimed identity. Thus, the aim is to make sure whether a person is who she or he claims to be by comparing biometrical data *one-to-one.*

This biometric recognition task and its possible privacy impact or consequences are less invasive than in the case of co-called *one-to-many* identification where person is searched from the crowd, databases or checklist and from the systems that use behavioural biometrics to monitor, detect, or profile a person based on some traits or behaviour pattern which may expose malicious intentions or dangerous activities (carrying explosives, etc.). Thus, different kinds of biometrical recognition tasks must be distinguished, since they entail different kind of security and privacy risks, and ethical considerations.

The main risk groups that are related to remote identity onboarding solutions are (1) falsified evidence, where the applicant applies for a false identity by using a forged document, or a manipulated video or photo, etc.; (2) identity theft, where applicant uses genuine evidence, which belongs actually to a different person; (3) phishing, where the attacker tries to get private or sensitive information with social engineering skills and pretends to be a trusted source/party to ultimately take over the identity of another person. The first two first risks groups are also addressed by European Telecommunications Standards Institute [29].

These risk groups/risks can have many risk sources including, technical system vulnerabilities or presentation attack detection system weaknesses, weak identity evidence with poor quality, to malicious social engineering, insider with malintent, brute force attacks, etc. Additionally, risks such as data leaks, data loss, or data integrity problems may cause consequences like identity misuse because of exposed identity data, and a user's rejection or discrimination etc. Also, unbalanced biometric dataset for biometric verification or identification testing, poor image quality etc. can increase the risk of a user´s rejection, discrimination, or accusations depending on the use-case. Possible consequences are discussed in the next sub-chapters about ethical values.

Regarding biometric identity verification for identity onboarding, the severity of consequences or harm are dependent on the use-case, including where and for which purposes biometric onboarding or use is implemented. If the use-case of onboarding is related to the single transaction—for example to sign some legal contract—then the practical consequence is limited with financial damage and privacy breach. However, if identity onboarding is for issuing certificates for authentication or electronic signature, then it would cause far-reaching identity damage, privacy breach, financial consequences or other problems for the person and critical reputational damage for the service provider.

Based on these above-mentioned risks and possible harms, the main ethical and social issues that will be raised in remote onboarding solutions case are (1) harming integrity of personal identity and misuse of it; (2) privacy and function creep; (3) ethical issues that are raising from algorithmically driven actions and decisions; and (4) public acceptance of technology.

20.4.2 Integrity of Practical Identity

Biometrics includes an individual biometric feature in the form of a physiological or anatomical attribute or distinctive behaviour that reflects "What I am" [29]. Biometrical information is representing and defining the person—his/her "informatized" body [34], or embodied identity. When we link personal information as name and some other kind of identifiers to the biomedical or "embodied" information—the practical identity of a person is created. This practical identity is included into identity systems and identity data processing activities.

When we talk about the risks for identity manipulation, the integrity the person's practical identity is in danger because through this practical identity and identity verification he/she is not proving his/her identity claim only but also or his/her rights, entitlements, ownership, and benefits. In case of remote identity onboarding solutions, new electronic identity will be issued based on biometrical verification. Your identity and corresponding data brings new entitlements, benefits, and/or rights, i.e., access to e-services and social benefits. The central component of the practical identity concept is the idea of an autonomous or self-determining person who is held accountable for his/hers reasons, motives, and actions. "If someone else engages in manipulation of a person's identity, that person is not fully able to use his own rights and entitlements; in the worst case, someone else will do this in their stead" [33]. As discussed above, identity theft can be severely damaging to a person, creating financial, legal, social, and psychological problems.

Biometric data are irreversible—they cannot be revoked because biometric traits are unique. If such data is copied and forged or confused, the data owner will have great difficulty proving that he or she is unconnected to the instances of use of the data or that identity is not created by themselves. At the same time, in the remote identity onboarding process context, the main objective of biometric verification is again to mitigate risks of identity loss and identity theft so that no one can pass him- or her-self off as someone else and thereby make use of the rights, entitlements and benefits belonging to another individual.

Therefore, regarding remote identity onboarding solutions, the security and integrity measures play a crucial role for detecting identity forgery or theft, or other vulnerabilities that might compromise the identity and the trust of those kind of identity systems. That presumes from the service provider a mature risk and a security management system.

20.4.3 Privacy and Function Creep

The recent studies have shown that the loss or violation of privacy as a result of potential data leaks and data disclosure, identity theft, misuse of personal data, and other risks remain the main ethical and social concerns in terms of using biometrics.

There are several privacy definitions; thus, it is important to define how it is used in the context of this chapter. Here, the privacy normative conception is used and can be described as limited to the 'sphere' surrounding the person, within which that person has the right to control access to himself or herself. Privacy is further defined as "the person's right to decide to what extent other persons can access and use information concerning him or her, and who those persons are who have access to his or her physical body; those who access and use physical/intimate space surrounding the person" [35].

Privacy is mostly regarded as instrumental value because it protects other values or interests of a person. The most favoured theoretical argument is that privacy protects a more fundamental value that of individual autonomy [36–38]. The modern concept of privacy implies respect for the autonomy of a person. In the field of scientific research, this is connected with the moral and legal claim for informed consent before intervention in other people's lives and the person's right to the self-identification that forms the core of a person's autonomy [33]. Also, [39] and [40] discuss privacy, individual value of autonomy and value of privacy in social construction of relationships and interaction. Steeves and Regan suggest that "/…/ privacy is an inherently social practice that enables social actors to navigate the boundary between self/other and between being closed/open to social interaction" [39].

How does this definition of privacy fit into the identity onboarding solution and biometrical data processing context? Mainly it means that biometrical data must be collected and used with a person's clear and informed consent, and this consent is basically autonomous act of a person to authorize data processing in the scope and on aims presented to the person. Thus, it means that presenting the transaction context to the person and clearly stating the conditions of data processing are crucial. Data processed without consent generally occurs when the party obtaining data forgets to ask for consent, and data are disclosed because of data leakage, hacker re-used some vulnerability to get personal data or even gains access to the person's data through hacking. These examples constitute a form of privacy loss as the person did not authorized the data processing activity. Also, as privacy is the instrumental value—the breach of privacy usually results in consequences from inconvenience of leaked biometrical images, until serious practical identity loss—where someone else is using your identity, accessing, and stealing your property, savings etc.

There is one special kind of privacy breach—namely "function creep". In short, function creep is the situation where someone's personal data (including biometric data) is used by the government or another data-processing body beyond the scope for which it was initially intended and informed to the person [20, 21]. It is important to understand that what this situation entails is not just the violation of privacy by the authorities but also their abuse of rights and exercising more power than they were granted. This can have social repercussions meaning that it could not be guaranteed that the databases of biometrics possessed by the state or service provider will be used solely for identity verification purposes as initially intended. For instance, the lack of transparency in processing biometric data means that the state or service provider could use it for covert mass-surveillance and identification of suspects [20, 21],

profiling and etc. This sort of privacy loss is related with value of self-determination and right to not be discriminated.

Privacy is not an absolute value but one that varies between individuals and cultures especially when it comes into contact with other values. In practice people routinely face trade-offs and balancing acts such as privacy vs. security (e.g., at airports) or convenience like regarding remote identity onboarding solutions. According to [41] privacy is a complex decision problem—subjective perceptions of threats and potential damages, psychological needs, and actual personal returns all play a role in affecting decisions to protect or to share personal information. However, Acquisti and Grossklags refer to problems in privacy valuation: incomplete and asymmetric information about privacy-related contexts, risks and outcomes of trade-offs and inconsistent decisions (due to uncertainty and limited knowledge about future events, people's behaviour, emotional judgements etc.), which may result in a dichotomy between attitudes and actual behaviour [41]. Also, people may not really have alternative choices for using technologies, services, etc. which may jeopardize their privacy (but not necessarily) [20].

Remote identity onboarding solutions are generally designed to soften the consequences of a crisis (as COVID-19) or to offer connivance services instead of processes where a person might have to travel hundreds of kilometres to get the desired or needed electronic identity token. At the same time, providers of identity boarding solutions recognize that there is a need for identity security monitoring to compare biometrical data not only 1:1 for creating a new identity but also matching identity with already known adversaries etc. Also, as we saw above, remote identity onboarding solutions are vulnerable to attacks against enrolment and verification of biometrical data or presented evidence, thus a system of presentation attack detection security control must be built up. To ensure transparency and trustworthiness of data processing, the context awareness checks and informed consent must be at the core of privacy policies. To this end, data protection laws and information security best practices must be followed.

20.4.4 Ethical Issues Raising from Algorithmically Driven Actions and Decisions

Kloppenburg and Van der Ploeg, prominent scholars in the surveillance studies and biometrics have conceptualised the nature of biometrics in terms of bodily differences and automated discrimination. They point out normative assumptions of biometric recognition that everybody has unique bodily characteristics and at the same time people in essence are similar, thus the human bodily features are defined into the range of different human features. The "normalized" bodily features are defined and built into algorithms, systems or equipment. Bodily differences and automated discrimination appear in multiple ways as for example with demographic distributions in a training set for tuning algorithms, quality of images, setting thresholds for

false negatives and positives etc. [42]. Hidalgo also points out that "interestingly, the use of learning and training sets, as well as the obscurity of deep learning, makes algorithms similar to humans by providing them with a form of culturally encoded and hard-to-explain intuition" [43].

Indeed, a large-scale performance test about demographic effects was made by the National Institute of Standards and Technology (NIST) in 2019 [44]. The overall conclusion was that there is empirical evidence for the existence of demographic differentials in most evaluated face recognition algorithms. But different algorithms perform differently, the most equitable also rank among the most accurate. Regarding identity verification (1:1), the main findings in this report suggest that for false positives, using higher quality photos rates are highest in the case of West and East African and East Asian people, and lowest in Eastern European individuals. With smaller impact, they found false positives to be higher in women than in men, also elevated in elderly and in children. For explanation that false positives may present security concerns, as this means that people with the wrong identity may pass identity verification. At the same time regarding 1:N, this would mean that for false positives, the person may be placed on some kind of "list"; which could lead to false accusations or a banned travel status. High quality false negatives are higher among Asian and American Indians, but African and Caribbean people, especially older people, false negatives triggered by lower quality border crossing images are higher. For those impacted by false negatives, this would mean wrongful rejection at border crossings and more inconvenience. Although the goal of the study was not to explore the causes and effects, it was noted that testing algorithms from different regions it seems to refer to the need for demographically more diverse training data [44].

As mentioned previously, in the case of remote identity onboarding solution biometrical recognition task 1:1 biometrical verification is used. For the person who is rejected as a false negative, it may bring some inconveniences, as he or she will be not allowed to get digital identity from distance and must go to the physical customer service point if alternative onboarding services are not available. Certainly, it does not foster digital inclusion in the e-society. Tolerance ranges are not usually open and obvious, which makes societal scrutiny also difficult [45].

False positives also play a crucial role in remote identity onboarding solutions. Weak algorithms or racial and sex biased solutions can accidentally associate a person with the wrong identity and issue a new identity. This then leads back to the integrity of a person's practical identity and how it can be misused.

Another issue concerns the automatic machine-learning and AI based decisions about human proceedings and actions. What are the contexts and situations where purely machine judgments are adequate in rational and moral sense and in which context should the human operator assist? Of course, biometrical recognition systems are very limited in their functions and decision power, there are moral implications embedded into algorithms and automated decisions (as discrimination), but it is hard to see the moral agent behind it. An interesting study was conducted 2018 by NIST researchers compared the performance of automated identification software to human participants who were identifying people using biometric verification and highly challenging image pairs. The conclusion was that the best face recognition

algorithms worked in the range of the best humans: professional forensic facial examiners. However, optimal face identification was achieved only when humans and machines worked in collaboration [46].

Nevertheless, there is question how to control the quality of automated decisions in operation and who carries the responsibility if automated decisions has serious consequences, such as false identity or identity misuse.

20.4.5 Public Acceptance of Technology

One of the possible barriers for introducing new technologies is the risk that they will not be accepted by the users. To our knowledge there are no studies specifically on the acceptance of biometrics in remote identity onboarding available. However, one can learn from other studies undertaken on related biometric technologies.

Large scale biometrical systems were introduced in Europe with implementing the so-called ePassports. And, already since their introduction of ePassports, scholars have concluded that insufficient public information on the objectives of the utilisation of ePassports and eIDs and their rapid adoption without public discussion can escalate public fears and create a trust deficit.

Our own studies confirm an absence of public information regarding the functions of ePassports and biometric impacts of their implementation. In particular, many people seem to lack information regarding the role of biometrics, ePassports and their functioning. In other words, how are ePassports meant to make our life easier and in what ways are they more effective than traditional identification methods? How are they meant to increase our security? The unclear reasoning behind implementation of new solutions has a negative impact on their acceptability and may raise questions about their relevance [20]. An important aspect in successful implementation of biometric technology is public trust and acceptability. Generally speaking, distrust among citizens regarding the technology, be it deployment difficulties, inconvenience, false acceptance rates or else, lowers the general trust in that particular technology among individuals but also state agencies deploying that technology [20, 21].

Tiits et al. have also analysed public perceptions on a number of potential future uses of ePassports and related data. It is found that the majority of the general public also agrees with public entities using passport photos for identity checks. The public is, however, less willing to accept the government making use of fingerprints and even less so other biometric applications in making identity checks. The majority of respondents are, in fact, against the use of fingerprints or eye iris images in the case of low security services that do not require strong authentication of a person. The acceptability of private businesses making use of biometrics for identity checks follows largely the above pattern, even though acceptance levels are lower than for public authorities [20, 21]. However, since the study was published, the use of biometrics has become wider in consumer level devices and we expect the wider approval of facial images by the public, as has happened with the fingerprint images.

The study concluded with several recommendations which are valid for increasing the acceptance of the biometrics in remote identity onboarding. It was concluded that the number of people who are uninformed or undecided about various aspects of ePassports and their use, remains high. The expected benefits and risks of ePassports have received only limited attention in the public media sphere in most of the countries and more public debate is needed. However, increasing awareness on the technical aspects of ePassports will not necessarily lead to higher acceptance among the future generations of ePassports. What the public expects is that the benefits of specific uses of ePassports are clear, and, most importantly, proper technological and organisational measures are in place to secure that privacy is maintained and that the use of personal data is limited only to the purposes originally stated. It was also confirmed that the acceptability of technology is context-dependent and a function of a trade-off between expected benefits and perceived risks (costs). This is where earlier experience becomes crucial. The research shows that if people accept the use of advanced biometrics, such as fingerprints or eye iris images in one scenario, they are more willing to accept them in others. Thus, the successful pathway to greater acceptability for the use of advanced biometrics in ePassports should start from the introduction of perceivably high-benefit and low-risk applications [20, 21].

20.5 Discussion and Conclusions

Until recently, government-issued identity documents, including strong electronic identity, which serves as a means for authentication or electronic signature, have been exclusively based on face-to-face customer onboarding. Checking a person's physical presence has been an essential part of identity enrolling procedures to avoid the risk of identity forgery. Yet, several weaknesses, including face morphing attacks, have been identified in document issuing processes. With synthetic media and artificial intelligence generated 'deep fakes', it is becoming increasingly difficult to tell apart a true identity from a fake one. So, with the increasing availability of data manipulation tools, forgery has also become massive and widespread. Hence, identity theft has become a growing concern for individuals, organisations, and businesses and has directed all the stakeholders to work on secure digital identity solutions. Thereby, the establishment of a trustworthy (electronic) identity, the fight against identity theft and privacy protection have become the cornerstones for further development of the society.

Furthermore, increasing international mobility, the COVID-19 pandemic, and greater priority on user convenience poses a significant challenge to the established onboarding rules and procedures. This is especially true when it comes to issuing a national electronic identity or opening bank accounts internationally. A solution is being sought—the remote customer onboarding and identity verification solutions—which would eliminate the barriers that stem from a physical distance while offering at least equal or better onboarding processes than face-to-face identity verification with the physical presence of a person.

Biometrics is only reliable link for binding together identity evidence and the real person that can be presented through a video-session. Face biometrics is used and seems to be a suitable biometric option from different perspectives. The use of such biometrics has the potential to raise the effectiveness and trust level in transactions, procedures, and systems where the verification or identification of a person is necessary. Also, biometric identification is considered more convenient compared to other identification tools or methods. Recently, novel remote onboarding solutions have appeared on the market; they vary from human-assisted video identification procedures to biometric-based automated verification procedures. The almost only biometric characteristic that can be viably used for remote identification is the facial image. It is a universal and accessible means that allows for enrolment of identity in an environment that is not strictly controlled; it is compatible with accessible primary authoritative sources (e.g., travel documents, databases) and mature technology with presentation attack detection mechanisms exists. However, putting the biometrics based remote identification solutions into use assumes the existence of high-level presentation attack detection methods and a security system that is regularly assessed and improved in terms of the detection of new attack-vectors and mitigation of emerging risks. In other words, on-going enhancement of the face morphing and other presentation attack detection methods is absolutely crucial.

We have analysed different use-cases of remote identity verification solutions for identity onboarding, main risks, and challenges from ethical, societal and privacy perspectives. Automated identity verification technologies based on biometrical algorithms and security techniques to ensure a person's genuine presence and aliveness identifying presentation, deepfake replay, and other similar attacks are key elements for a secure and reliable remote solution. In addition, other non-technical requirements for the reliability of the claimed identity presented during the identity onboarding process—user's context-awareness while the person is enrolled via remote solution, the trustworthiness of identity provider, etc.—must be not underestimated and shall be addressed as well.

Regarding biometrical identity verification for identity onboarding severity of consequences or harm is dependent on the use-case, where and for which purposes biometric onboarding or use is implemented. If the use-case of onboarding is related to the single transaction, then the practical consequence is limited with financial damage and privacy breach. However, if identity onboarding is for issuing certificates for authentication or electronic signature, then it would cause far-reaching identity damage, privacy breach, potential financial harm, and other problems for a person and critical reputational damage for the service provider.

The main social and ethical issues with biometrics in remote identity onboarding are (1) the risk of harming integrity of personal identity and misuse of it; (2) the risk of privacy invasion and function creep; (3) ethical issues that are raising from algorithmically driven actions and decisions; and (4) public perception and social acceptance of technology. In the case of integrity of person's identity, during the identity theft or loss more than privacy will be harmed, the person could be refused access to services, lose control over their identity, and face damages which are done in their name.

Regarding privacy and function creep, the main issues are related to remote onboarding solutions where a person's data are used without his or her authorisation. In these cases, how the data is leaked—whether it be from a data leak or unsecure service, hackers (adversaries), or vulnerable data systems—is not as important as what the consequences were. For example, differences in consequences and harm i.e., financial harm or adverse consequences manifesting from the takeover of a person's identity. In case of remote systems using biometric recognition, it may be temptation to perform one-to-many matching for profiling, blacklisting etc., which could go beyond the data processing purposes authorized by and communicated to the persons.

Algorithmical decisions and actions refer to situations where a person who is rejected as a false negative may suffer from an inconvenience at the very least. As an example, he or she may be refused from remote onboarding for new digital identity and may be referred to go to the physical customer service point where an alternative face-to-face onboarding service is available. Likewise, false positives are a crucial risk factor in remote identity onboarding solutions. Overly loose algorithms or racially or gender biased solutions may associate a person erroneously to a wrong identity or assign a new identity to the wrong person altogether.

Finally, it is important to understand and address the potential public acceptance issues. The end goal to be to support activities that increase the awareness of the benefits and risks for using technologies and methodologies for biometric identification. This is particularly important regarding the benefits of specific uses of biometrics in remote identity onboarding and ensuring to the would-be users that the proper technological and organisational measures are in place to secure that privacy is maintained and that the use of personal data is limited only to the purposes originally stated.

These non-technical concerns and risks need to be addressed in developing identity verification technologies based on biometrical algorithms and security techniques. At the same time, introduction of such innovative solutions puts challenges to public administrations.

The absence of a unified approach, common regulatory framework and commonly accepted practices has resulted in a situation where different initiatives emerge across countries which share some common elements but also numerous differences that can lead to challenges related to interoperability. It is recommended to share between the EU member states (and beyond) the technical know-how, but also how social and ethical risks have been managed.

Acknowledgements This research was funded by the European Commission, grant number 883356—Image Manipulation Attack Resolving Solutions (iMARS).

References

1. Dufva T, Dufva M (2019) Grasping the future of the digital society. Futures 107:17–28
2. Tsekeris C (2018) Industry 4.0 and the digitalisation of society: curse or cure? Homo Virtual 1(1)4–12
3. Helbing D (2015) The automation of society is next: how to survive the digital revolution. Create space independent publishing platform
4. Boneh D, Grotto AJ, McDaniel P, Papernot N (2019) How relevant is the turing test in the age of sophisbots? IEEE Secur Priv 17(6):64–71
5. Nash C, Jarrahi M, Sutherland W, Phillips G (2018) Digital nomads beyond the buzzword: defining digital nomadic work and use of digital technologies. Lect Note Comput Sci Conf 2018:1–10
6. Dang H, Liu F, Stehouwer J, Liu X, Jain AK (2020) On the detection of digital face manipulation. In: 2020 IEEE/CVF conference on computer vision and pattern recognition (CVPR), pp 5780–5789
7. Kalvet T, Karlzén H, Hunstad A (2018) Live enrollment for identity documents in europe: the cases of Sweden, Norway, Kosovo, and Estonia. J Democr Open Gov 10(2):53−73. https://doi.org/10.29379/jedem.v10i2.517
8. Kalvet T, Tiits M, Laas-Mikko K (2019) Public acceptance of advanced identity documents. In: Ojo A, Kankanhalli A, Soares D (eds) Proceedings of the 11th international conference on theory and practice of electronic governance. Galway, Ireland, pp 429−432. https://doi.org/10.1145/3209415.3209456
9. Akdemir N (2021) Coping with identity theft and fear of identity theft in the digital age. In: López Rodríguez AM, Green MD, Kubica ML (eds) Legal challenges in the new digital age. Leiden, Koninklijke Brill NV, pp 176–197
10. Reyns BW (2018) Identity-related crimes. In: Reichel R, Randa R (eds) Transnational crime and global security. Praeger Security International, 161–179
11. Kalvet T, Tiits M, Ubakivi-Hadachi P (2019) Risks and societal implications of identity theft. In: Chugunov A, Misnikov Y, Roshchin E, Trutnev D (eds) Electronic governance and open society: challenges in Eurasia: 5th international conference, EGOSE 2018. St. Petersburg, Russia, Revised Selected Papers. Springer, 14–16 Nov 2018
12. Tiits M, Ubakivi-Hadachi P (2016) Societal risks deriving from identity theft. EKSISTENZ D9.2. Tartu: Institute of Baltic Studies
13. U.S. Government Accountability Office (2014) Identity theft: additional actions could help IRS combat the large, evolving threat of refund fraud. Report to congressional requesters, GAO, 14–633. https://www.gao.gov/assets/670/665368.pdf
14. Harrell E (2015) Victims of identity theft, 2014. Bureau of justice statistics. https://www.bjs.gov/content/pub/pdf/vit14.pdf
15. Oudekerk B, Langton L, Warnken H, Greathouse SM, Lim N, Taylor B, Welch V (2018) Building a national data collection on victim service providers: a pilot test. Bureau of justice statistics. https://www.ncjrs.gov/pdffiles1/bjs/grants/251524.pdf
16. Javelin (2020) Identity fraud study: genesis of the identity fraud crisis. https://www.javelinstrategy.com/coverage-area/2020-identity-fraud-study-genesis-identity-fraud-crisis
17. Kantar (2020) Europeans' attitudes towards cyber security. Special Eurobarometer 499. https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/survey/getsurveydetail/instruments/special/surveyky/2249#p=1&instruments=special&yearFrom=1974&yearTo=2017&surveyKy=2249
18. TNS Opinion & Social (2017) Europeans' attitudes towards cyber security. Special Eurobarometer 464a. https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/Survey/getSurveyDetail/instruments/special/yearFrom/1974/yearTo/2017/surveyKy/2171
19. Tiits M, Ubakivi-Hadachi P (2015) Common use patterns of identity documents. EKSISTENZ D9.1. Institute of Baltic Studies, Tartu
20. Tiits M, Kalvet T, Laas-Mikko K (2014) Analysis of the epassport readiness in the EU. FIDELITY deliverable 2.2. Institute of Baltic Studies, Tartu

21. Tiits M, Kalvet T, Laas-Mikko K (2014) Social acceptance of epassports. In: Brömme A, Busch C (eds) Proceedings of the 13th international conference of the biometric special interest group. IEEE Darmstadt
22. Buciu I, Gacsadi A (2016) Biometrics systems and technologies: a survey. Int J Comput Commun Control 11(3):315–330
23. Liljander A (2019) Attitudes towards biometric authentication technologies between cultures: acceptance in Finland and Brazil. Information systems, master's thesis, University of Jyväskylä
24. Jain AK, Bolle R, Pankanti S (1996) Biometrics. Personal identification in networked society. Boston, MA, Springer
25. European Union Agency for Cybersecurity (2021) Remote id proofing. Analysis of methods to carry out identity proofing remotely. https://www.enisa.europa.eu/publications/enisa-report-remote-id-proofing
26. European Commission (2019). Report on existing remote on-boarding solutions in the banking sector: Assessment of risks and associated mitigating controls, including interoperability of the remote solutions, Brussels: directorate-general for financial stability. Financial Services and Capital Markets Union. https://europa.eu/!rj88wv
27. Kalvet T (2012) Innovation: a factor explaining e-government success in Estonia. Electron Gov 9(2):142−157
28. Kalvet T, Aaviksoo A (2008) The development of eservices in an enlarged EU: egovernment and ehealth in Estonia. Office for Official Publications of the European Communities. Luxembourg
29. European Telecommunications Standards Institute (2020). Electronic signatures and infrastructures (ESI); policy and security requirements for trust service components providing identity proofing of trust service subjects. Draft ETSI TS 119 461 V0.0.5 (2020–12). https://docbox.etsi.org/esi/Open/Latest_Drafts/Draft%20ETSI-TS-119-461-v0.0.5.pdf
30. Stahl BC, Heersmink R, Goujon P, Flick C, Hoven van den J, Wakunuma KJ, Ikonen V, Rader M (2010) Identifying the ethics of emerging information and communication technologies: an essay on issues, concepts and method. Int J Tech 1(4)
31. Nissenbaum H (2010) Privacy in context. Technology, policy, and the integrity of social life. Stanford University Press, Stanford, California
32. Brey PAE (2012) Anticipating ethical issues in emerging IT. Eth Inf Tech 14(4)
33. Sutrop M, Laas-Mikko K (2012) From identity verification to behaviour prediction: ethical implications of second-generation biometrics. Rev Policy Res 29(1)
34. Ploeg I (2003) Biometrics, and the body as information: normative issues of the socio-technical coding of the body. In: Lyon D (ed) Surveillance as social sorting: privacy, risk, and digital discrimination. Routledge, London, New York
35. Laas-Mikko K, Sutrop M (2016) How Do violations of privacy and moral authonomy threaten the basis of our democracy? In: Delgado A (ed) Technoscience and citizenship: ethics and governance in the digital society. Springer, Cham, Switzerland
36. Gavison R (1980) Privacy and the limits of law. Yale Law J 89
37. Kupfer J (1987) Privacy, autonomy, and self-concept. Am Philos Q 24
38. Rössler B (2005) The value of privacy. Polity Press, Cambridge
39. Steeves V, Regan P (2014) Young people online and the social value of privacy. J Inf Commun Eth Soc 12(5)
40. Rössler B, Mokrosinska D (2013) Privacy and social interaction. Philos Soc Crit 39(8)
41. Acquisti A, Grossklags J (2007) What can behavioral economics teach us about privacy? In: Acquisti A, Gritzalis S, Di Vimercati S, Lambrinoudakis C (eds) Digital privacy: theory, technologies, and practices. Auerbach Publications
42. Kloppenburg S, Van der Ploeg I (2018) Securing identities: biometric technologies and the enactment of human bodily differences. Sci Cult 29(2)
43. Hidalgo C (2021) How humans judge machines. MIT Press, Cambridge
44. Grother P, Ngan M, Hanaoka K (2019) Face recognition vendor test (FRVT). Part 3: demographic effects. https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf
45. Lyon D (2008) Biometrics, identification and surveillance. Bioethics 22(9)

46. Phillips PJ, Yates AN, Hu Y, Hahn CA, Noyes E, Jackson K, Cavazos JG, Jeckeln G, Ranjan R, Sankaranarayanan S, Chen JC, Castillo CD, Chellappa R, White D, O'Toole A (2018) Face recognition accuracy of forensic examiners, superrecognizers, and face recognition algorithms. PNAS 115 (24)