FIDELITY

Analysis of the ePassport readiness in the EU

CONTRACT NO	FIDELITY SEC-284862
DUE DATE OF DELIVERABLE	
SUBMISSION DATE	20 June 2014
ABSTRACT	This paper analyses the public readiness and perceptions for the adoption of the next generation ePassports in five EU member states - Estonia, France, Germany, Sweden, United Kingdom -, and in the United States of America
AUTHOR, COMPANY	Marek Tiits, Institute of Baltic Studies (IBS)
CONFIDENTIALITY LEVEL	PU
FILING CODE	FIDELITY_IBS_D2.2_Analysis-of-the-ePassport-readiness-in-the-EU_R1.0.doc
RELATED ITEMS	

DOCUMENT HISTORY

Release	Date	Reason of Change	Status	Distribution
1.0	20/06/2014	Final	Final	PU

Please refer to this publication as follows:

Marek Tiits, Tarmo Kalvet, Katrin Laas-Mikko. 2014. *Analysis of the ePassport readiness in the EU. FIDELITY Deliverable 2.2*. Tartu: Institute of Baltic Studies.

Marek Tiits is chairman of the board of the Institute of Baltic Studies.

Tarmo Kalvet is senior research fellow at the Ragnar Nurkse School of Innovation and Governance of Tallinn University of Technology and senior research fellow at the Institute of Baltic Studies.

Katrin Laas-Mikko is research fellow of the Institute of Baltic Studies, and quality manager of AS Sertifitseerimiskeskus.

The authors thank Maren Behrensen, Elin Palm, Joosep Raudsik, Anti Saar, Kadri Simm and the members of FIDELITY consortium for their assistance and advice during this study.

Table of Contents

Tables of Figures and Tables

Table of Figures

Table of Tables

1. Glossary

Abbreviation / acronym	Description
ABC gates	automated border control gates
eID	electronic identity card for online and offline identification
ePassport	combined paper and electronic passport issued by the government that contains biometric information
PIN	personal identification number, which is often used in connection to electronic identify cards, credit cards or similar
RFID	radio-frequency identification
UTAUT	unified theory of acceptance and use of technology

2. Executive Summary

The FIDELITY project finds broad social acceptance of the potential solutions to be built into next generation ePassports absolutely crucial. Therefore, in this report, the societal readiness and acceptance of specific technology options in relation to the potential next generation of ePassports is carefully considered. In doing so, the existing theoretical and empirical literature on the need for ePassports including its perceived benefits and risks were reviewed. This includes the need for ePassports, public trust and social acceptability of ePassports, ethical considerations in relation to privacy, social injustice and discrimination, and public perception on ePassports. Furthermore, this current study also analysed social acceptance of specific technology options for the establishment of identity, identity checks by public and private service providers and identity checks by domestic and foreign border control authorities.

As a part of the current study, an on-line survey of regular citizens was carried out between February – March 2014 in Estonia, France, Germany, Sweden, the United Kingdom and the United States of America. These countries represent a selection of Europe's larger and smaller nations, plus the USA for broader comparison. More than 400 complete questionnaires were collected from each of the above countries.

Based upon the responses, we find that the public believe's that it is not well informed about the personal data that government or private companies collect on them. They have only limited knowledge of the electronic data and functions ePassports include, and often have no clear opinion on various potential uses for ePassports and related personal data. We find, quite as expected, that younger persons judge themselves to be more knowledgeable about the data ePassports include and the government collects personally on them. While this is the case, people with relatively higher levels of education and those holding higher level (management) jobs consider themselves less informed.

There appears to be public consensus on the expectations from ePassports, which includes improvements in protection from document forgery, accuracy and reliability of the identification of persons and protection from identity theft. Broader public policy objectives, such as the fight against terrorism, human trafficking or illegal immigration are in the view of the public significantly less important in the context of the adoption and use of ePassports. Notably, those people who claim to have more detailed knowledge about ePassports also have higher expectations on the benefits of ePassports.

The risks that the public associates – rightfully or not – with novel identity documents reduces the acceptability of ePassports. The main risks the public associates with ePassports include the possible use of personal information for purposes other than those initially stated, and covert surveillance. The concerns regarding these two potential risks are high no matter what the level of knowledge on ePassports is. Compared to earlier studies, our research shows that issues of possible privacy invasion and abuse of information are much more perceived by the public.

The public favours the use of personal identity codes over fingerprints, eye iris images or DNA data in the establishment of the identity of newborns. It also finds it generally acceptable for the government to keep data on national identity documents in one national registry, which includes also the respective persons' photos and personal identity codes. Support for the inclusion of fingerprint data in such databases is slightly lower, while the acceptability of the inclusion of eye iris images and DNA data in such a registry is significantly lower. There is however, a strong opposition to the border control potentially making use of photos or other information travellers have themselves made publicly available on the Internet.

There appears to be a weak correlation between a persons' level of knowledge about ePassports and their willingness to accept the use of advanced biometrics, such as fingerprints or eye iris images, in different identity management and identity checking scenarios. Furthermore, the public becomes more undecided about ePassport applications as we move from the basic state of the art towards more advanced biometric technologies in various scenarios. This is where earlier experience becomes crucial. The current 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 as well. Thus, the successful pathway to greater acceptability of the use of advanced biometrics in ePassports should start from the introduction of perceivably high-benefit and low-risk applications.

As the public awareness is low, citizens' belief in government benevolence, i.e. the belief that the government acts in citizens' best interest, comes out as an important factor in the overall context. Furthermore, people who are informed about ePassports and the data they include, often believe that the government acts in citizens' best interest when introducing and using new identity documents, such as

ePassports or electronic ID cards. There is, thereby, a strong democratic argument for informing the public properly even if this will not always lead to greater acceptance of certain specific technologies or their applications.

So far, 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 current technical aspects of ePassports will not lead necessarily to higher acceptance for 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 ensure that privacy is maintained and that the use of personal data is limited only to the purposes originally stated.

3. Introduction

Broad societal acceptance is crucial if the deployment of new forms of technology, such as ePassports, is to be successful. The failed attempt to introduce the National Identity Register and electronic ID cards in the United Kingdom is a clear example of this. In 2013 the United Kingdom was forced to abolish the National Identity Register and cancel electronic ID cards launched two years earlier due to strong societal protests. The opposition foremost pointed out the overall high costs of the new ID card system, limited resources foreseen for ID cards security, and the risk of function creep (i.e. personal data could be used by data-processing bodies beyond the intended scope) (LSE, 2010).

It is therefore important to take potential social concerns into account in the earliest phases of the development and adoption of the next generation of ePassports. This is why FIDELITY is carefully considering the societal readiness and acceptance of specific technology options in relation to the next generation of ePassports.

The general point of departure in the analysis of technology acceptance is that there are a number of factors that influence the user as to whether or not to adopt the technology. The Unified Theory of Acceptance and Use of Technology (UTAUT), which we will rely on in this analysis, is currently perhaps the most widely used technology acceptance model. The UTAUT model covers various dimensions that influence technology acceptance, such as how the technology contributes to achieving one's goal(s), its ease of use, the influence of various stakeholders and the overall context.

In order to adopt the above UTAUT model for the analysis of ePassports, the existing theoretical and empirical literature on the need for ePassports including its perceived benefits and risks were reviewed. A limited number of interviews were also carried out with policy makers and experts in charge of adoption of ePassports. Building on this research, a questionnaire was developed and an on-line survey of inhabitants was carried out in Estonia, France, Germany, Sweden, the United Kingdom and the United States of America. More than 400 complete questionnaires were collected from each of the above countries.

This is a forward-looking study, therefore public perceptions on a number of potential future uses of ePassports were also analysed. Following the practice of foresight and technology assessment studies, a number of statements that described potential ways for the establishment of identity, identity checks by public and private service providers and identity checks by domestic and foreign border control authorities were presented, and the respondents were asked about the acceptability of such uses of ePassports and related technology.

In the following chapter, we synthesise the literature on social aspects of ePassports. This includes the need for ePassports, public trust and social acceptability of ePassports, ethical considerations in relation to privacy, social injustice and discrimination, and public perception on ePassports. Thereafter, we detail in chapter six our own research framework for analysing ePassport readiness in selected countries. The analysis of the results of the field work is presented from chapter seven onwards.

4. Literature on societal issues regarding ePassports

4.1 The need for ePassports

The direct aim of biometric technology and ePassports (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 on the basis of physiological or behavioural characteristics[1] (or a combination of both) that are unique to a specific human being (Future of Identity in the Information Society [FIDIS], 2009). Since biometrics provides a tight link between the physical person and virtual person/identity credential (e.g. an identity document such as an ePassport), it is considered a strong form of identification technology.

Biometrics as a form of identity technology has many advantages over traditional means of identification such as personal identification numbers (PIN), a 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, it is more convenient compared to other identification tools or methods, since biometrics is 'what you are' – and therefore always at hand (Jain et al 1996). But because of this connection there are also considerable risks related to the use of biometrics (see more in the following sections). 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 (Jain et al 1996). Therefore often multi-modal biometrical systems are considered (for example ePassport combines face and fingerprints).

Reliable identification of persons is an integral and crucial part of the infrastructure for diverse sectors such as government services, border control, IT security, finance and banking. 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 (Jain et al 2004). 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. Biometric identification can be applied and regarded as part of a larger 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 such as on national borders to ensure legal access to a state or area (such as Schengen). Thus the use of biometrics in border guard solutions can be used to identify illegal immigrants, people who have been blacklisted as international criminals or terrorists (see more Future of Identity in the Information Society [FIDIS], 2009).

The reliability of identities and identity documents depends largely on the security of the issuing process, from the person's registration through the support systems (information systems managing identity issuance) to organisation. 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 e.g. breeder documents, corrupt officials or information system weaknesses in order to forge an identity.

4.2 Public trust and social acceptability of ePassports

Trust is important for the adoption of new forms of technology. Public disappointment regarding the efficiency of technology such as inconvenience on borders because of false acceptance rates, device deployment difficulties etc. (Perakslis and Wolk, 2006) can erode trust in technology as well as in those adopting such technology (i.e. state agencies). A loss of trust and negative experiences may also strengthen fears about a 'surveillance state', even if these fears are unsubstantiated.

Trust, of course, is a complex phenomenon in this context. Societal acceptability of new technology does not wholly depend on the technology itself but also on the general *level of trust in government* and state agencies. The level of trust and willingness to accept propositions from a government could be a barrier or a boon for an innovation like ePassports (Ng-Kruelle et al., 2006). Acceptability also depends on the general level of perceived security in the state (ibid). Yet even proponents of the minimal state (see for

[1] E.g., facial images, fingerprints, eye iris, hand geometry, hand vein, retinal scan, DNA, gait.

example Nozick 1992) recognise that one of the state's most important functions is to maintain security and public order. The reliable identification of citizens and inhabitants is an increasingly important aspect of secure and stable states.

Trust in technology more generally is another aspect that is likely to affect the adoption of ePassports. Here cultural differences can play a significant role. For example, national debates regarding the acceptance or rejection of national ID cards or electronic voting demonstrate the vastly dissimilar perceptions and attitudes that populations have regarding the trustworthiness and usefulness of different forms of technology.

The 9/11 terrorist attacks significantly accelerated the RTD and the actual deployment of ePassports and related technology in the USA, Europe and around the world. The implementation of ePassports was seen by economic and political elites as a measure that would enhance security and public order at the national and international levels by providing reliable identification (Lodge, 2010). Below we discuss two major societal concerns regarding ePassports that pertain to the public trust aspect of these debates.

The first concern relates to insufficient public information about the **role of biometrics and ePassports** (European Biometrics Forum, 2006, Institute for Prospective Technological Studies, 2005). Namely, it is unclear how relevant ePassports are in raising overall (inter)national security against terrorists. How are biometric passports meant to enhance security? What is the expected outcome? The unclear role of and expectations for biometrics raise questions about the relevance of ePassports for security purposes and about the proportionality of biometric measures in managing risks. Risks can be overestimated – terrorism is a relatively low-probability risk, but with potentially dramatic consequences, and therefore zero risk options are favoured (Lyon, 2008). Yet blind trust in technological innovations may raise unrealistic expectations and eventually lead to widespread *distrust*.

The second prominent issue in debates about biometric technology and ePassports concerns the issue of *function creep*. Function creep describes the phenomenon where 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 thus communicated in public. The main concerns here are not linked only to privacy violation e.g. the use of personal data without consent and for purposes other than those for which it was collected, but to state abusing its authority over its citizens (Mordini and Massari 2008, Lodge 2010). But apart from individual fears, privacy violations can also have social repercussions (see more under the privacy heading below). It is feared that law enforcement agencies will use databases of biometrics under the guise of national security for other purposes than identity verification on borders[2], for example pursuing covert mass-surveillance for profiling in order to predict people's behaviour and pinpoint suspects. Such fears can be further aggravated by the fact that the activities of such authorities are not generally transparent, whilst they possess broad and exceptional rights. Opportunities for such use of biometrics are tempting (EU projects like ADABTS and INDECT and the U.S. Home Department project FAST are examples of this trend), but also particularly intrusive since all people in public places could in principle come under surveillance (Sutrop, Laas-Mikko, 2012). In Europe, this issue is complicated as the current practice in EU member states regarding ePassports issuance, biometric data collection and usage (question of databases and secondary use, mainly for criminal investigation purposes, etc.) varies as these issues are not covered by EU regulation.

Some scholars have concluded that insufficient public information on the objectives of the utilisation of ePassports and eIDs and the rapid adoption of new forms of technology like these without public discussion can escalate public fears and *trust deficit* (Sprokkereef and de Hert, 2007, Lodge, 2010).

Introduction of security technologies such as ePassport are often justified in terms of a beneficial trade-off, where the amount of privacy lost is compensated by an increase in national security (Pavone and Degli Esposti, 2012). According to a recent study of Pavone and Degli Esposti (2012), acceptability of new surveillance oriented security technologies is context-dependent and influenced by expected benefits and perceived risks of the technology. In order to weigh values, assessing and identifying *relevant* risks (to values) and benefits of technology, defining the context is important (Nissenbaum, 2010, Stahl et al, 2010). According to Stahl et al (2010) and Brey (2012), 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 etc.), as an artefact (hardware or smaller scale technical items, for example

[2] This is by no means a theoretical risk only. For example, in Finland the police have had access to biometric data collected from refugees for the purposes of residence permits. See: Pohjolan Sanomat 2012.

RFID chip), or at the level of applications of technology – the use of technologies (and artefacts) for particular purposes and in specific settings/technical configurations (for example ePassport, smart (automated) CCTV for the identification of abnormal behaviour, etc.). A particular high-level technology or artefact can raise different risks and ethical issues depending on the context and its application (Stahl et al 2010). The context in their understanding refers to the use of technologies for particular purposes and functionalities in specific configurations (components, features, etc.). For our purposes it means that we have to identify ethical and societal risks and benefits in the specific situation/case and level of technology application.

4.3 Privacy and function creep

The main social and ethical concerns regarding the deployment of ePassports and biometrics are related to the loss or violation of privacy as a consequence of such security threats as data leakages, eavesdropping (chips), cloning, identity theft and tracking of passport holders (Juels et al, 2005, European Biometrics Forum, 2006, Hoepman et al, 2006, Carlussio et al, 2007, Schouten and Jacobs, 2008, FIDELITY, 2010). These are all threats in which data processing and usage takes place without the consent of the data owner. Thus the main threat to privacy derives from the potential misuse of biometric data (Alterman, 2003). 'Data owner' in this context means the ePassport holder: someone using an ePassport that has been issued to him or her.

In the context of ePassports, the main objective of biometric verification is to mitigate risks of identity loss and identity theft so that no one can pass him- or herself off as someone else and thereby make use of the rights, entitlements and benefits belonging to another individual. 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 (for example, access to buildings or databases).

For our purposes and context it is important to analyse the value of privacy: why is privacy important to people? What is it that they lose in cases of data leakage or eavesdropping[3]? The theoretical concept of privacy is complex. Privacy is often analysed as a right (claim or liberty); a state or a condition; a social good or value or interest of an individual. Although different aspects of privacy can be distinguished (informational privacy, bodily and local privacy, decisional privacy etc.), in the context of ePassports and biometrics it is mainly understood as informational privacy: a person's control over the access and use of his or her data (Moore, 2008).

Privacy is mostly regarded as an individual and instrumental value – one which is treasured 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 (see Gavison 1980, Kupfer 1987, Rössler 2005 and others). 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 (Sutrop, Laas-Mikko, 2012). Informed consent is the autonomous authorisation by subjects to carry out a procedure (e.g. the processing of data with substantial understanding and in the absence of control by others). The basic moral meaning of informed consent is to protect data subjects from deception and coercion (Manson & O'Neill, 2007). Respect for moral autonomy implies taking into account the other person's self-identification: we ought to understand the other person's aims, evaluations, attitudes, thoughts and desires from his or her point of view (Williams, 1973).

Aside from the individual value of privacy, this notion has wider social relevance (Gavison, 1980, Regan, 1995, Solove 2008, Rössler and Mokrosinska, 2013 and others). Indeed, Daniel Solove (2008) has argued that the value of privacy should be understood specifically in terms of its contribution to society. Priscilla Regan (1995) has stated that that privacy serves not only individual interest, but also common, public and collective purposes. Privacy as a common value is a right, which protects interests that are regarded so fundamental that all individuals in common have a similar interest in them. A public value of privacy is derived from its importance to the exercise of rights essential to democracy and from its importance as a restraint on the arbitrary power of government. Also, recent studies of Valeria Steeves (2008) and Rössler and Mokrosinska (2013) discuss privacy, individual value of autonomy and value of privacy in social construction of relationships and interaction. A recent theory by Valerie Steeves (2009) revitalizes the

[3] For further discussion on the philosophical aspects of privacy, see the report compiled for the FIDELITY project by Elin Palm (Linköping University).

concept of privacy as a social value because it enables one to enter into meaningful relationships with others (see Jeffrey Reiman (1976)). She refers to „a social construction that we create as we negotiate our relations with others on a daily basis" (Steeves, 2009). Privacy is an inherently social practice that enables social actors to navigate the boundary between self and other, and between being closed or open to social interaction. According to this theory, social actors are able to choose what is more important to them; it is both an individual and a common value in so far as individuals share it.

In the surveys conducted about ePassports and/or biometrics (Ng-Kruelle et al., 2006, Perakslis and Wolk, 2006), individuals tended to name the loss of privacy and abuse of data as threats, but there was no further reference to any potential subsequent impact that a loss of privacy might have on the individual or society (surfacing as discrimination, damage to reputation, loss of autonomy, fear of the 'surveillance state', loss of trust in the state etc.). It appears that as in other general surveys about privacy (Hallinan et al., 2012), empirical data does not demonstrate privacy's dual functionality (individual and social).

However, value conflicts are an inherent part of life in pluralistic society, and privacy also has to be weighed and balanced against other important and sometimes incommensurable values. 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). According to Acquisti and Grossklags (2007) 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 (2007) 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. Also, people may not really have alternative choices for using technologies, services, etc. which may jeopardize their privacy. A part of the privacy problem in the context of ePassport involves people's limited bargaining power regarding privacy, since ePassports are in most cases the only state issued travel documents and obligatory for travelling for example to third countries outside EU.

4.4 Social injustice and discrimination

There are several ways in which the discrimination of a person or group of persons in relation to ePassports can occur:

1) upon the revelation of a bodily trait or characteristic or information (e.g. DNA can reveal information about a person's genetic invariance or health condition);
2) in the enrolment or registration process if biometric data are associated with another identity or other data (Lyon, 2008);
3) giving false negatives (the right person is rejected) or false positives (the system wrongly associates an identification with a particular person) caused by inaccuracies in measurement, algorithms, poor quality of biometric data etc.;
4) cross-matching of biometric data with other databases, profiling and categorising people; and
5) access to ePassports grants more convenience on borders compared to people who do not have them.

In the case of current ePassport settings where only facial, fingerprint and iris images are used, the first case is not that relevant. If new biometrical traits are added, the analysis of discrimination potential by bodily trait or information revealed by it must be reconsidered.

The second case is relevant when mistakes in the enrolment or registration process are made or the process or system is manipulated. As a result, a person's data is associated with another identity, i.e. another person's data.

In the third case false negatives and false positives are mostly related to inaccuracies in the enrolment process of biometric data, the poor quality of data (for example some people with certain professions have fingerprints of very poor quality) and poor algorithms. David Lyon (2008, p.502) notes that "tighter tolerances make for more false negatives; looser for more false positives." He also notes that tolerances are set in the interests of the scheme's primary sponsor and thus may vary according to the business case

(higher traffic demands more tolerance to ease flow etc.). Tolerance ranges are not usually open and obvious, which makes societal scrutiny difficult.

The fourth case of injustice and discrimination – cross-matching biometric data with other databases, profiling and categorising people – is especially problematic since it could lead to the social classification and stigmatisation of people, assigning them automatically to some suspect category, for example as a criminal or terrorist, but also as a Muslim and so on. David Lyon (2003) has pointed out that 'social sorting' is the key to understanding the nature of surveillance. Surveillance practices as described above, according to Irma van der Ploeg (2006), "produce infinitely better inhabitable identities for some people than for others". In addition, she argues that particular profiles can be created from aggregated data and social identities are attached to people behind their backs, whether they actually fit into the category in question. With growing interconnectedness, cross-matching databases and sharing information between parties, such attributed identities would become permanent and harder to refute later on (2005).

The last case concerns discrimination in a more general manner. Those travellers who do not have ePassports (maybe because his or her country of residence does not issue such documents), are automatically less trusted. ePassport owners can use for example automated border control (ABC) gates and do not have to wait in long queues for border control inspectors who have a right to interview travellers in-depth. It is questionable, whether such "security envelopes" - areas of secure travel and overly robust distribution to trusted and less trusted traveller's works in preventing terrorism and criminal activity.

4.5 Empirical studies on ePassports

The public perception of biometrics and ePassports are likely to vary between countries. However, only a few relatively small-scale surveys exist to date.

Eurobarometer (2012) has shown that the general public has very different views in different European countries even on the very basic question of the privacy of passport data. However, this data set does not go into details on ePassports.

Ng-Kruelle et al. (2006) conducted a survey (with 303 respondents) among EU citizens in Germany, the United Kingdom, Spain, Denmark and Greece on end-user perceptions of biometric implementation in ePassports and ID cards. According to the results, the most important factors in ePassport acceptability are the enhancement of security and the convenience of border solutions. When respondents considered the proposal of ePassports as a whole, 60% named enhanced security as a motivator, while 46% named convenience. Several other surveys, e.g. Perakslis and Wolk 2006, show similar results [4].

The same survey revealed that the most attractive implications of ePassports were protection and enhancement of personal security – protection from forgery and crime and a simplified and shortened identification process. National security benefits (such as protection from terrorism) were not important arguments for users.

However, these considerations are not supported by the results of consumer surveys conducted in the USA, which show that despite concerns about privacy there are clear motivators for the acceptance of biometric and RFID methods – such as reducing identity fraud, boosting security, the convenience of identification and fighting terrorism (Perakslis and Wolk, 2006).

According to Ng-Kruelle et al. (2006) the most significant negative aspect associated with ePassports is the invasion of privacy in information collection (mentioned by 30% of negative respondents) while other perceived disadvantages were related to the safety/security of information – the fear of illegal access to and abuse of personal information. Some respondents consider ePassports as having significant negative consequences for privacy. Unwanted access to and possible misuse of private information is a clear concern.

[4] Yet it remains relatively unclear what exactly 'enhanced security' means in this context. 'Convenience' in this context usually means the speed of border controls and no extra compensating security controls (physical search etc.).

Table 1. Perceptions of ePassport adoption

Perceived Positive (N=150)		Perceived Negative (N=30)	
Protection from crime/fraud	29%	Privacy invasion	30%
Security	19%	Abuse of information	13%
Speeding up of identification process	8%	Access to information	13%
Convenience	8%	Monitoring/Surveillance	10%
Innovative technology	5%	No benefits to citizens	10%
Accurate identification	5%	Accuracy of technology	7%
Additional functionalities	5%		

Source: Ng-Kruelle et al. (2006)

Only 23% of respondents felt comfortable with their information being accessed by organisations besides those they had specifically authorised – and worried about potential abuse of their personal information by unauthorised bodies. Even positive respondents named data safety as a precondition. Those respondents who were favourable towards information access by other organisations still shared the concern about the security of data. 30% were concerned about information access (who and what) as a possibility for third parties.

In sum, earlier surveys are fairly generic in terms of the societal benefits and risks of ePassports. They do not address perceptions towards specific technologies, such as fingerprints or eye iris images. They do not address specific use scenarios of passports, such as identity checks by a public or private service provider, or identity checks while travelling. This is why a tailored survey needed to be carried out for the purposes of the FIDELITY project.

5. Research framework

5.1 Unified theory of acceptance and use of technology

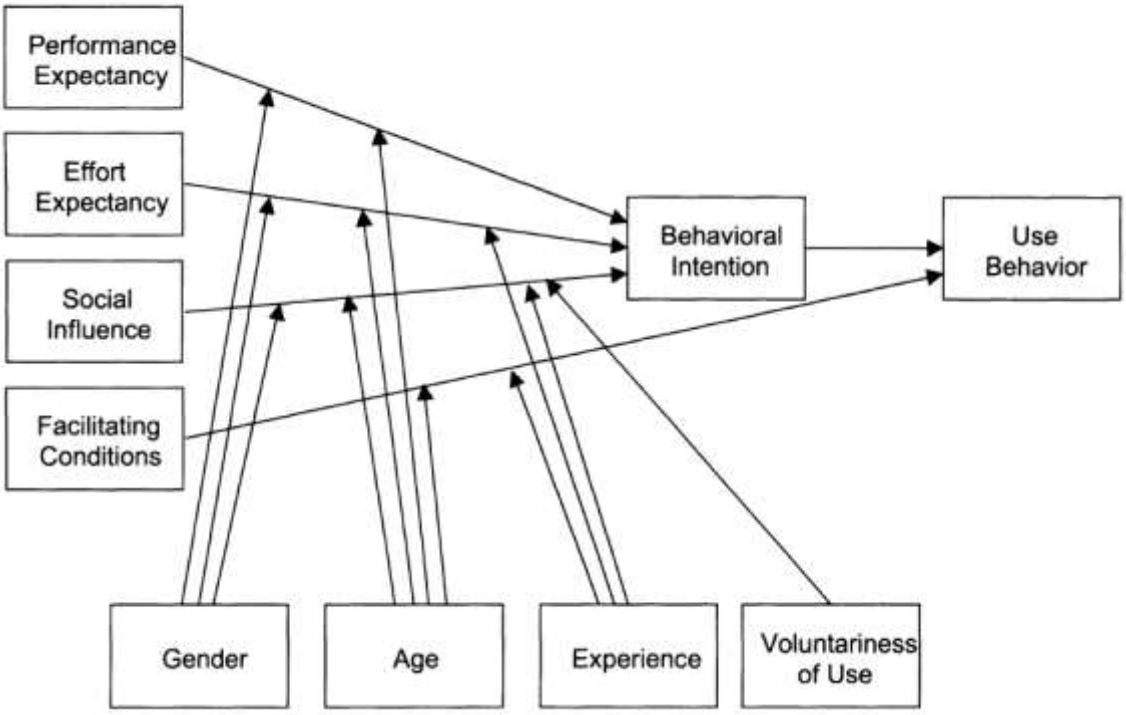
Technology acceptance is an important research issue and the development of models for technology acceptance has received increasing attention in academic literature. The general point of departure for these models is that there are a number of factors that will influence the user as to whether or not to adopt the technology. The goals of many studies have been to find factors that can be used to motivate the user to accept and start using the new technology (see, e.g., Ash 1997, Mathieson 1991, Venkatesh 2000).

One popular model for mapping those relevant factors is the *technology acceptance model* (TAM), which argues that the perceived usefulness (the degree to which a person believes that using a particular system would enhance his or her (job) performance) and ease of use (the degree to which a person believes that using a particular system would be free from effort) accounts for whether a technology is adopted or not (Davis 1989). Generally speaking, TAM is a theoretical model used in different contexts to help understand and explain the use of information technologies (see Lederer et al. 2000, King and He 2006, Legris et al. 2003).

Another approach, the *unified theory of acceptance and use of technology* (UTAUT) is perhaps the most widely used technology acceptance model currently available. It is more elaborate and incorporates additional factors than TAM. It was formulated first by Venkatesh and colleagues in (2003) and developed further in Venkatesh et al. 2012. It has since been empirically applied in several studies, including for example Lin and Anol (2008) who analysed instant messaging adoption in Taiwan and Curits and colleagues (2010) who analysed adoption of social media for public relations by nonprofit organizations.

UTAUT explains how a decision is formed about the use an information system. The theory builds on four key constructs: 1) performance expectancy, 2) effort expectancy, 3) social influence, and 4) facilitating conditions. The first three are direct determinants of the technology use intention and actual use behaviour, and the fourth a direct determinant of actual use behaviour. Also, gender, age, earlier experience with (related) technologies and voluntariness of use are also considered to influence the use intention and actual use behaviour (Figure 1).

Figure 1. Schematic view of the Unified theory of acceptance and use of technology



Source: Venkatesh & Davis 2003, p. 447.

In applying this model to the analysis of social acceptability of ePassports, we interpret the above elements, on the basis of the above literature review, as follows.

First, performance expectancy refers to the "the degree to which an individual believes that using the system will help him or her to attain gains in job performance" (Venkatesh et al. 2003, p. 447). For our purposes, performance expectancy covers both expectations of the government as well as public in relation to the adoption and use of ePassports. This includes direct benefits, such as greater protection from document forgery or speed of border control procedures, and more general public policy targets, such as the fight against illegal immigration or fight against serious crime.

Performance expectancy deals also with certain social risks of technology, including preservation of privacy. This is especially important regarding ePassports as even if higher security is potentially seen as a positive aspect, privacy considerations and especially fears of function creep – the phenomenon where personal data is used by data-processing bodies beyond the scope for which it was initially intended – might reduce the perceived benefits and lead to lower intention and actual use.

Importantly, performance expectancy relates also to the acceptability of specific ePassport solutions under consideration in the FIDELITY project. Thus, a number of scenarios were developed covering potential ways of using ePassports and related data in the establishment of identity and identity checks, including travel and border crossing.

The second factor – effort expectancy – relates to the degree of ease associated with the use of a technology. Basically, for the end users technology needs to be user friendly. ePassports as physical documents are not difficult to use. Earlier research is actually inconclusive if deeper knowledge about ePassports leads to higher acceptance of the use of advanced biometrics, such as fingerprints or eye iris images in ePassports. Still, we expect that citizens' existing knowledge on ePassports, e.g. what data ePassports include or how they differ from earlier passports, influences considerably public expectations towards benefits and risks of ePassports.

Social influence measures "the degree to which an individual perceives that important others believe he or she should use the new system" (Venkatesh et al., 2003, p. 451). So, it is about the influence of friends, family, or others (role models, opinion leaders) that would either encourage or discourage the use of ePassports and various related applications. It is therefore important to know the main sources of information regarding ePassports that are used by different groups within society. In particular this includes 'less informed people' for whom 'word-of-mouth' might be more relevant than other, more straightforward methods of communication (i.e. newspapers, government documents).

According to the UTAUT model, intention or usage is also determined by facilitating conditions; this relates to "the degree to which an individual believes that an organizational and technical infrastructure exists to support use of the system" (Venkatesh et al., 2003, p. 453). For example, to use electronic functions, such as automated border control gates, familiarity with modern ICT is necessary, but such skills are widely available in Europe (Bilbao-Osorio *et al* 2014), and Eurostat (2014) shows consistently high levels of personal computer and Internet usage in Europe.

The citizens' belief in government benevolence – the belief that the government acts in citizens' best interest – is another important facilitating condition. Even though the UTAUT model does not emphasise the issue of trust too much, the research on social construction of technologies, especially on more sensitive applications, such as those involving advanced biometrics, attaches a lot of importance to trust.

Finally, several variables like gender, age, experience with a specific or related technology, and voluntariness of use are considered to influence the adoption process (Venkatesh et al. 2003). Therefore, demographic variables like gender, age, education and occupation, are important for the current study for identifying different social groups. For example, representatives of more technology savvy younger generations who are more eager to accept and use the various ICT are more likely to be better informed about ePassports. They may be also better positioned to have an opinion in topics that deal with advanced technology, where some people would remain undecided. Still, we expect people to have clearer positions on currently used as well as on and less sensitive technologies, such as personal identity codes, while they would remain less decided or even reject the use of advanced (and more intrusive) biometrics (fingerprints, eye iris images, DNA data). Voluntariness of ePassports and availability of (potentially mandatory) alternatives, e.g. electronic identity cards, is another factor to be taken into account in the current analysis.

5.2 Research method and data collection.

A survey on the social aspects and readiness of ePassports was carried out over the period of February – March 2014 in the following countries: Estonia (EE), Germany (DE), France (FR), Sweden (SE), United Kingdom (UK) and the United States of America (US). These represents a selection of European larger (DE, FR, UK), and smaller (EE, SE) countries, plus the US. Both the establishment of identity and identity management are handled differently in different countries covered by this study. Some countries have personal identity codes and central identity document databases, which include all relevant document details (e.g. EE), while others do not have a personal identity code nor central identity documents database (e.g. DE). Furthermore, some countries (e.g. EE) are very advanced in issuing electronic identity cards, which have replaced passports in all intra-European transactions, while governments of some others (e.g. UK) do not issue electronic identity cards at all.

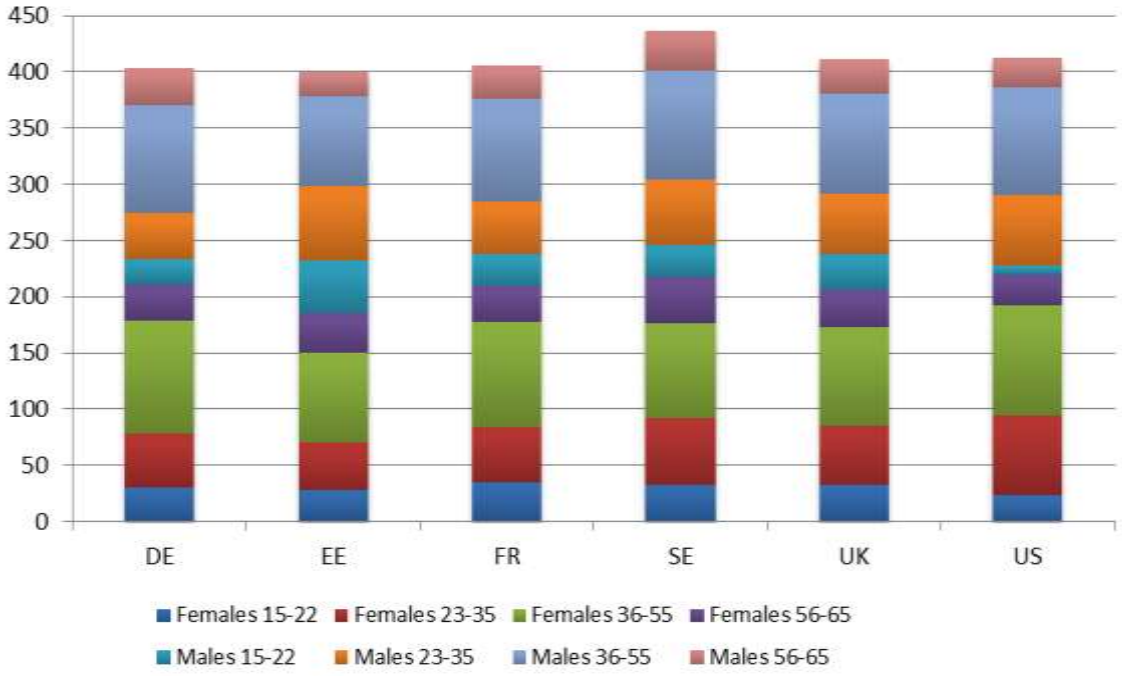
On the basis of the research framework described in Chapter 6.1, a survey questionnaire with 49 questions was developed. It was mostly composed of statements where the respondents replied on Likert scale (strongly agree, agree, undecided, disagree, strongly disagree); for clarity, the titles of the graphs in the following chapters reflect the statements proposed.

The survey was carried out as an online survey using SurveyGizmo (www.surveygizmo.com) a web survey service. Cint survey panels (www.cint.com) were used to target and recruit individuals between the ages of 15 and 65 from respondent database. The collected responses are generally representative of the gender and age distribution of the population of respective countries.

According to Eurostat, approximately 5-15% of the 16-74 years old population (Eurostat 2014) does not use the Internet and are thus automatically excluded from online surveys. We are aware of this inherent weakness of the survey data set and acknowledge in the subsequent analysis that online surveys exclude a minority who has no sufficient knowledge or skills for using Internet. However, such people are generally of older age (Brandtz et al. 2011) many of whom we would expect would be unable to respond to the technology specific questions that deal with ePassports. Thus, we expect that she share of persons how are uninformed or undecided about various technology specific questions or scenarios for using ePassports would have been greater if we would have been able to cover also persons not using Internet.

All together 2,833 persons responded to the survey, 2,468 of which were fully completed. In the analysis, still, we take their responses into account, where possible. Age and gender breakdowns for the respondents are presented in Figure 2.

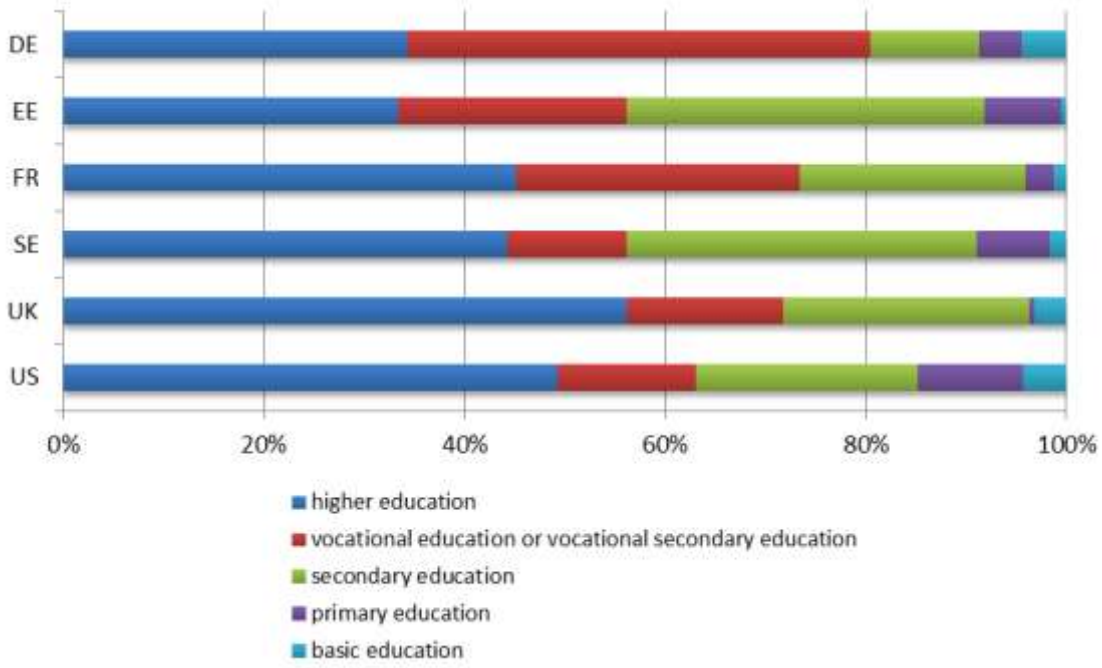
Figure 2. Age and gender breakdown of the survey respondents by countries



Source: ePassport web survey 2014, n=2,468.

Nearly half of the respondents had higher education (44%), one-quarter had secondary education (25%) and 23% had vocational education/vocational secondary education (Figure 3). It is difficult to compare the representativeness of our sample with the selected countries due to different age and education level groupings on Eurostat. Still, we can see that the share of those having upper secondary and post-secondary non-tertiary education dominates generally in all countries according to Eurostat (2014) as well as in our survey (2014). However, we also see that the persons with pre-primary, primary and lower secondary education are somewhat underrepresented in our survey.

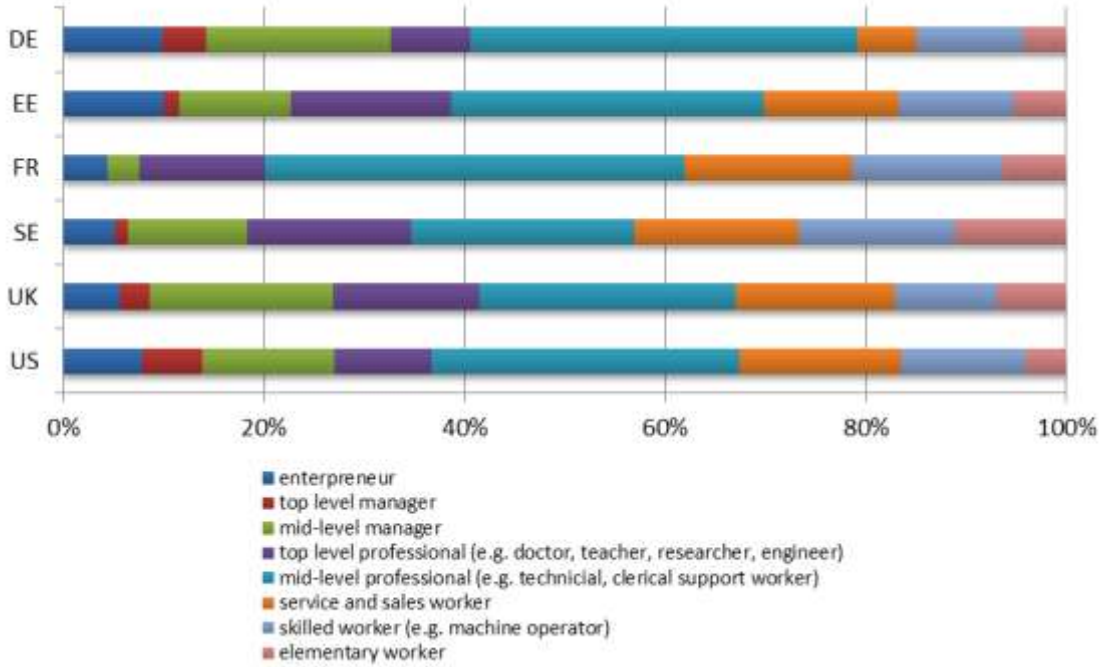
Figure 3. Education level of the respondents



Source: ePassport web survey 2014, n=2,473.

Of the 1,576 respondents active in the labour market, most of whom (32%) are mid-level professionals, e.g. technical, clerical support workers. (Figure 4)

Figure 4. Occupation of the respondents



Source: ePassport web survey 2014, n=1,563.

We control for the effect of education level and occupation in relation to acceptability of ePassports and their use scenarios in the following chapters.

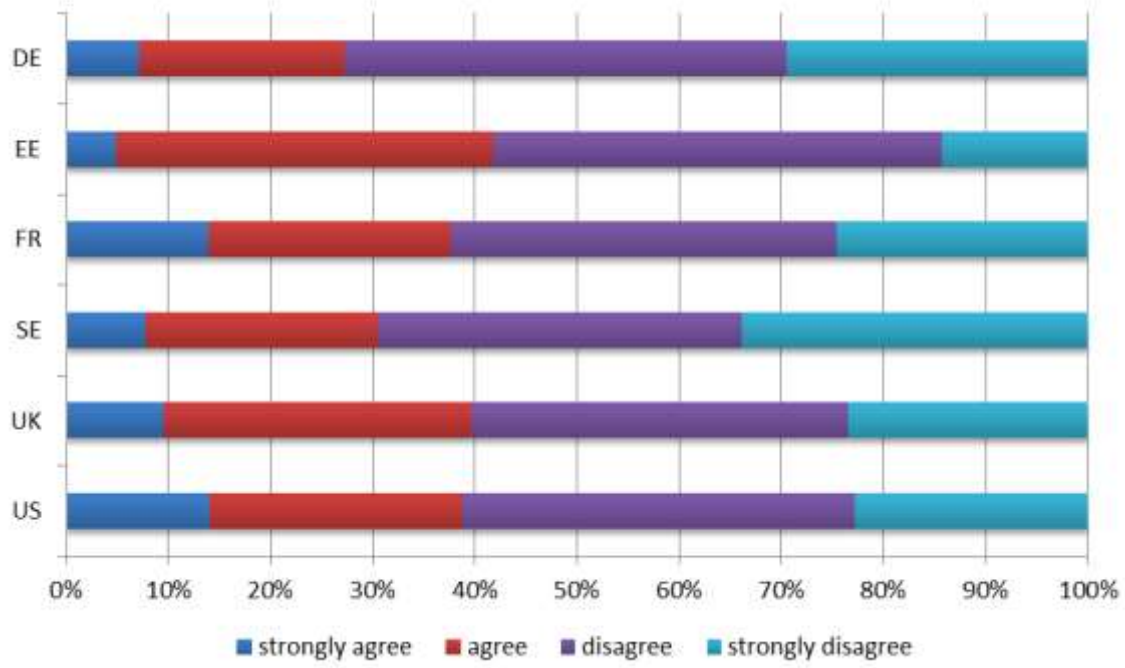
6. ePassports in six countries

6.1 Awareness on ePassports and personal data collection

The residents of the six countries surveyed indicated that in general they are fairly little informed about the personal data that both government and private companies collect on them.

Only a minority of the respondents indicated that they have enough knowledge on personal data private companies collect on them personally, i.e. they strongly agreed with the statement “I have enough information about the data different private companies collect on me personally”. The majority (2/3) of respondents disagreed or disagreed strongly with that statement (Figure 5).

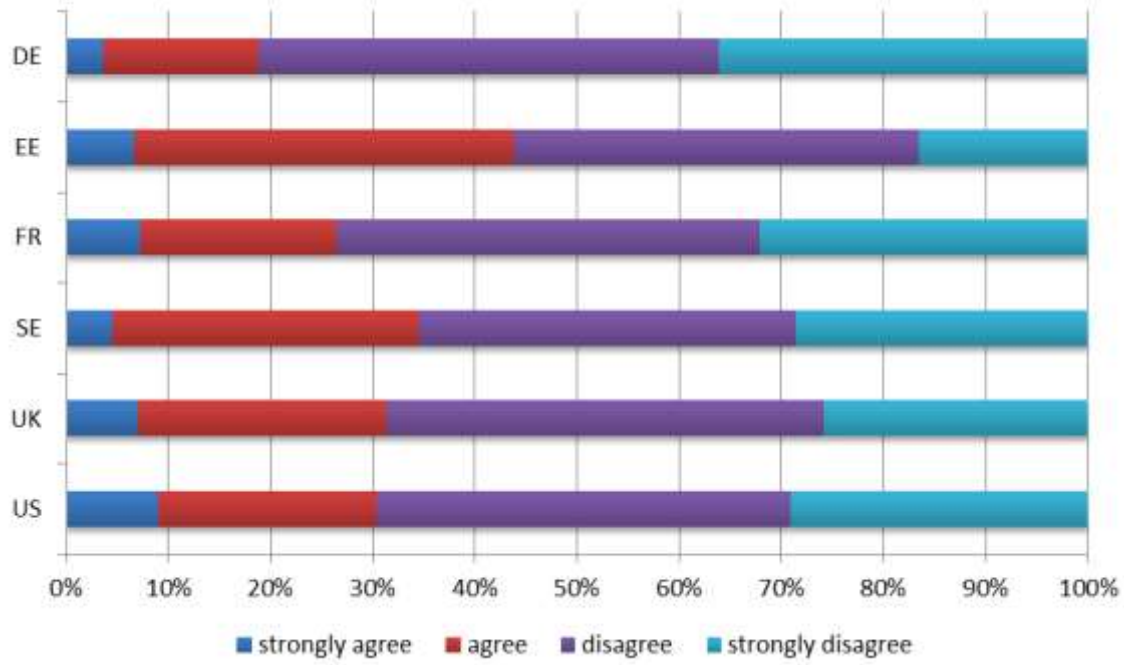
Figure 5. I have enough information about the data different private companies collect on me personally



Source: ePassport web survey 2014, n=2,768.

The population of the majority of countries are even less informed about the personal data that government collects about them (compare Figure 5 and Figure 6). People with higher education and top level managers are less likely to consider that they have enough information about the personal data that private companies and the government collects on them (see Table 2, Table 3 and Table 4 in appendices).

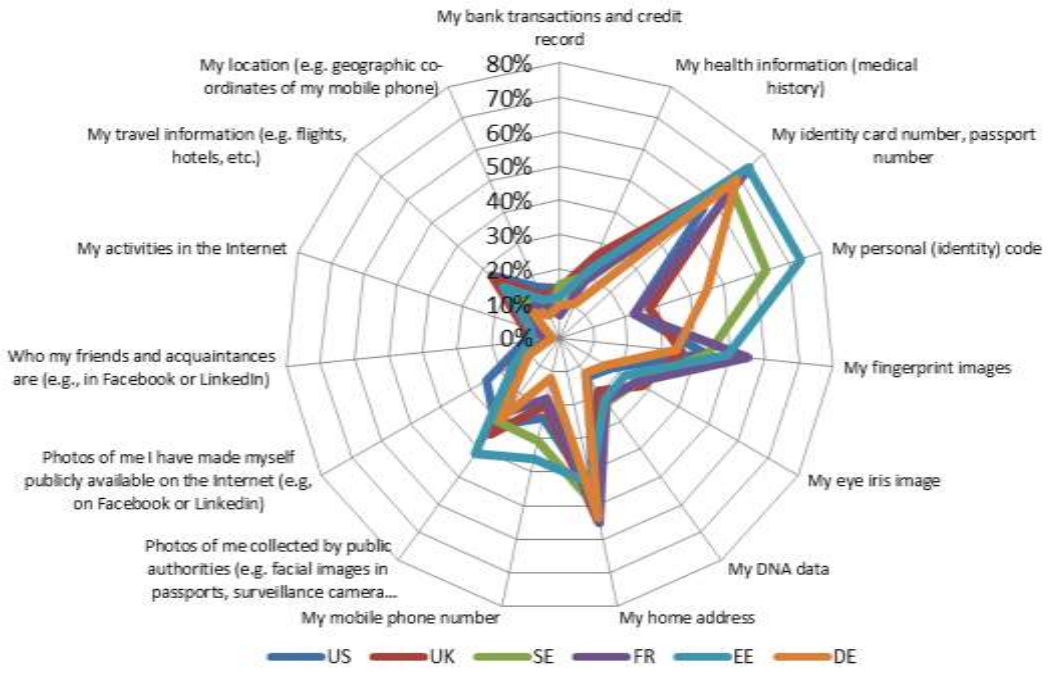
Figure 6. I have enough information about the data the government collects on me personally



Source: ePassport web survey 2014, n=2,751.

The public of different countries is in principle willing to grant the government, for public security purposes, access to their identity document numbers and home address. In some countries, such as SE and EE, where personal identity codes are in widespread use, the use of this data is widely supported. Contrastingly, the FR and UK public offers very limited support for this. Support for the use of photos and fingerprints collected by the government is also notable, but varies also across countries. The public is, however, particularly unwilling to surrender their financial data, data published on the Internet and Internet activities and travel/location data to the government for public security purposes. (Figure 7)

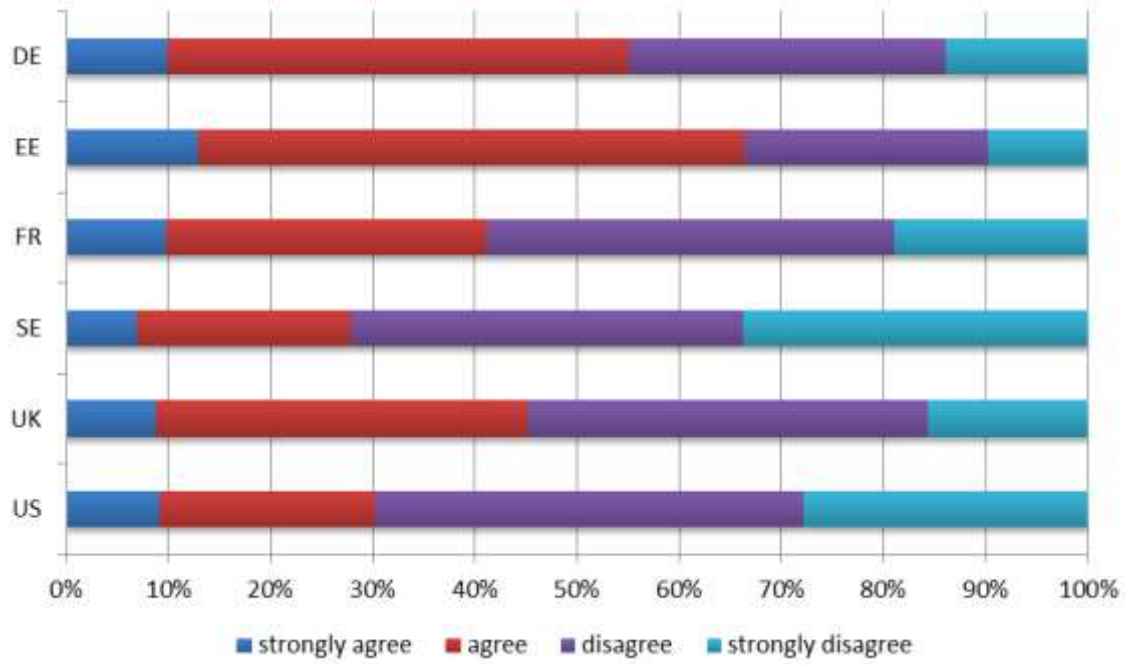
Figure 7. I find it acceptable that government authorities collect and analyse the following information for public security purposes



Source: ePassport web survey 2014, n=2,841.

The share of population of the countries covered by this study who has detailed information on data included in biometric passports is low – ca 10% strongly agreed with the statement “I know what data biometric passports include”, and the share of disagreeing respondents is generally high. Awareness in EE is higher. Females were more likely to estimate their knowledge to be lower and professionals and managers were more likely to state that they have knowledge of information about the data included in biometric passports (Table 4 in appendices).

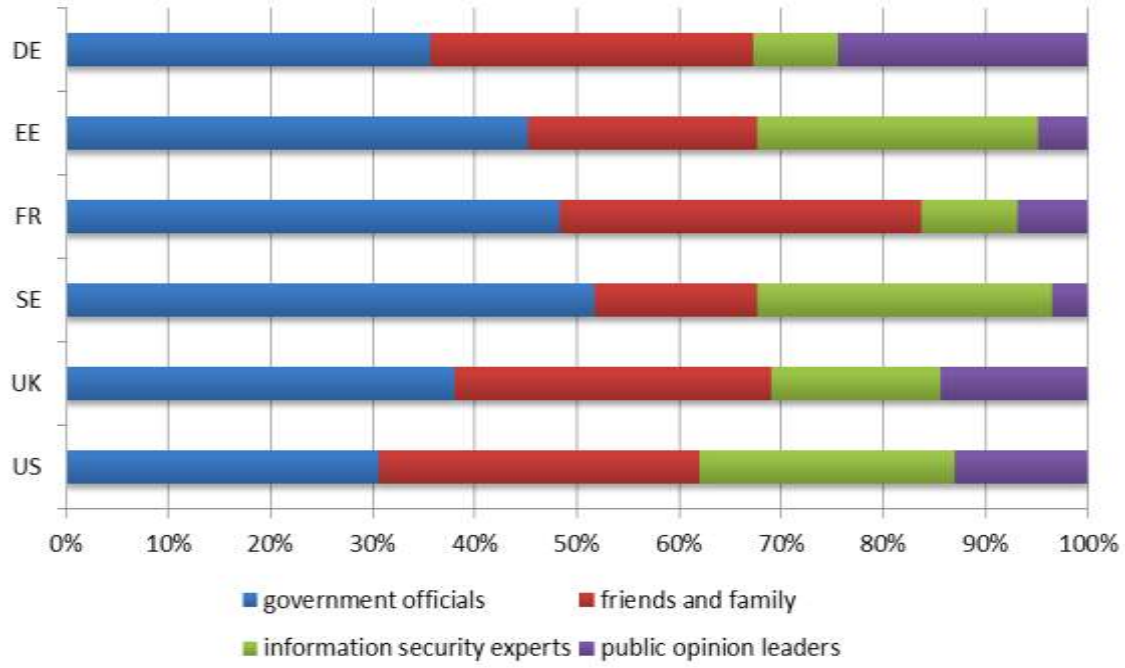
Figure 8. I know what data biometric passports include



Source: ePassport web survey 2014, n=1,899.

Government officials, and friends and family are typically the main sources for learning about novel identity documents. In some countries, such as SE, EE and US, also information security experts are an important source of information, while the role of public figures tends to be fairly low. (Figure 9)

Figure 9. Where do you learn about government issued identity documents, i.e. biometric passports and electronic ID cards?

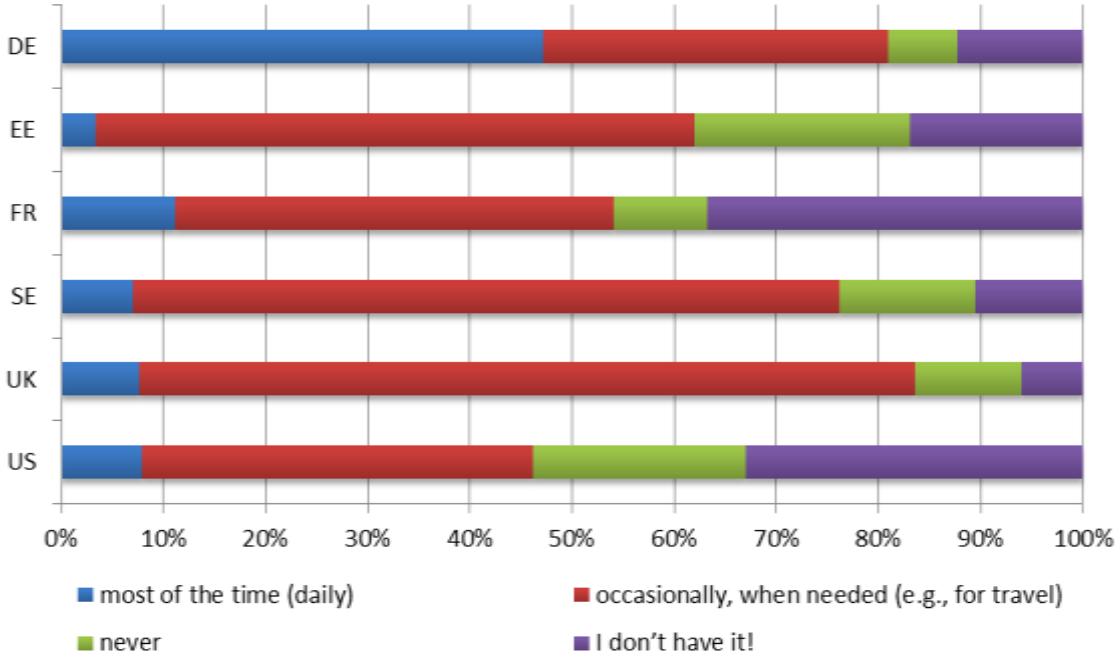


Source: ePassport web survey 2014, n=2,841.

6.2 Experience with ePassports

In Germany, half of the population carries passport on a daily basis. This is very different from the rest of the countries in the FIDELITY ePassport survey, where passports are mostly carried only on an as needed basis. (Figure 10)

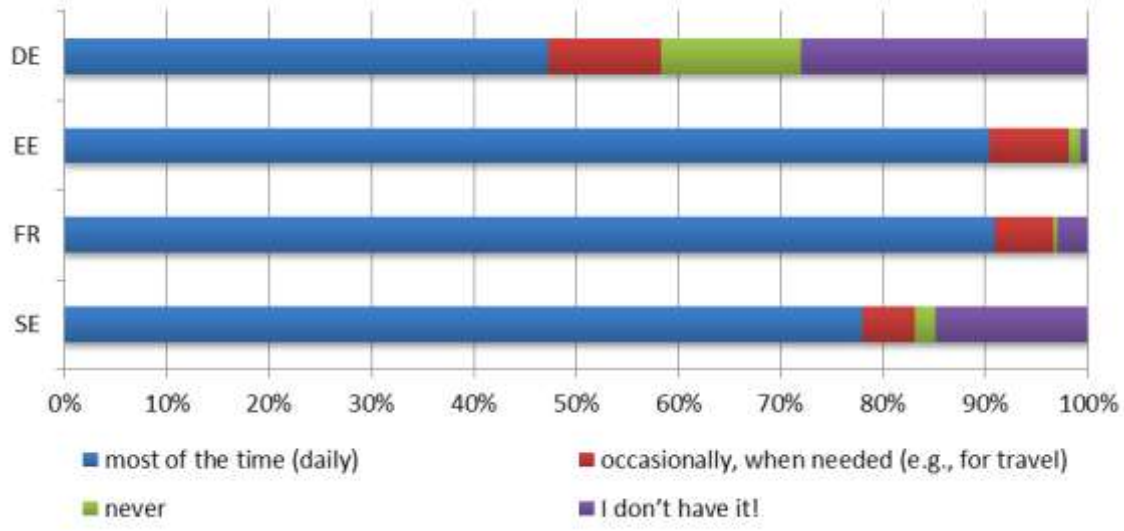
Figure 10. How often do you carry your passport with you?



Source: ePassport web survey 2014, n=2,663.

The governments of Estonia, Germany and Sweden issue electronic identity cards. France has only a non-electronic identity card, and the United Kingdom cancelled national identity cards in 2011. The United States does not have a true national identity card right now, as various other documents such as the social security card or driver's licence replace it for many purposes. An identity card, where a country issues it, is a preferred replacement of passport in daily use. In Estonia and France more than 90%, and in Sweden about 80% of persons carry an identity card with them on a daily basis, while the number of ID card users is considerably lower in Germany. (Figure 11)

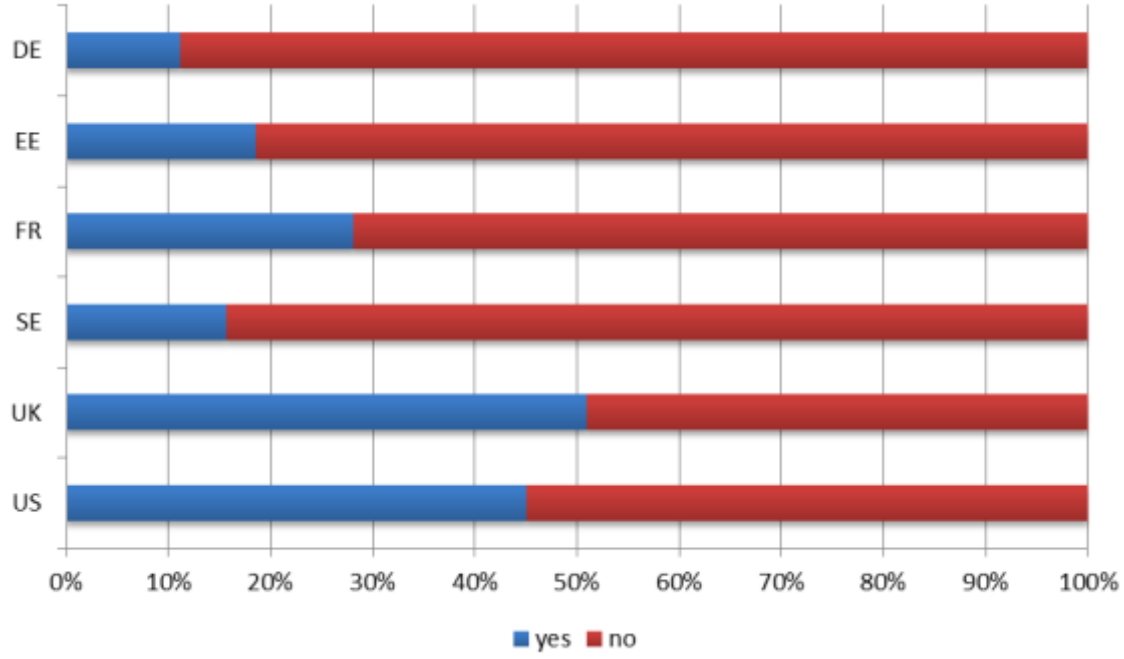
Figure 11. How often do you carry your identity card with you?



Source: ePassport web survey 2014, n=2,654.

In the United Kingdom and the United States about half of the owners of biometric passports have used automated border control (ABC) gates. The use of ABC gates is more limited in the rest of the countries covered by this survey. We have no reliable data to show why this is so, but assume that it has largely to do with the availability and intensity of deployment of ABC gates in major airports, ports, etc. (Figure 12)

Figure 12. Have you used automated border control gates for border crossing?



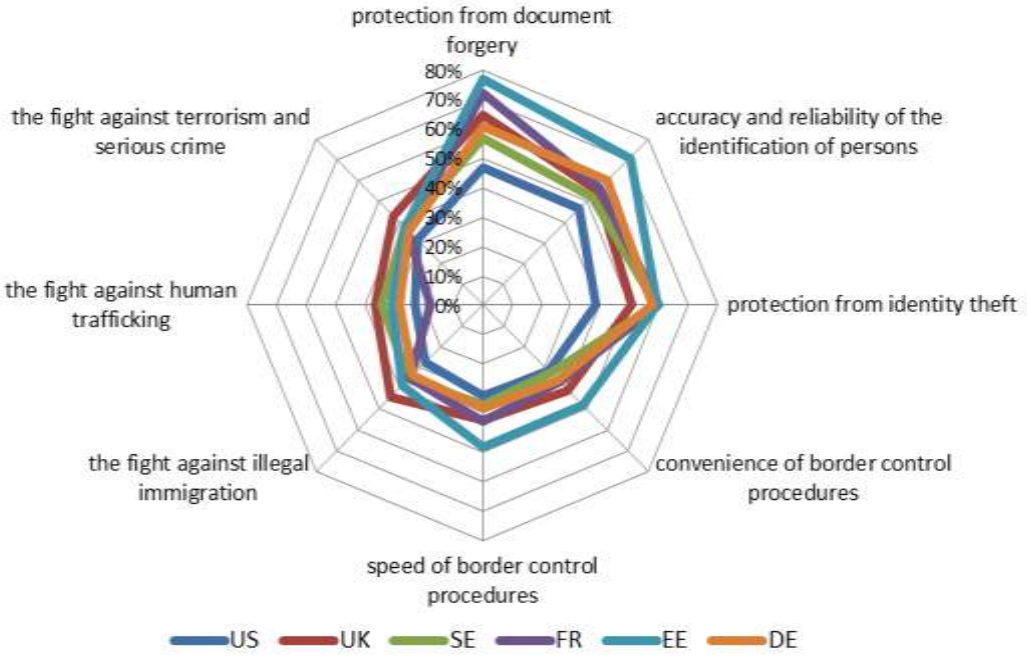
Source: ePassport web survey 2014, n=922.

6.3 Expectations and perceived risks of ePassports

The three main expectations regarding biometric passports were improvements in the protection from document forgery (63% of the overall respondents from all countries covered expressed this expectation), accuracy and reliability of the identification of persons (57%) and protection from identity theft (54%). Other expectations such as convenience of border control procedures, speed of border control procedures, the fight against illegal immigration, human trafficking and terrorism were less represented in the overall sample (28%-38%).

Some significant differences can be observed on the country level. Expectation regarding the protection from document forgery is more important in EE (77%) and FR (72%) and less so in the US (47%). In the US it is less expected that biometric passports protect from identity theft (Figure 13).

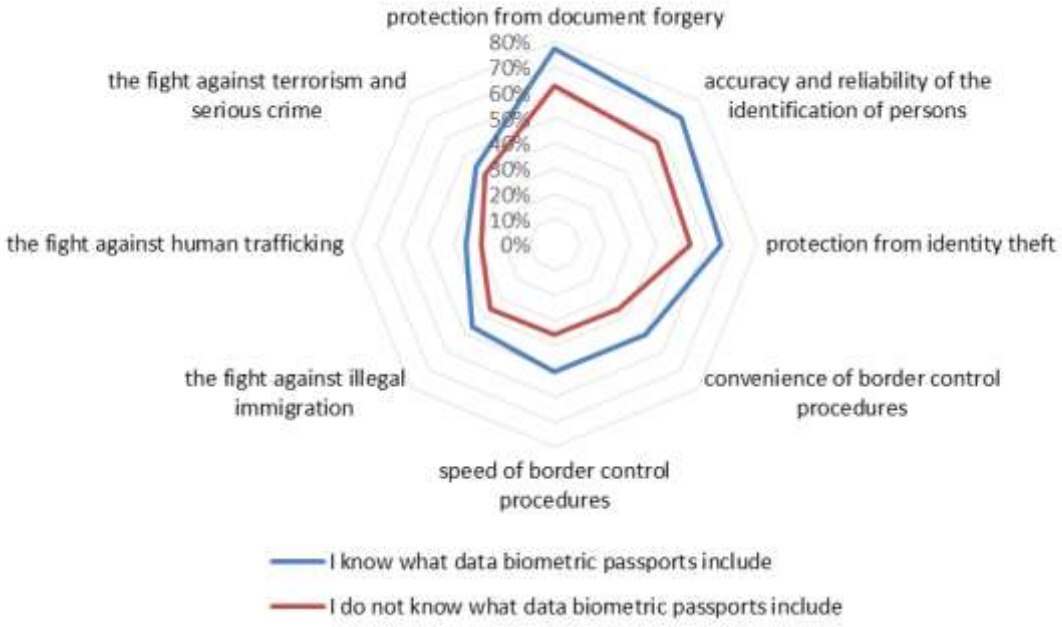
Figure 13. Biometric passports improve…



Source: ePassport web survey 2014, n=2,841.

If we look at the expectations of the respondents according to their knowledge on data biometric passports (see also section 7.1), it follows that people who have higher awareness (i.e. strongly agreed or agreed with the statement that “I know what data biometric passports include”) also have higher expectations regarding biometric passports in all areas (Figure 14).

Figure 14. Biometric passports improve…

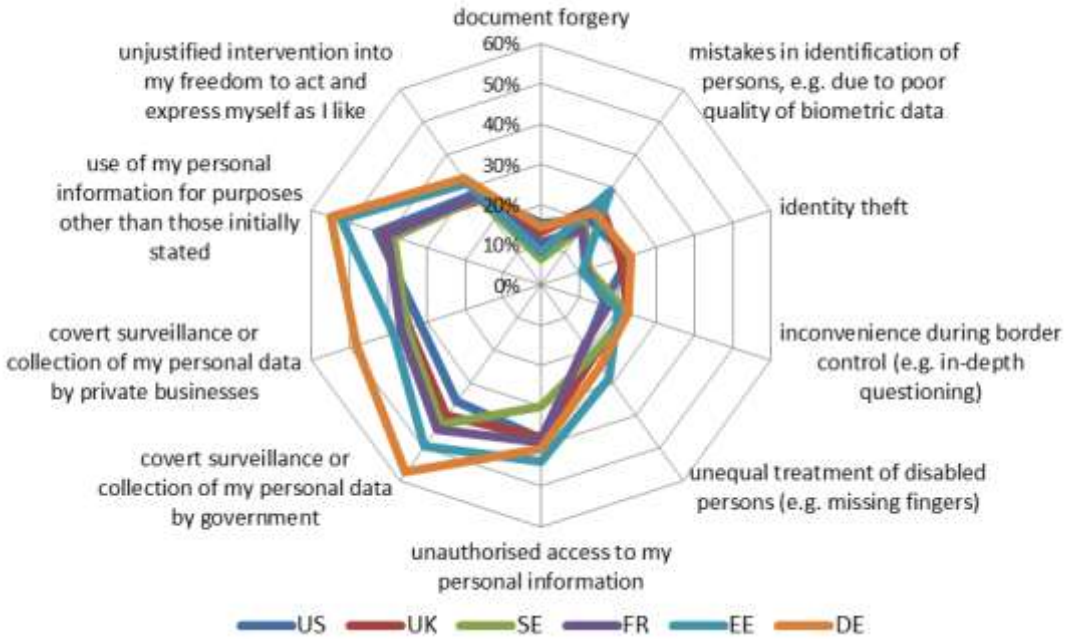


Source: ePassport web survey 2014, n=1,899

The main two risks that respondents see are related to the use of personal information for purposes other than those initially stated (45% of the overall respondents from all countries covered expressed this concern) and covert surveillance or collection of personal data by government (45%). Slightly less important were (rather related) risks of unauthorised access to their personal information (38%) and covert surveillance or collection of their personal data by private businesses (37%).

The risks of covert surveillance or collection of personal data by government and private businesses as well as the use of personal information for purposes other than those initially stated are of higher concerns for the DE respondents. Also, it is interesting that while the respondents from EE had high expectations regarding the biometric passports, they are also more concerned about the main risks. In SE the unauthorised access to personal information is considered of a less risk compared to other countries (Figure 15).

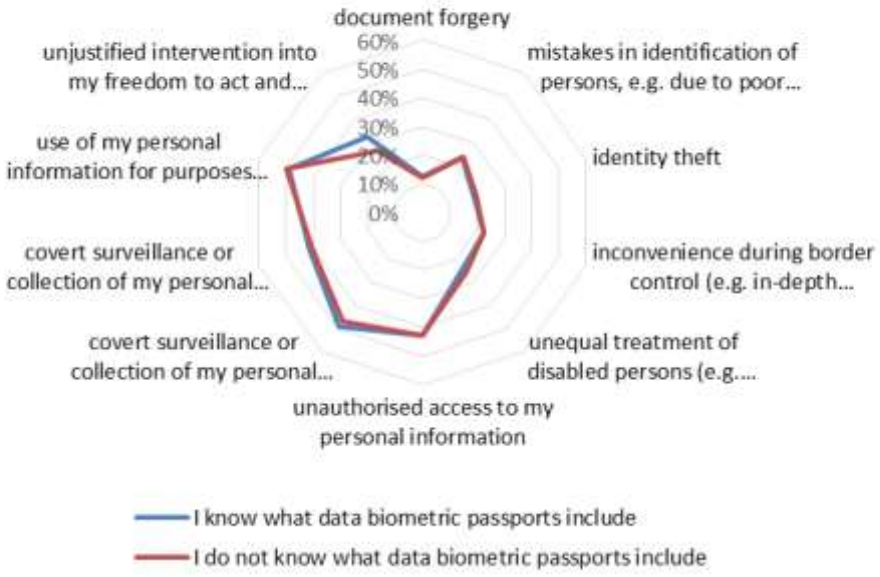
Figure 15. Biometric passports increase the risk of…



Source: ePassport web survey 2014, n=2,841.

Interestingly, the perceived risks of biometric passports is almost exactly the same whether the person knew them or not. (Figure 16).

Figure 16. Biometric passports increase the risk of…

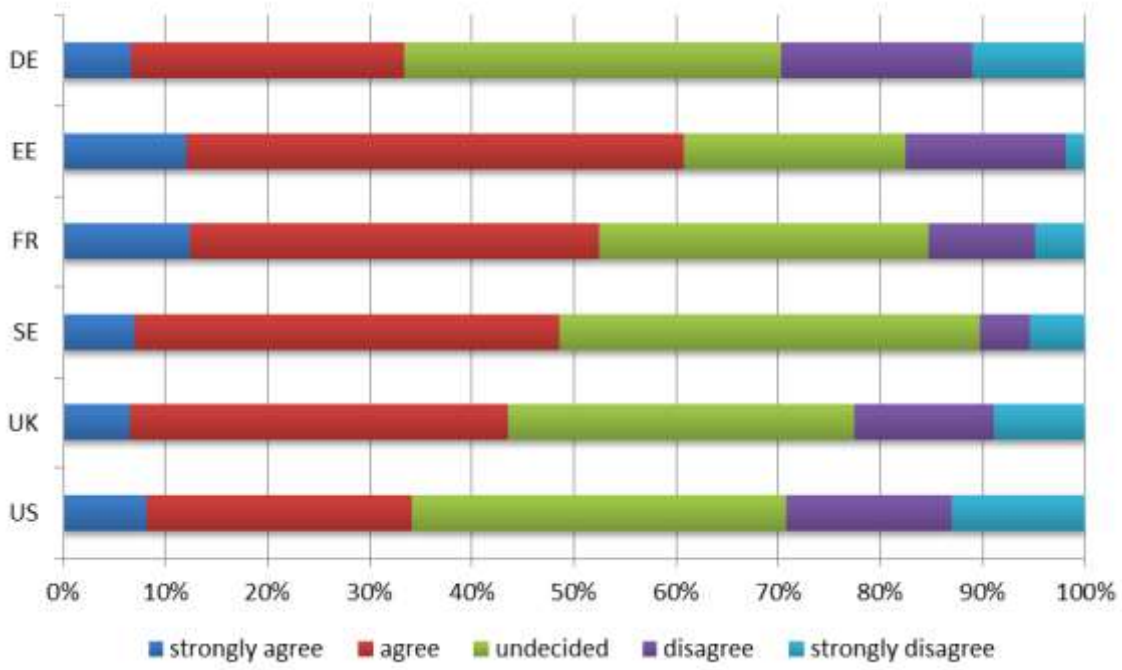


Source: ePassport web survey 2014, n=1,856.

6.4 Trust and ePassports

The share of people who strongly agreed or agreed with the statement “I believe, that the government acts in citizens’ best interest, when introducing and using new national identity documents, e.g., biometric passports or electronic identity cards” varied from relatively higher trust level in EE to more moderate level in FR, SE and UK, and lower levels in DE and US. High share of people remain undecided about intentions of government, though (Figure 17).

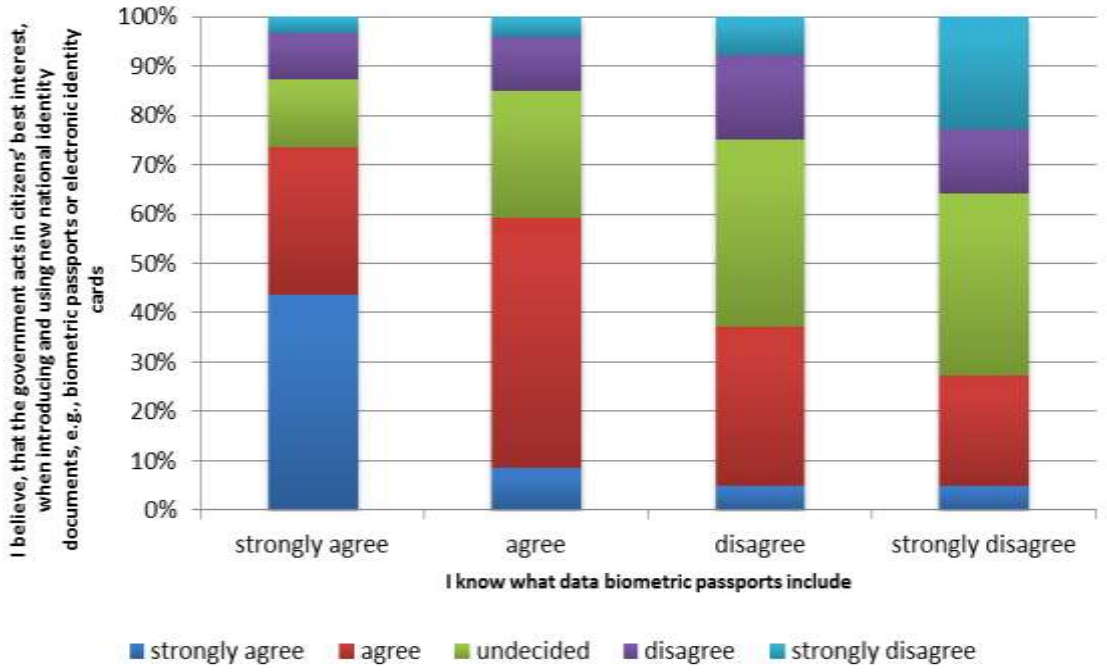
Figure 17. I believe, that the government acts in citizens’ best interest, when introducing and using new national identity documents, e.g., biometric passports or electronic identity cards



Source: ePassport web survey 2014, n=2,617

Citizens’ trust in government appears to be in correlation with their knowledge about ePassports. About 60-70% of the respondents who know what data ePassports include believe that government acts in citizens’ best interest when introducing and using new identity documents. The trust toward government in introducing and using new identity documents diminishes rather rapidly depending on the level of background knowledge on ePassports. Less than 30% of these respondents, who do not know at all what data ePassports include trust government activities in relation to new identity documents. (Figure 18)

Figure 18. Citizens' knowledge about ePassports and trust in government in introducing and using new national identity documents



Source: ePassport web survey 2014, N=1899.

7. The scenarios for potential future use of ePassports

7.1 Introduction to scenarios

In the following, we analyse public perceptions on a number of potential future uses of ePassports and related data. To do so, a number of statements were presented to the survey respondents. Each statement described a potential way for the establishment of identity, identity checks by public and private service providers, and identity checks by domestic and foreign border control authorities when travelling. The acceptability of scenarios was ranked on Likert scale (strongly agree, agree, undecided, disagree, strongly disagree).

The scenario statements used in the survey were not set to check the respondents' awareness on what governments currently do. These statements were meant to find out if the respondents would agree or disagree with such activities, should they surface in the future. The introduction to the survey as well as the comments on pages that present scenario questions also made it clear that this study includes hypothetical elements, and that the scenarios described do not imply that the European institutions or governments are officially considering adopting identity documents or data in such ways.

The survey data collected indicates that the respondents have understood scenario statements as we intended. For example close to 50% of the respondents (who had a personal view) indicated that they would accept the inclusion of eye iris and DNA data in a central identity documents database. Inclusion of DNA data into central ID database is clearly something no country does today, and it would be hard for the respondents not to know this, as no DNA data are collected together with passport applications.

7.2 Establishment of identity

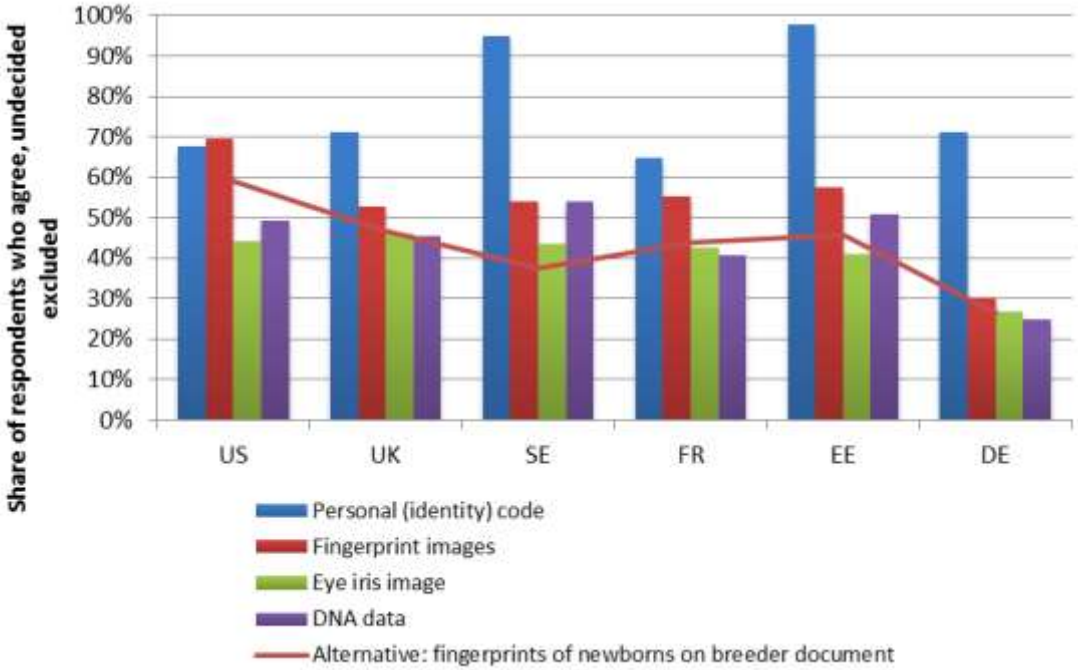
In many countries, breeder documents provided to newborns serve as the primary proof of identity, which acts as the main basis for issuing identity documents, such as passports or identity cards. However, breeder documents typically have, very little, if any, security features; and come in various forms and shapes in different countries. There is, therefore, a need to either update breeder documents with new security features, or to establish an alternative way of establishing the identity of newborns. The current ePassport survey tested public support for one potential approach: inclusion of the fingerprints of the newborns in their breeder documents, and recording this data in one centralised national registry.

It appears that the general public of the countries that rely on identity management via personal identity codes, (such as Sweden and Estonia) favours strongly this practice[5]. Support for this approach is not as strong in other countries, but still favours the use of personal identity codes rather than fingerprints, eye iris images or DNA data in the establishment of the identity of newborns. (Figure 19)

In regards to data collected in national registries for passports/identity cards, the public finds it quite acceptable that the government keeps personal identity codes and photos. There is also strong support for inclusion of fingerprint data in such databases, while the public acceptability of the inclusion of eye iris images and DNA data is much lower. (Figure 20)

[5] Personal identification codes were introduced nationwide in Sweden in 1947. Sweden was probably the first to cover the whole resident population of a country in such a way. The Social Security number in the United States is older, but it did not cover from the very beginning the whole population.

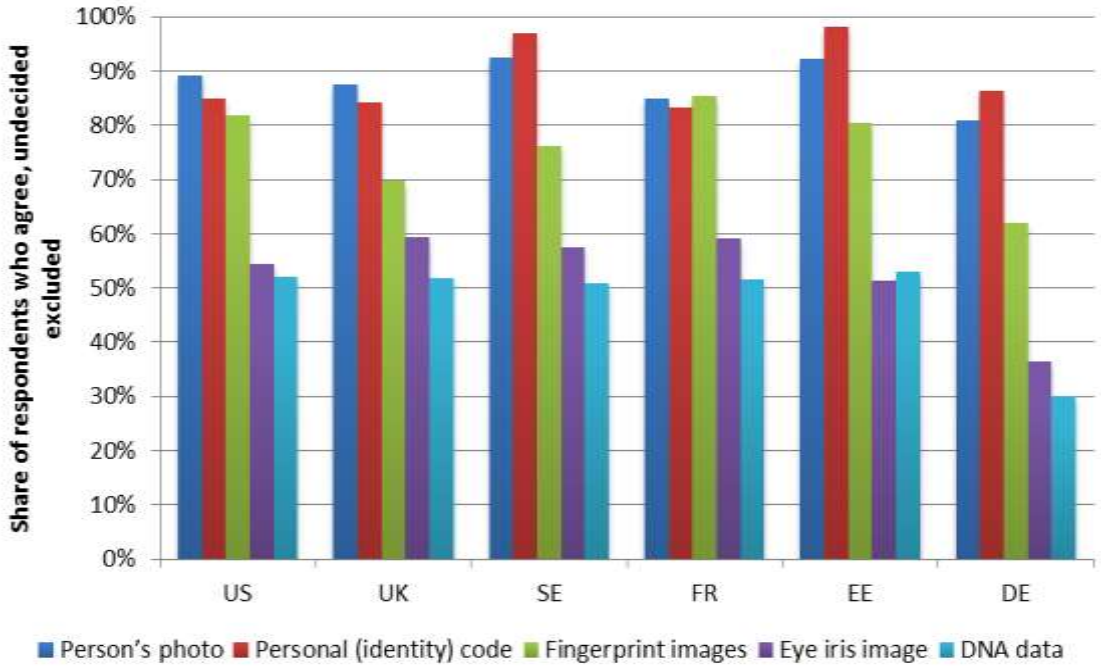
Figure 19. Government records the following data on all newborns in one centralised national registry, which serves later as the definitive basis for issuing passports and identity cards[6]



Source: ePassport web survey 2014, n=2,546.

[6] The vertical axis here and in the following figures reflects the share of those strongly agreeing and agreeing with the statement as compared to those of strongly disagreeing and disagreeing.

Figure 20. Government keeps in one national registry the following data on all passports and identity cards it has issued

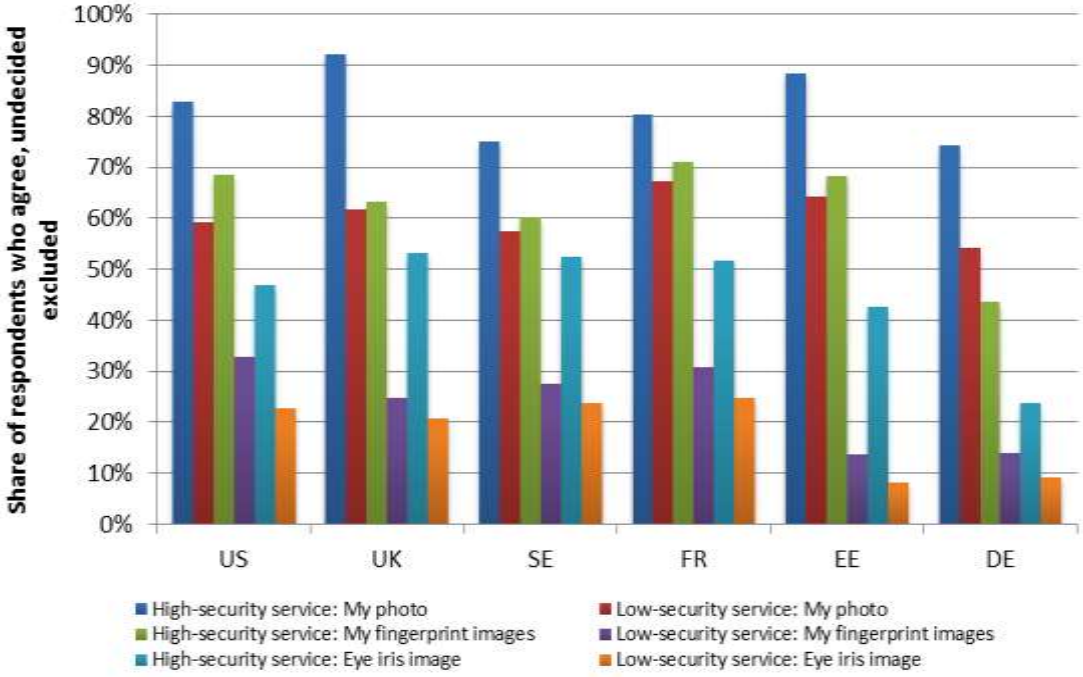


Source: ePassport web survey 2014, n=2,545.

7.3 Identity checks

The majority of the public agrees with the use of passport photos for identity checks for face-to-face delivery of high-security public service, such as notary service or declaring taxes. There is less support for the use of fingerprints or eye iris images for delivery of high security services. The acceptability of the use of biometrics in face-to-face delivery of low security services, such as public library services or applying for a permit, is notably lower. The majority of respondents are, in fact, against the use of fingerprints or eye iris images for such low security services that do not require the strong authentication of a person. (Figure 21)

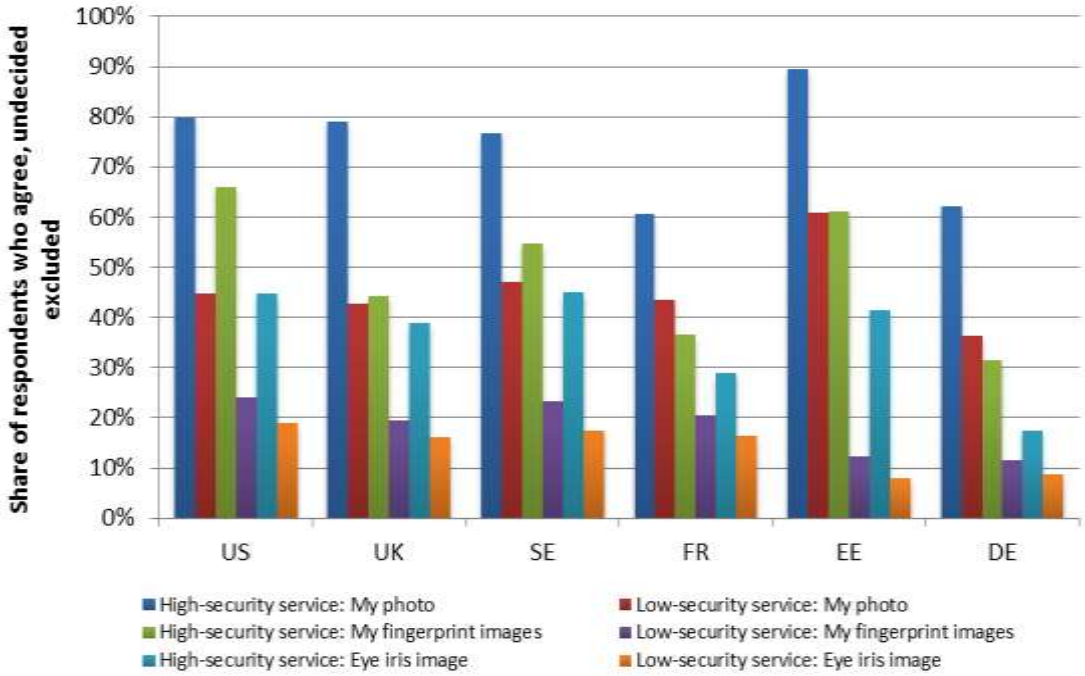
Figure 21. I agree that for the face-to-face delivery of a public service I am identified using any of the following



Source: ePassport web survey 2014, n=2,514.

The acceptability of the use of passport photos for face-to-face delivery of a high security business service, such as signing a bank contract or entering a high-security room, is also quite high, albeit somewhat lower than for public services. The public is, however, less willing to surrender their biometric data to business entities than public entities. The acceptability of business entities using fingerprint or eye iris images for delivery of low security services, such as entering an office building or signing a cable TV contract, is very low. (Figure 22)

Figure 22. I agree that for the face-to-face delivery of a business service I am identified using any of the following

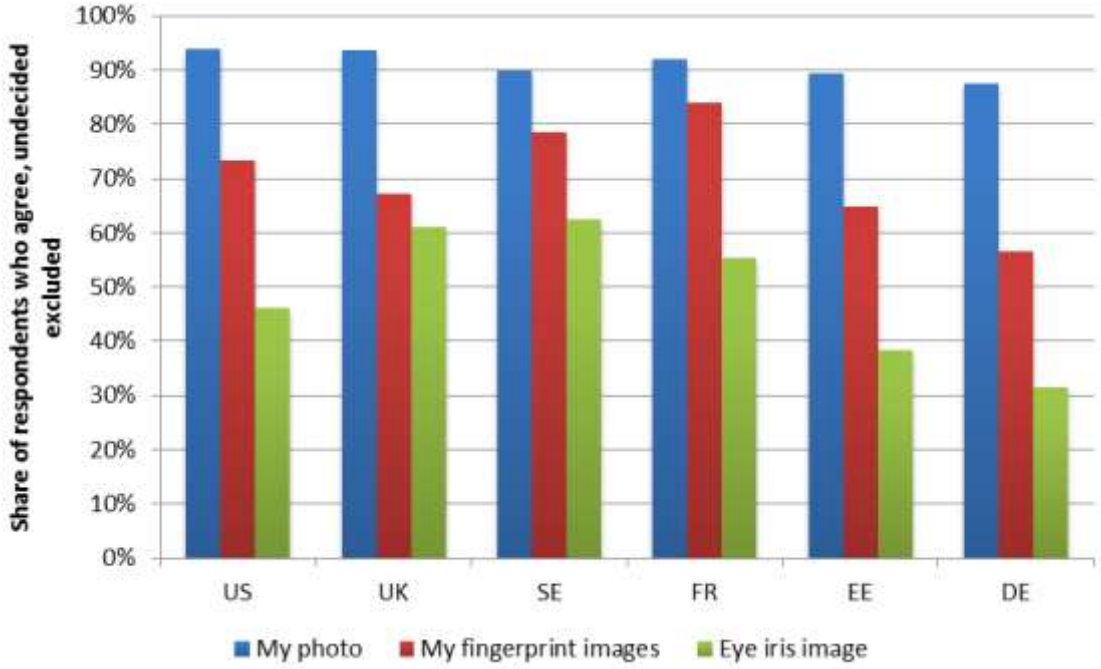


Source: ePassport web survey 2014, n=2,514.

7.4 Travel and border control

We indicated above that, depending on the specific country, between 20 and 50% of the respondents have used ABC gates so far (Figure 12, page 27). There is, nonetheless, broad support for the use of passport photos in automated border control gates. About ¾ of the respondents, who have an opinion in this matter, agree with ABC gates making use of fingerprint images. Subject to a specific country, between 30% and 60% of the respondents agree that ABC gates should make use of eye iris images for identity checks. (Figure 23)

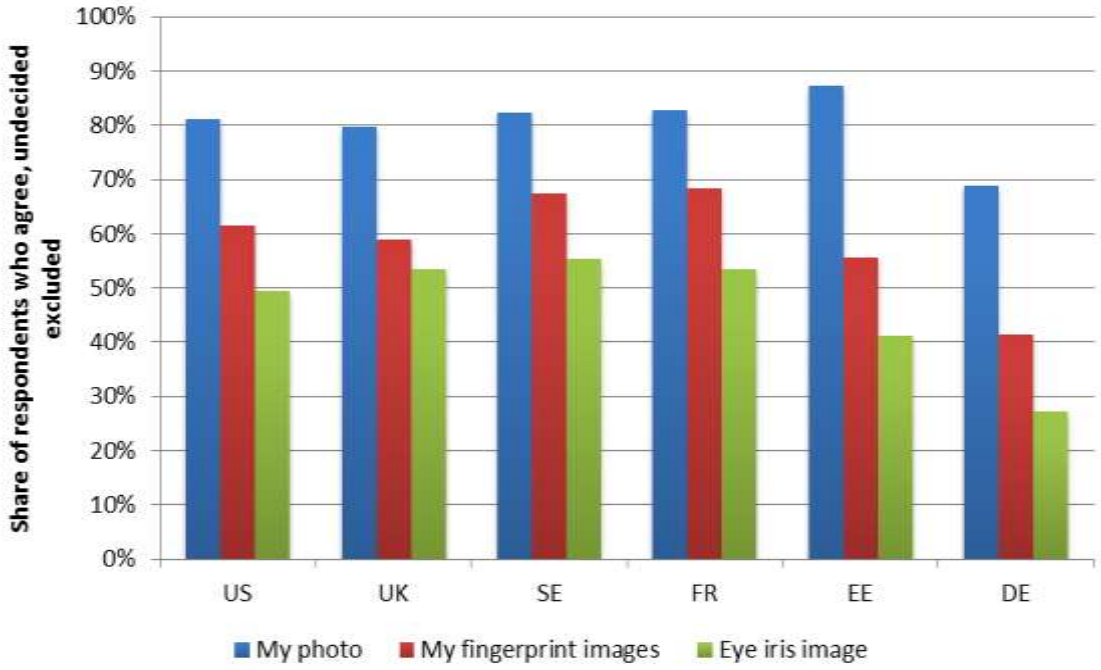
Figure 23. My identity is checked by automated border control gates using the following



Source: ePassport web survey 2014, n=2,493.

Technological advances may enable next generations of automatic border control systems to identify travellers on the move so that there will be no need stop on the border for an identity check. The social acceptability of such border control systems is slightly lower than the acceptability of ABC gates, but the acceptability of the use of photos is still quite high in this scenario. A substantial number of the respondents, who have an opinion in this matter, accept also the utilisation of fingerprint and eye iris images for non-stop identity checks. (Figure 24)

Figure 24. Border police captures my data and identifies me "on the move" so that there is no stopping on the border to check/obtain the following:

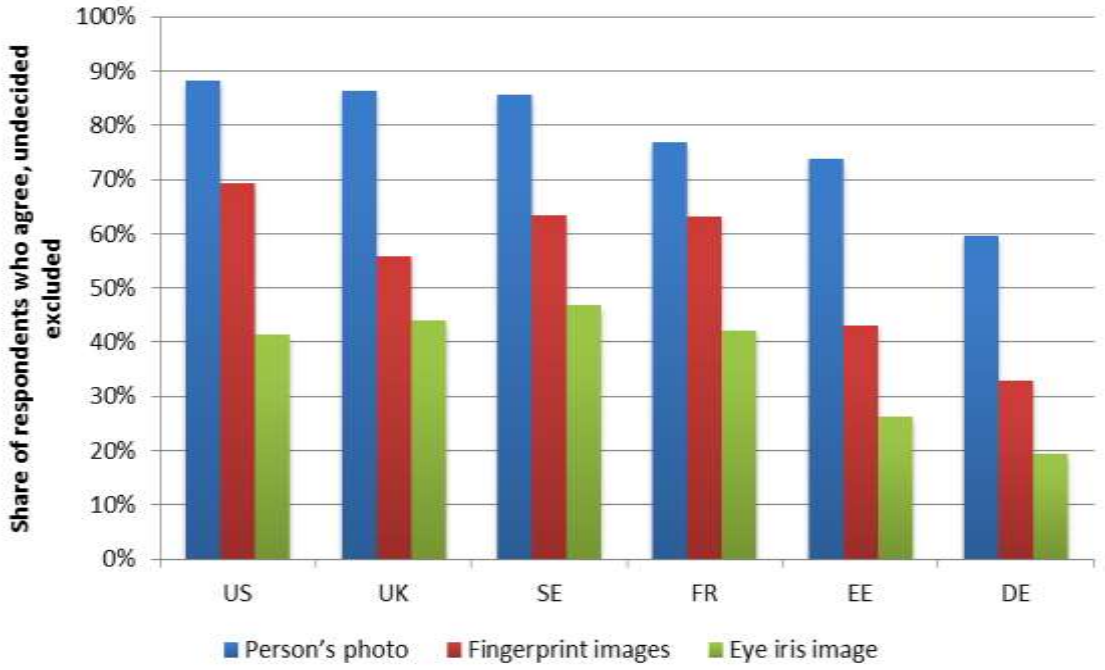


Source: ePassport web survey 2014, n=2,493.

Somewhat surprisingly, we find a lot of trust towards foreign governments[7]. The majority of the respondents, who have an opinion in this matter, agree that officials of a foreign country should record, when entering their country, travellers' photos. Very roughly, half of the respondents think that border police should record the travellers' fingerprints, and 20-45% would surrender eye iris images as well. (Figure 25)

[7] Most of the respondents might have replied on the basis of the country they visit the most or visited the most recently; the statement was a general.

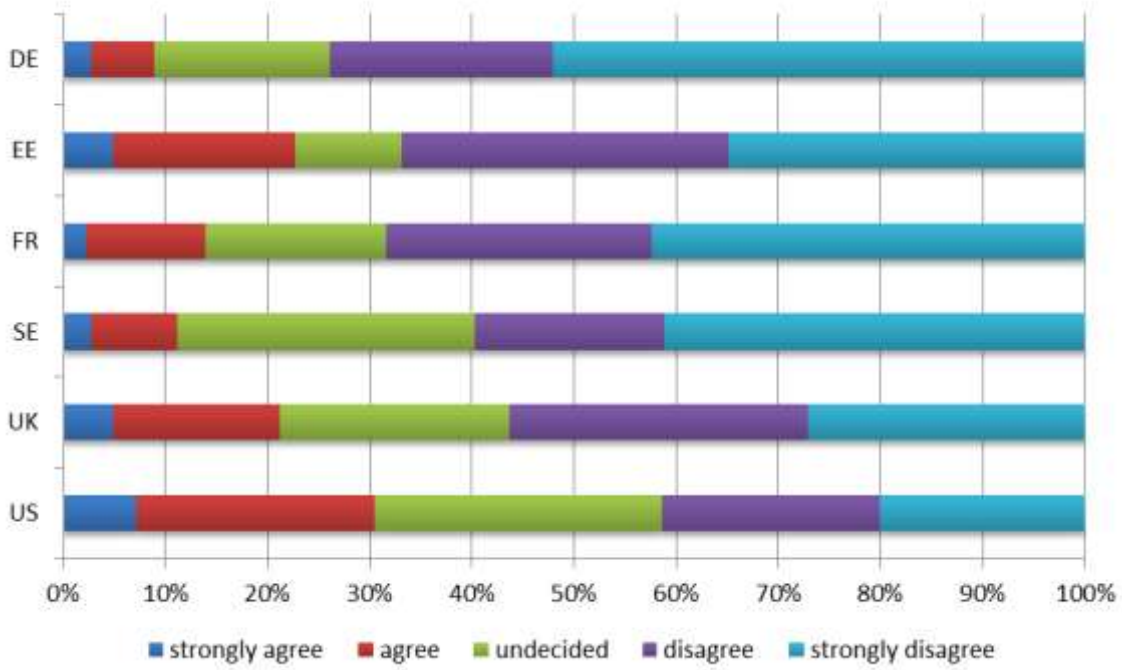
Figure 25. Authorities of a foreign country should record, on entry to their country, the following information



Source: ePassport web survey 2014, n=2,493.

There is, however, a strong opposition to the border control making use of photos or other information travellers have made publicly available on the Internet. German, Estonian and French respondents are especially strongly against this, while the American respondents hold a mixed view in this matter. (Figure 26)

Figure 26. During identity checks, such as border control, government officials can attempt to verify my identity by checking my photos, friends list and other public information I have made available on the Internet (e.g. on Facebook)



Source: ePassport web survey 2014, n=2,493.

7.5 Acceptance of biometric technologies

In analysing people's responses over various biometric technologies and scenarios, the following can be concluded.

First, people tend to have similar views on technology-wise similar scenarios. For example, regarding the establishment of identity we see that people who agree with the statement „Government records the fingerprints of newborns on their birth certificates, which serve later as the definitive basis for issuing passports and identity cards" (Q25) also tend to agree with the government recording fingerprint images on newborns in one centralised national registry, which serves later as the definitive basis for issuing passports and identity cards (Finger_26) (Figure 27). Similarly, those that agree with storing DNA data on all newborns in one centralised national registry (DNA_26) also agree with keeping DNA data in a national registry along the identity data (DNA_27). Or, eye iris data (Iris_26 and Iris_27). In identity establishment people who indicated they support personal identity code also support photos; people who support iris scans are more likely to support DNA. (Figure 27 in appendices)

Strong technology-based correlations can be observed regarding biometric-based identity checks in delivering services as well as for travel and border control processes. Here, however, eye iris and fingerprint images are accepted in a rather similar way for the identification processes, both for the public[8] as well as private[9] actors (Figure 28 in appendices) as well as for travel and border control processes[10] (Figure 29 in appendices).

[8] Q29 states that "I agree that for the face-to-face delivery of a public service that demands high security, such as notary service or declaring taxes, I am identified using any of the following"; Q31 states "I agree that for the face-to-face delivery of a public service that does not demand high security, such as public library services or applying for a permit, I am identified using any of the following

[9] Q30 states "I agree that a private company can use any of the following to identify me for the face-to-face delivery of a service demanding high security, such as signing a bank contract or entering a high-security room"; Q32 states "I agree that a private company can use any of the following information to deliver a

Additional analysis (Figure 30, Figure 31, Figure 32 in appendices) confirms that if people are convinced to use their biometric data for one application, they are more positive in using it for other purposes as well, although variations apply, especially for more sensitive applications. The correlations on those figures are always positive and occasionally very strong (above 0.7).

Overall, the public is fairly confident with the use of photos and personal identity codes in ePassports and related applications. However, it also follows that knowledge on what data biometric passports include (Q17) is only a minor factor in public acceptance of the use of biometrics in various scenarios. As it was discussed earlier, people who have higher knowledge on data included in ePassports have also higher expectations, while their perception of risks remains the same, and might diminish their use of biometrics in more sensitive scenarios.

The above analysis has demonstrated that the acceptability of the use of certain personal data or technologies (personal identity code, biometric data) varies significantly across scenarios. This seems to confirm that the acceptability of technology is a function of a trade-off between expected benefits and perceived risks (costs).

Furthermore, undecidedness varies according to technologies under discussion: about 20% of the population of the countries covered by this survey are undecided about the use of personal identity codes, 27% about use of fingerprints in passports, 32% are not sure, if it is a good idea to use eye iris images, and 33% are undecided about potential use of DNA data in various identity check scenarios.

service that does not demand high security, such as entering an office building or signing a cable TV contract"

[10] Q33: My identity is checked by automated border control gates using the following…; Q34: Border police captures my data and identifies me “on the move” so that there is no stopping on the border to check/obtain the following...; Q35: Authorities of a foreign country access the following data contained in my passport when checking my identity...;

Conclusions

The current study confirms that acceptance of novel ePassport technology is dependent on the technology itself as well as on broader social and cultural issues like trust towards the government and institutions initiating ePassports. On the basis of an original empirical study on public perceptions in relation to ePassports in Estonia, Germany, France, Sweden, United Kingdom and the United States of America, the following conclusions on the societal aspects of biometric technologies and ePassports are derived.

Performance expectancy, i.e. how using the technology will help a user to attain gains, is, according to the widely used Unified Theory of Acceptance and Use of Technology (UTAUT) model one of the key factors in influencing the adoption of a particular technology. The public of the six countries covered by this survey expects from ePassports improvements in protection from document forgery, accuracy and reliability of the identification of persons, and protection from identity theft. Broader public policy objectives, such as the fight against terrorism, human trafficking or illegal immigration are in the view of the public significantly less important in the context of the adoption and use of ePassports. Notably, those people who claim to have more detailed knowledge about ePassports have also higher expectations on the benefits of ePassports.

The risks that the public associates – rightfully or not – with novel identity documents reduces the acceptability of ePassports. The main risks the public associates with ePassports includes the possible use of personal information for purposes other than those initially stated, and covert surveillance. The concern regarding these two potential risks are high no matter what the level of knowledge on ePassports is. Compared to earlier studies, our research shows that issues of possible privacy invasion and abuse of information are much more perceived by the public.

The current study analysed also various scenarios for potential uses of ePassports and related data, such as establishment of identity, and identity checks in various situations, etc.

Some countries, such as Sweden and Estonia, rely strongly on personal identity codes in the establishment of identity and identity management. The general public of these countries accept broadly this way of creation and management and identity. The public of other countries has a more hesitant view on such use of personal identity codes, but favours still the use of personal identity codes rather than fingerprints, eye iris images or DNA data in the establishment of the identity of newborns. The public finds it generally acceptable that the government keeps the data on national identity documents in one national registry, which includes also the respective persons' photos and personal identity codes. Support for the inclusion of fingerprint data in such databases is slightly lower, while the acceptability of the inclusion of eye iris images and DNA data in such a registry is significantly lower.

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 for using eye iris images 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.

Automated border control (ABC) gates, which is perhaps the most widely used ePassport application, have been used by close to one half of the respondents in the United Kingdom and the United States, but the experience of ABC gates remains so far much more limited in the rest of the countries. There is, nonetheless, a broad support for the use of passport photos and fingerprints in automated border control gates.

Surprisingly, respondents to this survey find it also acceptable that foreign authorities record on border entry travellers' photos and fingerprint images. There is, however, a strong opposition to the border control potentially making use of photos or other information travellers have themselves made publicly available on the Internet.

The public of the six countries covered by this survey is not well informed about the personal data that government or private companies collect on them. They have only limited knowledge of the electronic data and functions ePassports include, and often have no clear opinion on various potential uses for ePassports and related personal data. We find, quite as expected, that younger persons judge themselves to be more knowledgeable about the data ePassports include and the government collects personally on them. While

this is the case, people with relatively higher levels of education and those holding higher level (management) jobs consider themselves less informed.

There appears to be a weak correlation between a persons' level of knowledge about ePassports and their willingness to accept the use of advanced biometrics, such as fingerprints or eye iris images, in different identity management and identity checking scenarios. Furthermore, the public becomes more undecided about ePassport applications as we move from the basic state of the art towards more advanced biometric technologies in various scenarios: about 20% of the population of the countries covered by this survey are undecided about the use of personal identity codes, 27% about use of fingerprints in passports, 32% are not sure, if it is a good idea to use eye iris images, and 33% are not sure about potential use of DNA data in identity documents.

As the awareness is low, citizens' belief in government benevolence, i.e. the belief that the government acts in citizens' best interest, comes out as an important factor in the overall context. Furthermore, people who are informed about ePassports and the data they include, often believe that the government acts in citizens' best interest when introducing and using new identity documents, such as ePassports or electronic ID cards. There is, thereby, a strong democratic argument for informing the public properly even if this will not lead always to greater acceptability of certain specific technologies or their applications.

As preliminary recommendations, to be detailed in FIDELITY Deliverable D2.4, the following aspects deserve more attention. First, 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 lead necessarily to higher acceptability 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.

The above analysis has demonstrated that the acceptability of the use of certain personal data or technologies (personal identity code, biometric data) varies significantly across scenarios. This seems to confirm 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 current 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 as well. Thus, the successful pathway to greater acceptability of the use of advanced biometrics in ePassports should start from the introduction of perceivably high-benefit and low-risk applications.

Finally, the development of an ePassport dissemination and public relations strategy should start from the identification of specific demographic groups according to their level of understanding and acceptance of the scenarios for using ePassports.

8. Bibliography

Alterman, A. (2003). A Piece of Yourself: Ethical Issues in Biometric Identification. *Ethics and Information Technology* 5 (3).

Acquisti, A., Grossklags, J. (2007). What can behavioral economics teach us about privacy? In: A. Acquisti, S. Gritzalis, S. Di Vimercati, C. Lambrinoudakis (Eds.) *Digital Privacy: Theory, Technologies, and Practices*, Auerbach Publications.

Ash, J. (1997). Factors for Information Technology Innovation Diffusion and Infusion in Health Sciences Organizations: A Systems Approach. Portland State University.

Bilbao-Osorio, B., S. Dutta, B. Lanvin (eds.) (2014) *Global Information Technology Report*, World Economic Forum: Geneva.

Brandtz, P.B., Heim, J., Karahasanovi, A. (2011). Understanding the new digital divide-A typology of Internet users in Europe. *Int. J. Hum.-Comput. Stud*., 69(3).

Brey, P. A. E. (2012). Anticipating ethical issues in emerging IT. *Ethics of Information Technology*, 14 (4).

Carlussio, D., K. Lemke-Rust, C. Paar, A.-R. Sadeghi (2007). E-Passport: The Global Traceability or How to Feel Like a UPS Package. In J. K. Lee, O. Yi, M. Yung (Eds) *Information Security Applications*. 7th International Workshop, WISA 2006, Jeju Island, Korea, August 28-30, 2006, Revised Selected Papers. Springler.

Curtis, L., Edwards, C., Fraser, K. L., Gudelsky, S., Holmquist, J., Thornton, K., et al. (2010). Adoption of social media for public relations by nonprofit organizations. *Public Relations Review*, 36 (1).

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology, *MIS Quarterly*, 13(3).

European Biometrics Forum (2006). *Report on Security & Privacy in Large Scale Biometric Systems.* Retrieved from: http://is.jrc.ec.europa.eu/documents/SecurityPrivacyFinalReport.pdf.

Eurostat (2014) *Statistics database*, http://epp.eurostat.ec.europa.eu/portal/page/portal/eurostat/home.

Fast and Trustworthy Identity Delivery and Check with ePassport Leveraging Travellers Privacy (FIDELITY) (2010). *Proposal part B*. Work Program SEC-2011.3.4-1 Security of biometric data and travel documents.

Future of Identity in the Information Society (FIDIS) (2009). *D3.10: Biometrics in identity management*. Retrieved from http://www.fidis.net/resources/deliverables/hightechid/#c2057.

Gavison, R. (1980). Privacy and the Limits of Law. *The Yale Law Journal* 89.

Hallinan, D., M. Friedewald, and P. McCarthy (2012). Citizens' Perceptions of Data Protection and Privacy. *Computer Law and Security Review* 28 (3).

Hoepman, J.-H., E. Hubbers, B. Jacobs, M. Oostdijk, R. W. Schreur (2006). *Crossing Borders: Security and Privacy Issues of the European e-Passport.* 1st Int. Workshop on Security, Kyoto, Japan, October 23-24. Retrieved from: http://arxiv.org/abs/0801.3930.

Institute for Prospective Technological Studies (2005). *Biometrics at the Frontiers: Assessing the Impact on Society.* For the European Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs (LIBE). Retrieved from: http://is.jrc.ec.europa.eu/pages/TFS/Biometrics.html.

Jain, A., Bolle, R., Pankanti, S. (1996). Introduction to Biometrics. In A. Jain, R. Bolle, S. Pankanti (eds.), *Biometrics, personal identification in networked society.* Springer: New York.

Jain, A. Pankanti, S., Prabhakar, S., Hong, L., Ross, A., Wayman, J. L. (2004). Biometrics: A Grand Challenge. *Proceedings of International Conference on Pattern Recognition*. vol. II, Cambridge. Retrieved from: http://www.cse.msu.edu/~rossarun/BiometricsTextBook/Papers/Introduction/Jainetal_BiometricsGrandChallenge_ICPR04.pdf

Juels, A., D. Molnar, D. Wagner (2005). Security and Privacy Issues in E-passports. *SECURECOMM '05 Proceeding from the First International Conference on Security and Privacy for Emerging Areas in Communications Networks.* IEEE Computer Society: Washington. Retrieved from: http://eprint.iacr.org/2005/095.pdf.

Kupfer, J. (1987). Privacy, Autonomy, and Self-concept. *American Philosophical Quarterly* 24.

King, W.R., He, J. (2006). A meta-analysis of the technology acceptance model. *Information & Management*, 43 (6).

Lederer, A.L., Maupin, D.J., Sena, M.P., Zhuang, Y. (2000). The technology acceptance model and the world wide web. *Decision Support Systems*, 29.

Legris, P., Ingham, J., Collerette, P. (2003). Why do people use information technology? A critical review of the technology acceptance model. Information & Management, 40 (3).

Lin, C.-P. and Anol, B. (2008). Learning online social support: An investigation of network information technology based on utaut. *CyberPsychology & Behavior,* 11 (3).

Lodge, J. (2010). Quantum surveillance and "shared secrets". A biometric step too far? Justice and Home Affairs. *CEPS Liberty and Security in Europe.*

LSE (2010). *LSE Identity Project*, The London School of Economics and Political Science, http://www.identityproject.lse.ac.uk.

Lyon, D. (2003). Surveillance as social sorting: Computer codes and mobile bodies. In D. Lyon (Ed.), *Surveillance as social sorting: Privacy, risk and automated discrimination*. Routledge: London.

Lyon, D. (2008). Biometrics, identification and surveillance. *Bioethics*, 22 (9).

Manson, N. C., O'Neill, O. (2007). *Rethinking informed consent in bioethics*. Cambridge University Press: Cambridge.

Mathieson, K. (1991). Predicting User Intentions: Comparing the Technology Acceptance Model with the Theory of Planned Behavior. *Information Systems Research*, 2 (3).

Moore, Adam (2008) 'Defining privacy'. *Journal of Social Philosophy*, 39 (3).

Mordini, E., Massari, S. (2008). Body, biometrics and identity. *Bioethics*, 22 (9).

Nissenbaum, H. (2010). *Privacy in Context. Technology, Policy, and the Integrity of Social Life*. Stanford University Press: Stanford, California.

Ng-Kruelle, G., Swatman, P. A., Hampe, J. F., Rebne, D. S. (2006). Biometrics and e-Identity (e-Passport) in the European Union: End-user perspectives on the adoption of a controversial innovation. *Journal of Theoretical and Applied Electronic Commerce Research* 1 (2).

Pavone, V., Degli Esposti, S. (2012). Public assessment of new surveillance-oriented security technologies: Beyond the trade-off between privacy and security. *Public Understanding of Science* 21 (5).

Perakslis, C., Wolk, R. (2006). Social Acceptance of RFID as a Biometric Security Method. *IEEE* 25 (3).

Pohjolan Sanomat (2012). Ulkomaalaisten sormenjäljet päätyvät rikostutkijoille kiertotietä. 4 May. Retrieved from:
http://www.pohjolansanomat.fi/Kotimaa/1194741199613/artikkeli/ulkomaalaisten+sormenjaljet+paatyvat+rikostutkijoille+kiertotieta.html

Regan, P. (1995). *Legisating Privacy. Technology, Social Values, and Public Policy*. University of North Carolina Press : Chapel Hill and London.

Reiman, J. (1984). Privacy, Intimacy, and Personhood. In F. D. Schoeman *Philosophical Dimensions of Privacy: An Anthology.* Cambridge University Press: Cambridge 1984.

Rössler, B. (2005). *The value of Privacy.* Polity Press: Cambridge.

Schouten, B., Jacobs, B. (2008). Biometrics and their use in e-passports. *Journal for Image and Computer Vision. IMAVIS* 2726, June.

Solove, D. J. (2007) "I've got nothing to hide" and other misunderstandings of privacy. *San Diego Law Review* 44.

Sprokkereef, A., de Hert, P. (2007). Ethical Practice in the use of biometric identifiers within the EU. *Law, Science and Policy*, vol. 3.

Stahl B. C., Heersmink R., Goujon P., Flick C., Hoven van den J., Wakunuma K. J., Ikonen V., Rader M. (2010). Identifying the Ethics of Emerging Information and Communication Technologies: An Essay on Issues, Concepts and Method. *International Journal of Technoethics*,1 (4).

Steeves, V. (2009). Reclaiming the Social Value of Privacy. In I. Kerr, V. Steeves and C. Lucock (Eds.) *Privacy, Identity and Anonymity in a Network World: Lessons from the Identity Trail*. Oxford University Press: New York.

Sutrop, Margit and Katrin Laas-Mikko (2012). From identity verification to behaviour prediction: ethical implications of second-generation biometrics. *Review of Policy Research* 29 (1).

Van der Ploeg, I. (2005). The Politics of Biometric Identities. Normative aspects of automated social categorisation. *BITE, policy paper no 2*. Retrieved from: http://www.biteproject.org/documents.asp.

Van der Ploeg, I. (2006) Borderline Identities: The Enrollment of Bodies in the Technological Reconstruction of Borders. In T. Monahan (Ed.) *Surveillance and Society: Technological Politics and Everyday Life*, Routledge: New York.

Venkatesh, V. (2000). Determinants of Perceived Ease of Use: Integrating Control, Intrinsic Motivation, and Emotion into the Technology Acceptance Model" *Information Systems Research*, 11(4)..

Venkatesh, V., Morris, D. (2003). User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly* 27 (3).

Venkatesh V., Thong J.Y.L., and Xu, X., (2012). Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology. *MIS Quarterly*, 36 (1).

Williams, B. (1973). *Problems of the self*. Cambridge University Press: Cambridge.

Appendix A : Appendices

Table 2. Model parameters for demographic variables and awareness about the data private companies collect

With the development and application of logistic regression (logit regression) model, a probabilistic statistical classification model on the significance level 0.1, the following model parameters were derived regarding the profile of the strongly (dis)agreeing respondents. Data is related with the following base values: Country: DE; Education: Basic Education; Occupation: Elementary Worker.

Estimate	Estimate[11]	Pr[12]
(Intercept)	-50,368	0,018
Year.of.Birth	0,025	0,02
(Country.1)EE	0,318	0,562
(Country.1)FR	1,192	0,007
(Country.1)SE	0,336	0,519
(Country.1)UK	0,885	0,065
(Country.1)US	1,238	0,007
(Education)higher education	**-1,987**	0,039
(Education)primary education	-1,605	0,153
(Education)secondary education	-1,356	0,161
(Education)vocational education	-1,354	0,159
(Occupation)Enterpreneur	0,701	0,347
(Occupation)Mid-level manager	**1,771**	0,009
(Occupation)Mid-level professional	0,871	0,159
(Occupation)Service and sales worker	0,363	0,576
(Occupation)Skilled worker	0,96	0,132
(Occupation)Top level manager	**4,319**	0
(Occupation)Top level professional	0,883	0,204

Source: Logit regression model based on ePassport web survey 2014, n=356.

[11] Refers to the estimated coefficients in proportion to reference level in the logit regression model used to predict a binary response for strongly agreeing (value 1.0) or disagreeing (value 0) about the statement “I have enough information about the data different private companies collect on me personally”.
[12] Refers to corresponding p-values in proportion to reference level.

Table 3. Model parameters for demographic variables and awareness about the data the government collects

With the development and application of logistic regression (logit regression) model, a probabilistic statistical classification model on the significance level 0.1, the following model parameters were derived regarding the profile of the strongly (dis)agreeing respondents. Data is related with the following base values: Country: DE; Education: Basic Education; Occupation: Elementary Worker.

	Estimate	Pr
Intercept	-58,534	0,012
Year.of.Birth	0,029	0,015
Country EE	1,237	0,018
Country FR	0,79	0,117
Country SE	0,066	0,925
Country UK	1,109	0,038
Country US	1,052	0,035
Education higher education	**-1,665**	0,032
Education primary education	-0,852	0,35
Education secondary education	-1,52	0,055
Education vocational	-1,27	0,107
Occupation Enterpreneur	1,113	0,155
Occupation Mid-level manager	**1,383**	0,072
Occupation Mid-level professional	0,587	0,407
Occupation Service and sales worker	0,544	0,46
Occupation Skilled worker	1,508	0,039
Occupatihon Top level manager	**3,07**	0,001
Occupation Top level professional	0,976	0,215

Source: Logit regression model based on ePassport web survey 2014, n=411.

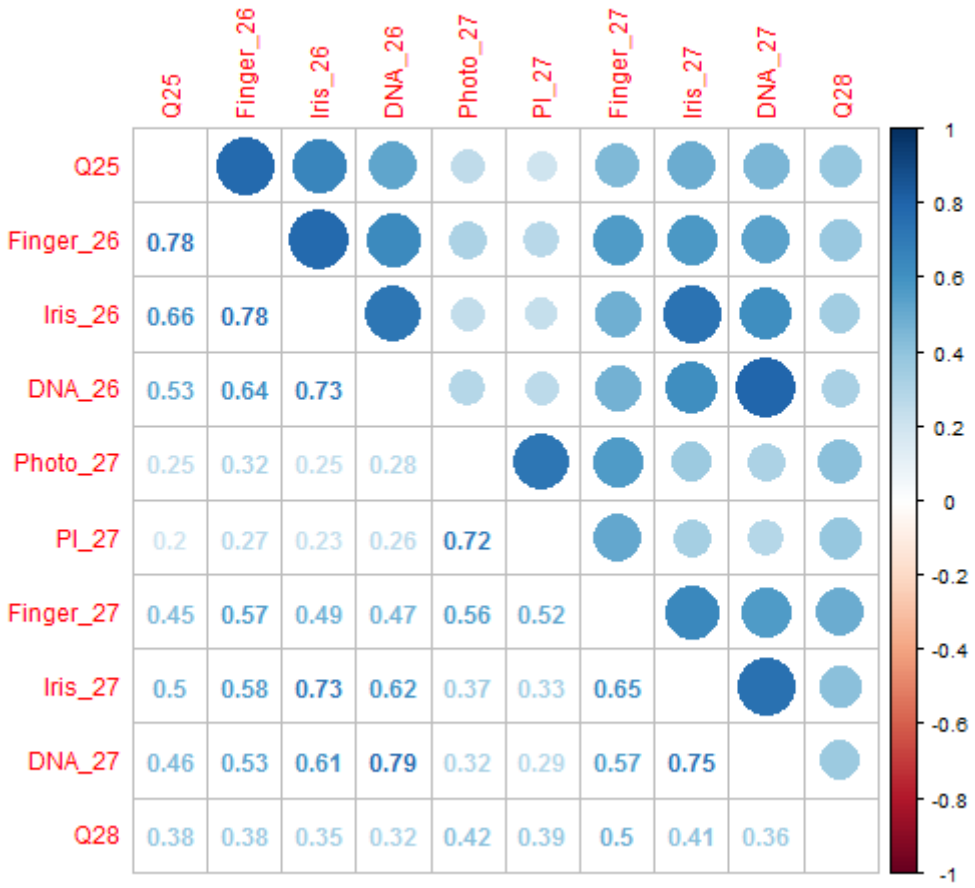
Table 4. Model parameters for demographic variables and awareness about the data biometric passports include

With the development and application of logistic regression (logit regression) model, a probabilistic statistical classification model on the significance level 0.1, the following model parameters were derived regarding the profile of the strongly (dis)agreeing respondents. Data is related with the following base values: Country: DE; Education: Basic Education; Occupation: Elementary Worker.

	Estimate	**Pr**
(Intercept)	-38,048	0,088
Year.of.Birth	0,019	0,09
(Country)EE	0,658	0,192
(Country)FR	-0,388	0,407
(Country)SE	-2,089	0
(Country)UK	-0,727	0,141
(Country)US	-0,973	0,025
(Gender) 2	**-1,01**	0
(Occupation)Enterpreneur	0,74	0,36
(Occupation)Mid-level manager	**1,992**	0,009
(Occupation)Mid-level professional	0,673	0,345
(Occupation)Service and sales worker	0,315	0,679
(Occupation)Skilled worker	0,562	0,483
(Occupation)Top level manager	**2,696**	0,006
(Occupation)Top level professional	**1,579**	0,041

Source: Logit regression model based on ePassport web survey 2014, n=328.

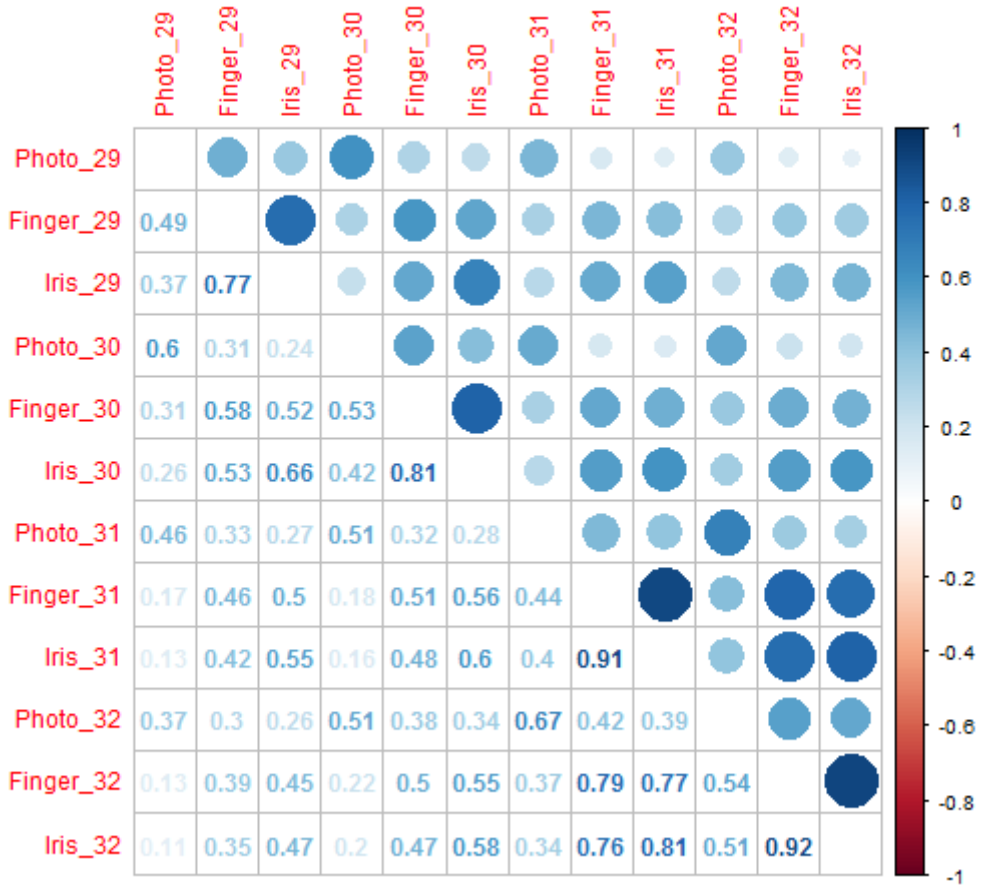
Figure 27. Correlation matrix regarding establishment of identity



	Q25	Finger_26	Iris_26	DNA_26	Photo_27	PI_27	Finger_27	Iris_27	DNA_27	Q28
Q25										
Finger_26	0.78									
Iris_26	0.66	0.78								
DNA_26	0.53	0.64	0.73							
Photo_27	0.25	0.32	0.25	0.28						
PI_27	0.2	0.27	0.23	0.26	0.72					
Finger_27	0.45	0.57	0.49	0.47	0.56	0.52				
Iris_27	0.5	0.58	0.73	0.62	0.37	0.33	0.65			
DNA_27	0.46	0.53	0.61	0.79	0.32	0.29	0.57	0.75		
Q28	0.38	0.38	0.35	0.32	0.42	0.39	0.5	0.41	0.36	

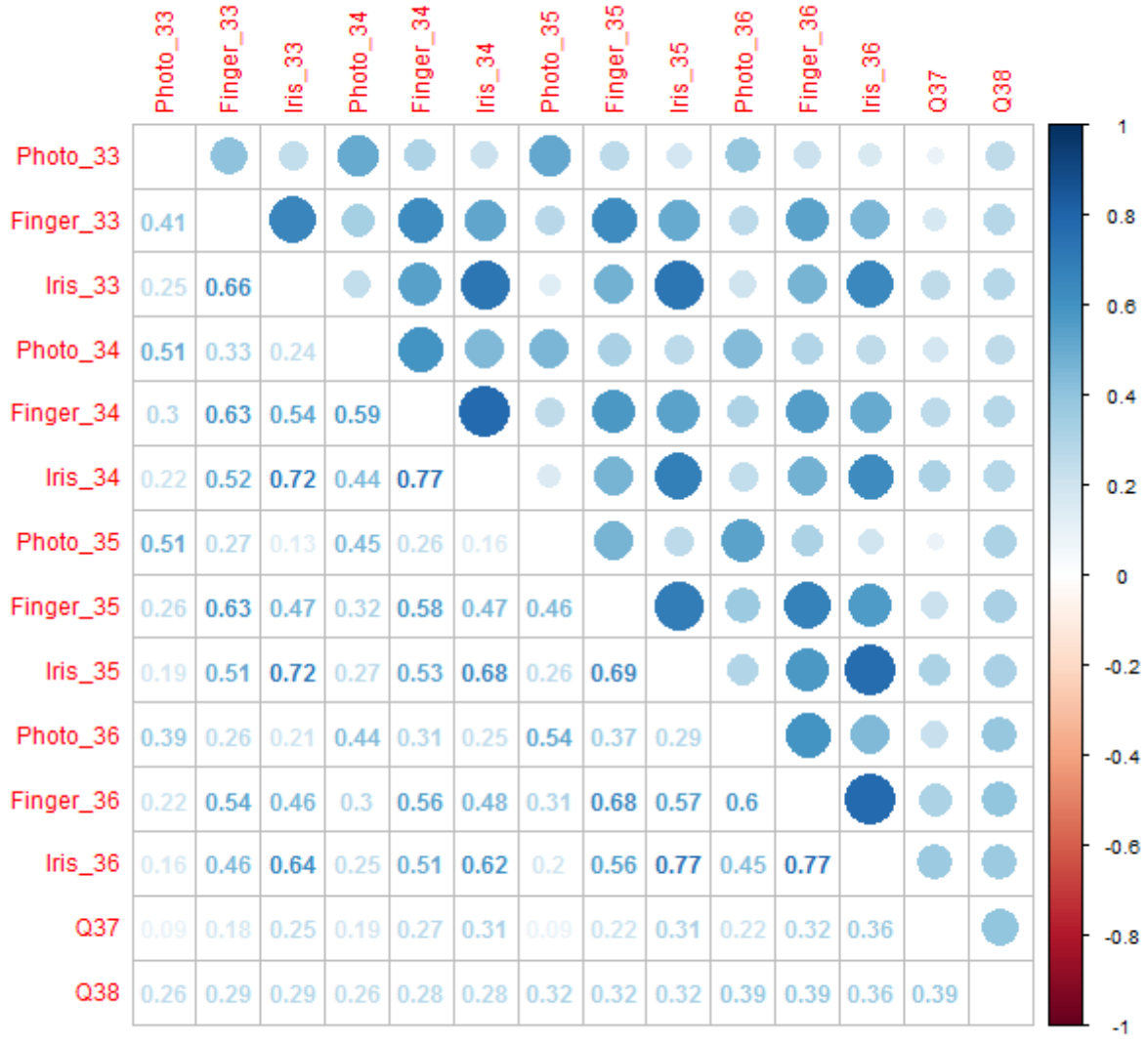
Source: ePassport web survey 2014 , n=2,477.

Figure 28. Correlation matrix regarding identity check



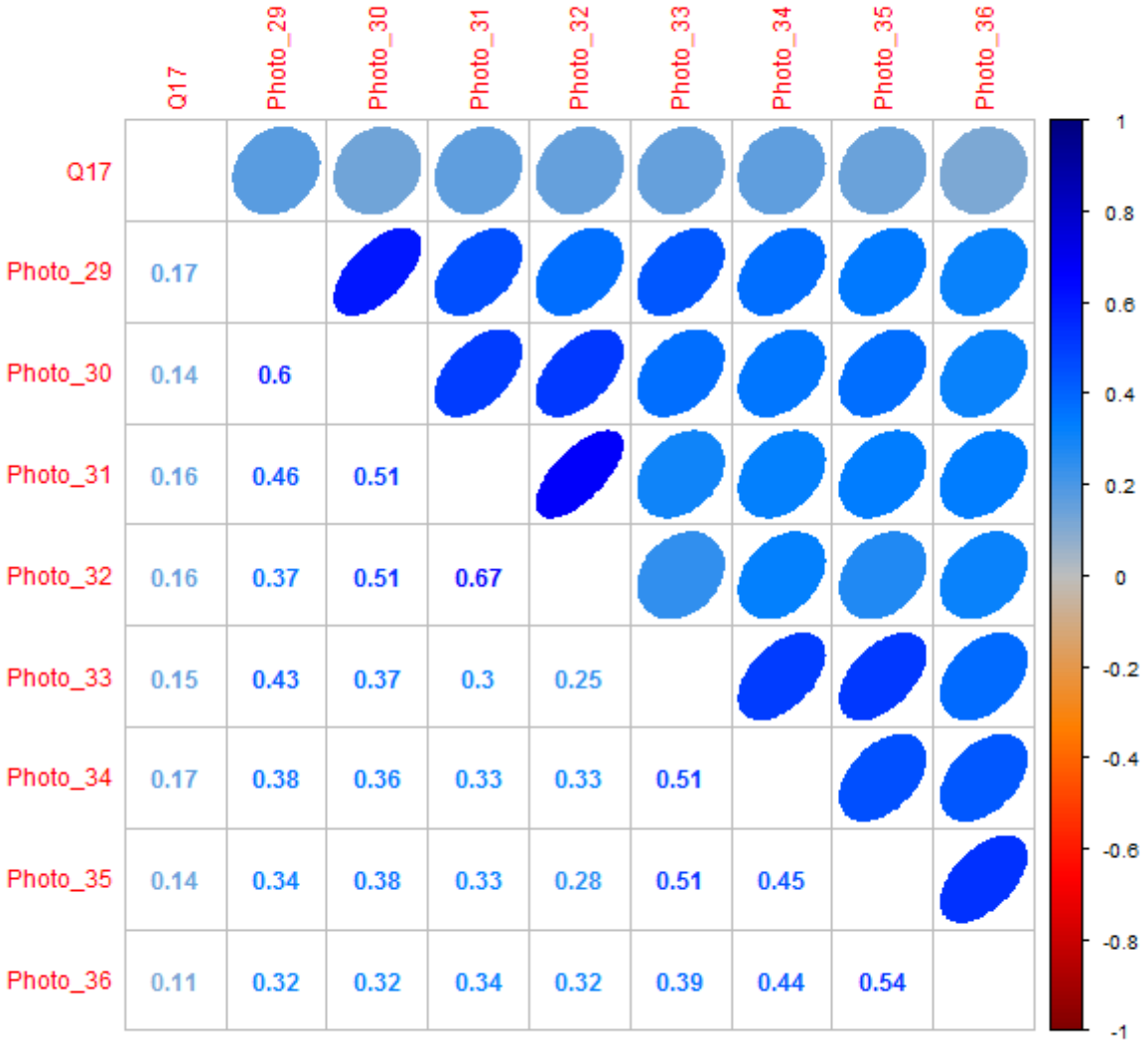
Source: ePassport web survey 2014, n=2,477.

Figure 29. Correlation matrix regarding travel and border control



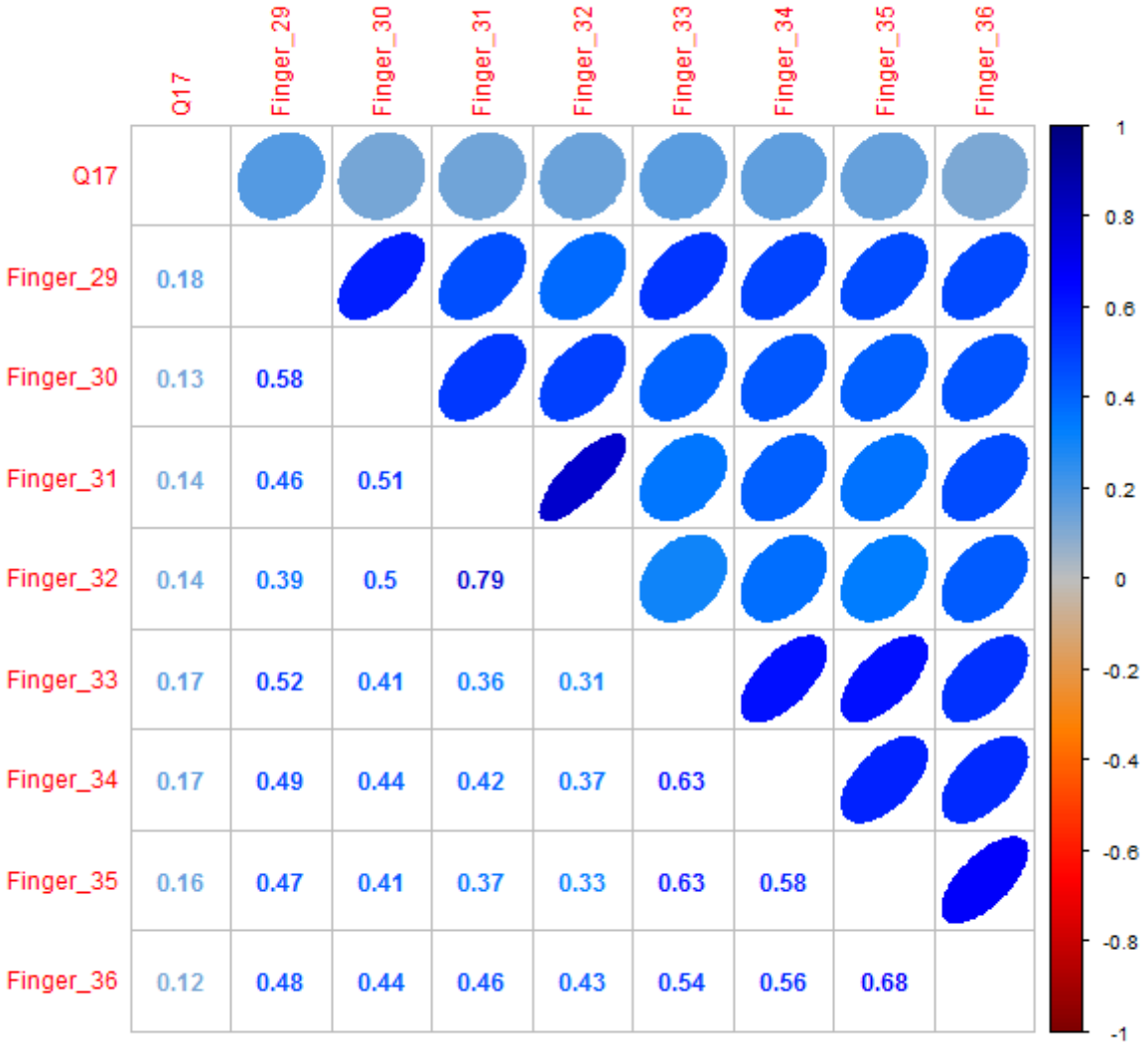
Source: ePassport web survey 2014, n=2,477.

Figure 30. Correlation matrix regarding photo images



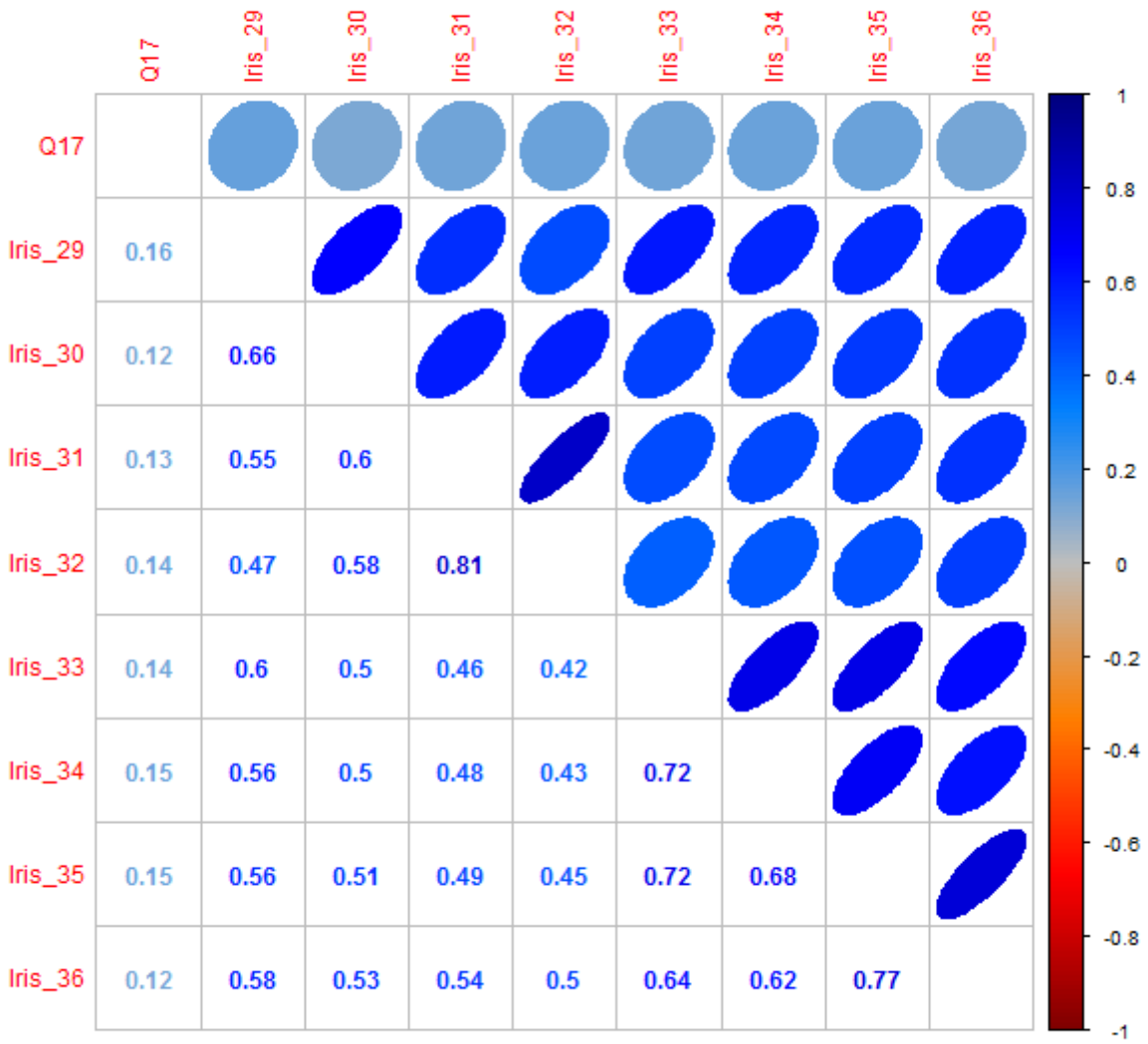
Source: ePassport web survey 2014, n=2,477.

Figure 31. Correlation matrix regarding fingerprint images



Source: ePassport web survey 2014, n=2,477.

Figure 32. Correlation matrix regarding eye iris images



Source: ePassport web survey 2014, n=2,477.