Social Acceptance of ePassports

Marek Tiits, Tarmo Kalvet and Katrin Laas-Mikko

Institute of Baltic Studies
Lai 30, 51005 Tartu, Estonia
marek@ibs.ee, tarmo.kalvet@ttu.ee, katrin.laas-mikko@sk.ee

Abstract: Using large-scale web survey in six countries we study the societal readiness and acceptance of specific technology options in relation to the potential next generation of ePassports. We find that the public has 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. Still, the public expects from ePassports improvements in protection from document forgery, accuracy and reliability of the identification of persons, and protection from identity theft. 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. Compared to earlier studies, our research shows that issues of possible privacy invasion and abuse of information are much more perceived by the public. There is 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. 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.

1 Introduction

Broad societal acceptance is crucial if the deployment of new forms of technology 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 set aside to ensure security is preserved, and the risk of function creep (i.e. personal data could be used by data-processing bodies beyond the originally intended and communicated scope) [LS10].

The current paper looks at the ePassports – combined paper and electronic passport issued by the government that contains biometric information. Previously, only limited

empirical research has been done on public acceptance and perceptions in relation to ePassports. Those surveys are fairly general in terms of the societal benefits and risks of ePassports and neither are they applying comprehensive theoretical technology acceptance models available.

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 regular citizens 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. Based on the above, we detail in chapter three our own research framework for analysing ePassport readiness empirically in selected countries. The analysis of the results of the field work is presented in chapter four. We discuss the findings and conclusions in chapter five.

2 Societal issues regarding ePassports

Some of the most important social issues that have been raised in the literature in relation to the adoption of ePassports are related to the need for ePassports, public trust and social acceptability of ePassports, privacy and function creep, and public perception.

First, the direct aim of biometric technology and ePassports is to enhance the reliability of identification. Biometrics is the scientific distsipline of methods of establishing the identity of individual based on the physical, chemical or behavioural attributes of the person (or a combination of them) that are unique to a specific human being [JR08].

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. And, biometrics as a form of identity technology have many advantages [SL12].

Second, trust is important for the adoption of new forms of technology. In the mid- and long term public disappointment regarding the efficiency of technology (e.g. inconvenience on borders because of false acceptance rates, device deployment difficulties etc. [PW06]) 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 enforce fears about a 'surveillance state', even if these fears are unsubstantiated. Trust, however, 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 [Ng06]. The first concern relates to insufficient public information about the role of biometrics and ePassports [Eb06, If05]. Another, related, prominent issue in debates about biometric technology and ePassports concerns the issue of function creep. Function creep describes the phenomenon where the use of technology or system is extended/shifted beyond its original purpose and context, and often also related 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 citizen [e.g., MM08].

Third, from the literature follows that 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 from biometric databases, eavesdropping or cloning of RFID chips, identity theft and tracking of passport holders (e.g., Ho06]). 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 [Al03]. Biometric data are irreversible – they cannot be revoked, because they are unique. If such data is copied and forged or confused, the data owner will have a great difficulty proving that he or she is unconnected to the instances of use of the data.

There are only limited studies on the public perception on biometrics and ePassports. Eurobarometer 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 [Eb11]. However, this data set does not go at any length into details on ePassports. Ng-Kruelle and colleagues [Ng06] conducted a survey (with 303 respondents) among EU citizens in selected countries 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. Several other surveys [e.g., PW06] show similar results. 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 [PW06].

3 Unified theory of acceptance and use of technology

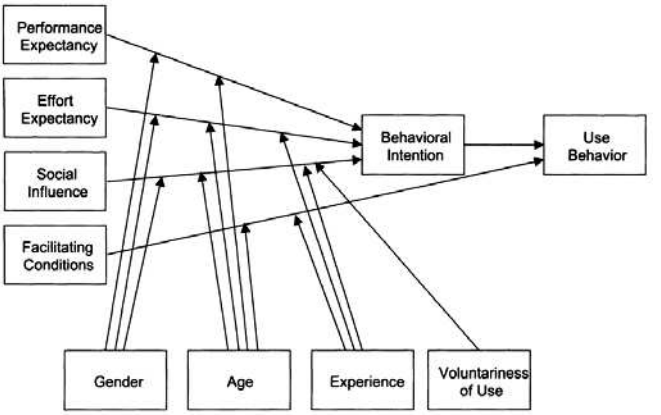
Technology acceptance is an important research issue and the development of models for technology acceptance has received increasing attention in academic literature. The general point of departure for these models is that there are a number of factors that will influence the user as to whether or not 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., [As97], [Ma91], [Ve00]).

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 [Da89]. Generally speaking, TAM is a theoretical model used in different contexts to help understand and explain the use of information technologies (see [Le00], [KH06]).

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 [VM03] and developed further in [VTX12].

UTAUT first explains user intentions to use a technology and then identifies their subsequent usage behaviour. 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: [VTX12, 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 perfofrmance" [VTX12, 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 future consideration. 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, knowledge on security measures such as access control mechanisms 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” [VTX12, 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” [VTX12, 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 [BDL14].

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 [VTX12]. 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.

4 Survey results

In order to adopt the above UTAUT model for the analysis of ePassports, a limited number of semi-structured interviews were carried out with policy makers and technical experts in charge of adoption of ePassports. Building on the above, a questionnaire with 49 questions was developed and an on-line survey of regular citizens (with 2,833 respondents) was carried out in over the period of February – March 2014 in Estonia

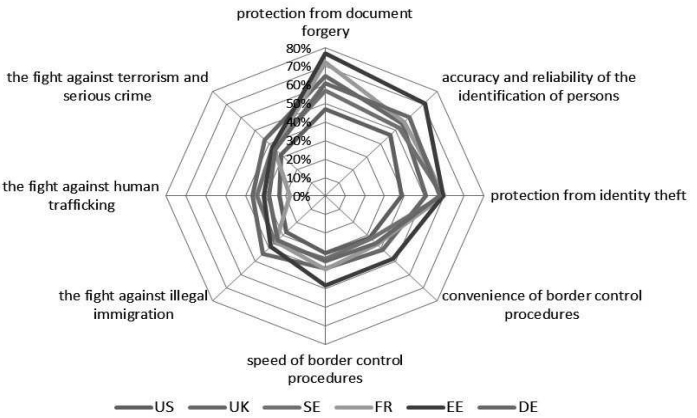
(EE), France (FR), Germany (DE), Sweden (SE), the United Kingdom (UK) and the United States of America (US). These countries represent a selection of European larger (DE, FR, UK), and smaller (EE, SE) nations, plus the US for broader comparison. Both the establishment of identity and identity management are handled differently in different countries covered by this study (for detailed survey results, see [TKL14]).

One of the key findings is that the population has only limited knowledge on data included in biometric passports, and how to use them. In the most of the countries covered by this study, only 10% of the population strongly agree with the statement "I know what data biometric passports include".

And, the experience regarding the use of biometric functions is also rather limited. 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 remains so far much 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.

The three main expectations regarding the 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%) (Fig. 2).

Figure 2. Biometric passports improve…

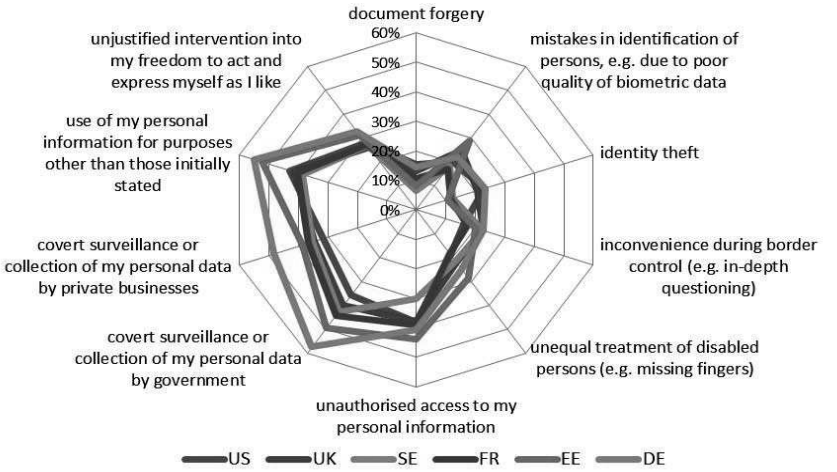


Source: ePassport web survey 2014, n=2,841.

The main two risks the respondents see, are related to 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%) (Fig. 3). Notably, those people who claim to have more detailed knowledge about ePassports have also higher expectations on the benefits of ePassports.

Figure 3. Biometric passports increase risk of…



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

The share of the 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. Furhermore, citizens' trust in government is in correlation with their knowledge about ePassports.

We also analysed 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 own and foreign border control authorities when travelling.

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. 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.

The majority of the general public agrees with public entities using passport photos in identity checks. However, the general public is less willing to agree with the use of fingerprints or eye iris images for identity checks. Majority of respondents are, in fact, against the use of advanced biometrics in case of such low security services that do not require strong authentication of a person. The public is, however, less willing to surrender their biometric data to business entities than public entities.

Furthermore, regarding the cross-border flow of ePassport related information roughly half of the respondents agreed that airlines make available passport and ticket information to the government agencies of the destination country, which happens in practice even before the actual arrival of the flight.

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. The German, Estonian and French respondents are especially strongly against this, while the American respondents hold a mixed view in this matter.

5 Discussion and 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.

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 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.

Acknowledgements

This work was supported by the European Commission through the FIDELITY EU FP7 project (Grant No. SEC-2011-284862) and "Challenges to state modernization in 21st century Europe: Theoretical developments and future scenarios" (IUT19-13). 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.

References

[Al03] Alterman, A. A Piece of Yourself: Ethical Issues in Biometric Identification. Ethics and Information Technology 5 (3), pp. 139-150, 2003.

[As97] Ash, J.: Factors for Information Technology Innovation Diffusion and Infusion in Health Sciences Organizations: A Systems Approach. Portland State University, 1997.

[BDL14] Bilbao-Osorio, B.; Dutta, S.; Lanvin, B. (eds.): Global Information Technology Report. World Economic Forum, Geneva, 2014.

[Da89] Davis, F.D.: Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13 (3), pp. 319-340, 1989.

[Eb06] European Biometrics Forum: Report on Security & Privacy in Large Scale Biometric Systems, http://is.jrc.ec.europa.eu/documents/SecurityPrivacyFinalReport.pdf, 2006.

[Eb11] Eurobarometer: Attitudes on Data Protection and Electronic Identity in the European Union. http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf, 2011.

[Ho06] Hoepman, J.-H. et al. Crossing Borders: Security and Privacy Issues of the European e-Passport. 1st Int. Workshop on Security, Kyoto, Japan, October 23-24, pp. 1-16, 2006.

[If05] Institute for Prospective Technological Studies: Biometrics at the Frontiers: Assessing the Impact on Society. For the European Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs (LIBE). http://is.jrc.ec.europa.eu/pages/TFS/Biometrics.html, 2005.

[JR08] Jain, A.K.; Ross, A.: Introduction to Biometrics. In (Jain, A.K.; Flynn, P. Ross, A. Eds.): Handbook of Biometrics. Springer, 2008; pp. 1-22.

[KH06] King, W.R.; He, J.: A meta-analysis of the technology acceptance model. Information & Management, 43 (6), pp. 740-755, 2006.

[Le00] Lederer, A.L. et al.: The technology acceptance model and the world wide web. Decision Support Systems, 29, pp. 269-282, 2000.

[LS10] London School of Economics. LSE Identity Project. The London School of Economics and Political Science, 2010.

[Ma91] Mathieson, K.: Predicting User Intentions: Comparing the Technology Acceptance Model with the Theory of Planned Behavior. Information Systems Research, 2 (3), pp. 173-191, 1991.

[MM08] Mordini, E.; Massari, S.: Body, biometrics and identity. Bioethics, 22 (9), pp. 488-499, 2008.

[Ng06] Ng-Kruelle, G.; Swatman, P.A.; Hampe, J.F.; Rebne, D.S.: 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), pp. 12-35, 2006.

[PW06] Perakslis, C.; Wolk, R.: Social Acceptance of RFID as a Biometric Security Method. IEEE Technology and Society Magazine, 25 (3), pp. 34-42, 2006.

[SL12] Sutrop, M.; Laas-Mikko, K.: From identity verification to behaviour prediction: ethical implications of second-generation biometrics. Review of Policy Research, 29 (1), pp. 21-36, 2012.

[TKL14] Tiits, M.; Kalvet, T.; Laas-Mikko, K.: Analysis of the ePassport readiness in the EU. FIDELITY Deliverable 2.2. Institute of Baltic Studies, Tartu, 2014.

[Ve00] Venkatesh, V.: Determinants of Perceived Ease of Use: Integrating Control, Intrinsic Motivation, and Emotion into the Technology Acceptance Model". Information Systems Research, 11 (4), pp. 425-478, 2000.

[VM03] Venkatesh, V.; Morris, D: User Acceptance of Information Technology: Toward a Unified View. MIS Quarterly, 27 (3), pp. 425-478, 2003.

[VTX12] Venkatesh V.; Thong J.Y.L.; Xu, X.: Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology. MIS Quarterly, 36 (1), pp.157-178, 2012.