Article

JIM
ISSN: 2183-0606
(CC BY 4.0)
Vol. 13, 2 (2025)
p. 129-173
AM: Apr/2025
SM: May/2024

What Determines the Acceptance of Digital Identity and Facial Recognition-Based Technologies? Evidence From an eID System and a Multi-Country Survey

Nicholas Martin[1] and Frederik M. Metzger[2]

[1]Fraunhofer Institute for Systems and Innovation Research ISI, Breslauer Straße 48, 76139 Karlsruhe, Germany | *nicholas.martin@isi.fraunhofer.de*
[2]Fraunhofer Institute for Systems and Innovation Research ISI, Breslauer Straße 48, 76139 Karlsruhe, Germany | *frederik.metzger@isi.fraunhofer.de*

Abstract

This paper investigates what factors determine user acceptance of a novel digital identity solution, and of facial recognition for identity authentication, respectively. We explore the relative significance of socio-demographic explanatory variables, attitudinal variables like technology affinity and privacy concerns, and technology characteristics (as perceived by the user) like usability and data sovereignty, as well as the impact of prior usage experience. The analysis builds upon survey data of 651 respondents from eight European countries, and a case study of a novel digital identity (eID) system. The study finds that socio-demographic variables do not significantly impact adoption decision for either the new digital identity technology, or facial recognition for authentication. Rather, technology affinity, privacy concerns, perceptions of data sovereignty, usability and prior experience, as well as country effects are significant. Indeed, we find evidence that national context may have important impacts on individual attitudes to privacy and technology acceptance and adoption decisions. We contribute to research on technology acceptance by providing evidence on acceptance of digital identity solutions and facial recognition for authentication, and by identifying the effects of national context as a new avenue for research.

Keywords: technology acceptance, digital identity, facial recognition, privacy.

Cite paper as: Martin, N., Metzger, F.M., (2025). What Determines the Acceptance of Digital Identity and Facial Recognition-Based Technologies? Evidence From an eID System and a Multi-Country Survey, *Journal of Innovation Management*, 13(2), 129-173.; DOI: https://doi.org/10.24840/2183-0606_013.002_0006

1 Introduction

What explains why some people adopt a novel technology and others do not? This is an important question for many actors and institutions, from entrepreneurs and technologists to governments and researchers. Prior work has examined factors driving (non-) acceptance of numerous different technologies, including workplace technologies (e.g. Davis 1989; Venkatesh et al. 2003), health technologies (e.g. Rouidi et al. 2022) and consumer technology (e.g. Förster 2024). One type of technology whose drivers of acceptance do not seem to have been investigated much as yet, is digital identity technologies. With reliable digital identity authentication becoming ever more important for economic growth (White et al. 2019), and governments seeking to promote the uptake of more advanced digital identity solutions, this gap deserves to be filled. This is particularly so as digital identity solutions are undergoing rapid technical evolution (Mühle et al. 2018), both to improve security (Naik and Jenkins 2020) and to increase user convenience (Korir et al. 2022). Biometric authentication technologies such as fingerprint, facial, iris (eye) and voice recognition, in particular, are becoming more widespread, but also raise concerns over privacy loss and data protection. This raises the question of what factors determine whether individuals will adopt new identity technologies or not, allowing us to formulate the first Research Question:

> *RQ 1:* What factors determine whether individuals adopt a new digital identity technology?

While biometric authentication technologies have advantages over legacy technologies like passwords, PINs and smartcards (in particular as regards their security; e.g. Jain et al. 2004), they have nevertheless encountered significant levels of public scepticism and opposition – even while many people have also opted to use them. It is thus important to understand better what determines whether individuals are inclined to adopt these technologies. While a growing body of scholarly work has explored the factors driving acceptance of facial recognition technology (FRT), this work has mainly focused on FRT in security and law-enforcement contexts (e.g. "smart" surveillance cameras). Acceptance of FRT *for authentication* has not been previously explored to our knowledge. We thus formulate Research Question 2:

> *RQ 2:* What factors determine whether individuals adopt facial recognition technology for authentication?

This paper provides evidence from a survey about attitudes and intentions to use a specific novel digital identity solution based on FRT. It finds that acceptance of the identity solution in question is mainly driven by four factors: usability, technology affinity, the perceived degree to which the solution puts users in control of their own data, and country effects. Technology affinity and, especially, prior usage experience as well as country effects drive the acceptance of FRT. Conversely – and contrary to our initial expectations – socio-demographic variables (e.g. age, gender, education etc.) consistently manifest little explanatory power. Even more surprisingly, privacy concerns – which we had expected to strongly affect (non-) acceptance – in fact show relatively weak and inconsistent effects and seem to be moderated by country effects. This runs counter to some prior work, which has emphasised the importance of both socio-demographic factors and privacy concerns (e.g. Hilowle et al. 2022). We thus contribute to research on technology acceptance by providing evidence on acceptance of digital identity solutions and facial recognition for authentication, and by identifying the effects of national context as a new avenue for research.

The paper proceeds as follows. Section 2 describes digital identity technologies, including the particular system used in this study, and builds on existing literature to derive hypotheses. Section 3 provides information on the methodology, survey and data. Sections 4 and 5 present the results of the data analysis. Section 6 discusses the implications and concludes.

2 Theoretical background and hypotheses

2.1 Digital identity technology and facial recognition[1]

Digital identities (sometimes also called electronic identity, eID)[2] are an electronic (digital) means for entities (citizens, businesses, machines, etc.) to prove who they say they are, via a digital

[1] This section is loosely based on Martin et al. 2023, pp. 11–12. Some sentences may be lifted from that text.

[2] For linguistic variation, the terms "digital identity", "electronic identity" and "eID" are used interchangeably in this text.

channel (European Commission n.d.; White et al. 2019). A digital identity thus includes a subset of attributes about the entity (e.g. name, date of birth) that uniquely identify it within a given set of other entities (Gritzalis and Lambrinoudakis 2008), with the composition of this subset varying by use case. Providing people with secure and user-friendly digital identities is critical to enable digital government and the further digitisation of social and economic processes and transactions (Vassil 2016; White et al. 2019, Echikson 2020). This is expected to generate substantial economic benefits (ibid.; more critically see Martin et al. 2023).

Digital identity solutions can be distinguished along two axes. One is the technology used for authentication; the second the range of services they enable. Authentication, or, from the user's perspective, Log-In, is the act of verifying that a user is indeed who they claim to be, including verifying that the attributes they claim to be true about themselves are in fact so. It is a common prerequisite for allowing a user access to certain services or resources (NIST n.d.). Many different authentication technologies for digital identities exist today; e.g. passwords and usernames, smartcards or USB sticks and PINs, or biometrics (fingerprint, iris scan, facial or voice recognition). Yet, password/username is still the most widely used authentication technology today. Smartcards seem to be mainly still used in legacy systems while being gradually supplanted with newer technology. Biometric systems are increasingly common, in particular fingerprint (FP) and facial recognition (FR). These have several advantages over password-, PIN- or smartcard-based systems: For one, they tend to provide a higher level of security. Users are not tempted into using weak passwords, and identity theft becomes substantially harder. Secondly, they are more user-friendly (no passwords that need to be remembered, no need for additional hardware). Thus they tend to lead to less usage-disrupting and for businesses, costly, "friction" (e.g. forgotten passwords requiring time-consuming resets and calls to helplines, abandoned service requests).

Many digital identity systems enable only authentication. These are sometimes also referred to as "basic" digital identity systems. More "advanced" systems, conversely, provide users with a broader suite of identity-related services. These can include the ability to make qualified electronic signatures, and to store automatically verifiable digital credentials – e.g. a digital version of one's university degree or one's state identity card – on the identity system (e.g. on one's smartphone or other device), usually in a digital wallet (White et al. 2019, Echikson 2020). "Advanced" digital identity systems of this kind are gradually becoming more prevalent. Their spread is strongly supported by many governments and private companies, as widespread adoption of advanced eID systems is seen as critical for realising the economic and larger societal benefits expected from continued digitisation (ibid.).

2.2 Acceptance of digital identity solutions

The existing literature on the determinants of digital identity systems' acceptance can be divided into two broad approaches: macro system-level determinants, and individual and solution-specific determinants. The macro literature has focused on the wider system-level and infrastructural determinants of whether people switch to using digital identity systems and digital channels to interact with the public and private sector and access services, rather than remaining with face-to-face (F2F) services. The key insight from this literature is that people will only adopt digital identity systems once at least three conditions are met: firstly, there needs to be a sufficiently high penetration of end devices (smartphones, computers); secondly, a reliable digital infrastructure with good internet connectivity and – for more advanced services – digital payment and know-your-customer systems has to exist; and thirdly, a sufficient volume of high-value and/or intensively-used digital services must be available (White et al. 2019, Vassil 2016, Pöhn et al. 2019, Felden et al. 2020, Echikson 2020, World Bank 2019). The latter point, this literature has shown, means that private-sector use cases are important: because few people use public-sector services (online or offline) intensively (TUM/Initiative D21 2018), public sector online services by themselves rarely suffice to prompt widespread adoption of digital identity systems. Rather, a sufficient volume of online private-sector services accessible via a digital identity system is needed to prompt adoption of the latter (White et al. 2019, Felden et al. 2020, Eaton et al. 2018, Echikson 2020, Mahula et al. 2021).

The macro literature provides important perspectives on the drivers of society-wide digitisation. What it does not provide much insight on, however, is the determinants of individual-level decisions over whether to switch to using a new digital identity system, or not. Yet it is well-known that people adopt new technologies at different speeds, even when the external structural conditions (that the macro literature focuses on) are kept constant. To understand the determinants of who does and does not adopt, we must therefore turn to individual-level studies.

This also implies a methodological switch. The macro literature mostly consists of case studies of the political economy of different countries' introduction of digital identity systems. Conversely, the individual-level literature generally uses survey evidence.

Indeed, the individual attitudinal and behavioural determinants of digital technology acceptance have long been a subject of research. The very influential Technology Acceptance Model (TAM; Davis 1989) focused on the *perceived usefulness* and perceived ease-of-use of a technology; basically, the degree to which users believed that the technology would help them perform a given task, and how easy they believed it would be to use the technology to this end. Subsequent research on and testing of the TAM was ultimately consolidated by Venkatesh et al. (2003, 2012) into the Unified Theory of Technology Acceptance (UTAUT). UTAUT identified seven factors that may condition technology usage; *performance expectancy* (how well technology is expected to perform), *effort expectancy* (how complex and effortful use is expected to be), *social influence* (whether using it meets with social approval), *facilitating conditions* (whether sufficient supporting infrastructure, e.g. helplines, are available to assist with usage), *hedonic motivation* (whether using it is fun), *price value* (whether it offered good value for money) and *habit/experience* (the extent to which a technology has been previously used), as well as *age* and *gender* as moderating factors.

Neither TAM nor UTAUT have to our knowledge been directly applied to the question of the acceptance of digital identity systems, or to acceptance of facial recognition technology for identity authentication purposes. Rather, these theories have tended to focus on acceptance of digital technology in the workplace, as well as various consumer technologies. Indeed, while the political economy and macro-structural determinants of the adoption of digital identity technologies has been extensively discussed (see references cited above), the individual-level determinants of the adoption of digital identity solutions have been studied relatively little, from any theoretical perspective. (Acceptance of facial recognition technology has been studied somewhat more, though rarely with a focus on its use for authentication. This is discussed further below.)

The main set of prior studies of acceptance of digital identity solutions is the German non-profit foundation TUM/Initiative D21, which since 2011 has commissioned annual representative surveys of residents of the DACH region (Germany, Austria and Switzerland) to understand their views and adoption of digital government services, digital identity technology and to some extent private sector online services. The TUM/Initiative D21 surveys reveal several consistent patterns (TUM/Initiative D21 2018, 2020, 2021, 2022, 2023). These tend to be consistent with the TAM and UTAUT literatures' findings on the general determinants of the acceptance of digital technology.

Firstly, age seems to correlate negatively with the acceptance of digital services and digital identity technologies: older people tend to prefer to access services through face-to-face channels and are less keen on using digital identity technologies than younger people. The same goes for lower levels of education and income: poorer and less educated respondents were less keen on switching to digital services and adopting digital identity solutions for this than better educated or more affluent respondents. Likewise, people living in rural areas proved more reluctant to adopt these technologies than those in major urban centres. This is broadly consistent with other studies of digital technology acceptance or use, which have tended to find that younger, better educated, more affluent and urban individuals tend to be more accepting and/or more intensive users of digital technologies than older, less educated and affluent and rural individuals (e.g. Woolley et al. 2023, Venkatesh et al. 2012) There was also some evidence in the TUM/Initiative D21 surveys of a gender gradient, with men being slightly more inclined to adopt these technologies than women.

These differences seem to be at least partly related to trust and habituation, with older, less educated and less affluent people being more distrustful of the digital world in general, and less familiar with using digital tools. At the same time, the TUM/Initiative D21 surveys also find that the strength of these patterns varies somewhat by country: age gradients for instance seem to be less pronounced in Austria than in Germany. In other words, country-level effects seem at least partly to moderate the strength of the socio-demographic variables. That said, numerous other studies also have found age and gender to affect the adoption of digital technology, with respondents who are younger or are male more likely to adopt than older and/or female respondents (e.g. Venkatesh et al. 2012, Woolley et al. 2023).

At the same time, many of these variables can go together – people can be older, rural, less educated and poorer, all at the same time. As the TUM/Initiative D21 surveys do not analyse their survey results statistically, it remains unclear whether all of these variables are in fact significantly related to acceptance, or whether some are merely spurious correlations. By proposing hypotheses – shown as an overview in Table 1 – we direct our further analysis, which follows in the remainder of this section. The TUM/Initiative D21 surveys, as well as the wider literature, allow us to formulate the first set of hypotheses, on the effect of socio-demographic variables:

> *Hypothesis 1.1 – Age*: The older respondents are, the lower will be acceptance of a new digital identity solution.
>
> *Hypothesis 1.2 – Gender*: Women will be less likely to accept a digital identity solution than men.
>
> *Hypothesis 1.3 – Income*: The higher the respondents' income, the higher will be acceptance of a digital identity solution.
>
> *Hypothesis 1.4 – Education*: The higher the level of respondents' education, the higher will be acceptance of a digital identity solution.
>
> *Hypothesis 1.5 – Place of abode*: Respondents living in villages or small towns will be less likely to accept a digital identity solution than respondents who live in major urban areas.

Table 1. Hypotheses overview.

Explanatory Variables	Dependent Variables	Acceptance of digital identity solution: Hypothesis number and expected relationship	Acceptance of FRT: Hypothesis number and expected relationship
Socio-demographic variables	Age	1.1 (−)	2.1 (−)
	Gender	1.2 (women: −)	2.2 (women: −)
	Income	1.3 (+)	2.2 (+)
	Education	1.4 (+)	2.4 (+)
	Place of abode	1.5 (rural: −)	2.5 (rural: −)
	Country effects	1.6 (▪)	2.6 (▪)
	Ethnic minority status	1.7 (minority: −)	2.7 (minority: −)
Attitudinal variables	Technology affinity	1.8 (+)	2.8 (+)
	Privacy concerns	1.9 (−)	2.9 (−)
	Data sovereignty	1.10 (+)	N.A.
	Usability	1.11 (+)	N.A.
	Prior Use of FRT	N.A.	2.10 (+)
	Prior use of other biometric technologies	N.A.	2.11 (+)

Note: “ ▪ “ means that while we expect the variable to be significant no prediction as to the direction of the effect seemed possible.

The TUM/Initiative D21 studies point to national differences having some effect on acceptance of digital identity solutions and digital services, but do not provide strong evidence for which direction these effects may take. It is plausible – and to some extent supported by the TUM/Initiative D21 surveys – that people in countries with well-developed digital services ecosystems should be more accepting of new digital identity systems because they are generally more familiar with and have greater trust in digital technology. However, one may also theorise that an opposite effect could hold: people from countries where digital services ecosystems are already highly developed may also be more likely to already possess a digital identity system that works for them and thus feel less need for a *new* digital identity system. This may lead them to be more likely to reject a new system, not so much from a general non-acceptance of digital identity systems than because they feel little need to go to the trouble of getting a new one and paying the cost (mental, financial, time) of switching from their existing system to a new one. Conversely, people from countries without well-developed digital services ecosystems may also be less likely to already possess a digital identity solution, and thus be more open to adopting one since they do not face switching costs. Yet, many other country-specific effects are conceivable, too. For example, since public debates and public discourse, even in Europe, remain heavily national, it is possible that the dominant, socially hegemonic perspectives on digital technologies vary somewhat by country, in turn leading to variation in how people respond to a new technology. We thus formulate the following hypothesis:

> *Hypothesis 1.6 – Country effects*: Respondents' country origin will affect acceptance of a digital identity solution.

One variable not covered in the TUM/Initiative D21 work is ethnic identity. To the best of our knowledge, there is no study specifically investigating acceptance of digital *identity* technologies by ethnic minorities. However, several studies have found that, at least in the West, members of ethnic minorities tend to manifest somewhat lower levels of digital technology acceptance, at least for digital health technologies (Woolley et al. 2023) or Covid contact tracing technology (Horvarth et al. 2022). Given many minorities' historical experience of discrimination and sometimes oppressive state power and, given the fact that digital identity systems – like digital health tech – by definition process rather sensitive personal data, it is thus plausible that members of ethnic minorities may be somewhat less accepting of digital identity technology than members of the majority ethnicity. We thus formulate a final socio-demographic hypothesis:

> *Hypothesis 1.7 – Ethnic minority status*: Respondents indicating to be part of ethnic minorities will be less likely to accept a new digital identity solution compared to non-minority respondents.

We turn next to attitudinal variables. People's interest in technology varies. While some people are very open to new technology and derive pleasure from experimenting with new devices, others do not. This has been theorised as "hedonic motivation" (Venkatesh et al. 2012) and has consistently found to be a strong predictor of technology use and acceptance (Venkatesh et al. 2012 and the literature cited therein). Here we prefer the term "technology affinity", because we do not focus on the pleasure derived from the concrete usage of a specific technology system, but on respondents' general attitude towards technology. That is, people are more interested in and derive enjoyment from new technology. We thus formulate

> *Hypothesis 1.8 – Technology Affinity*: The greater respondents' affinity for new technology, the higher will be acceptance of a digital identity solution.

Many people have concerns about their data privacy. To what extent this impacts actual behaviour and usage and adoption decisions remains unclear, however. There is survey evidence that at least in Europe, the adoption of technologies like smart home solutions, Covid tracking apps and services like e-government has been negatively impacted by users' privacy concerns (TUM/Initiative D21 2018, Horvarth et al. 2022). Acceptance of biometric technologies also seems to be impacted by privacy concerns (Kostka et al. 2021). Conversely, research has also consistently shown that people manifest a "privacy paradox", viz. expressing strong concerns over data privacy while continuing to use services and technologies that they know to be highly privacy invasive (Barth and de Jong 2017). It thus remains an open question whether and how privacy concerns might affect the acceptance of a new digital identity technology. However, we expect that at least at the margins increased privacy concerns should be associated with reduced acceptance of a new digital technology, especially one that by definition processes sensitive personal data – as digital identity solutions do. We therefore formulate:

> *Hypothesis 1.9 – Privacy Concerns:* The greater respondents' privacy concerns, the lower will be acceptance of a digital identity solution.

Relatedly, there is growing survey evidence that people greatly like the idea of "having control" over their data (e.g. PWC 2021, Spiekermann and Korunovska 2017). This suggests that people will be more likely to accept a digital identity solution if they believe (correctly or not) that this solution gives them "control over their data", that is, data sovereignty. We thus formulate:

> *Hypothesis 1.10 – Data Sovereignty:* The higher respondents' perception of some measure of control (sovereignty) over their data, the higher will be acceptance of a digital identity solution.

It is intuitively plausible that users will be more likely to accept a new technological solution if they think its usability is high. This is also borne out by much prior work (Hedström et al 2015, Gustafsson and Wihlborg 2013, BCG and Nortel 2020, Pöhn et al. 2019, Venkatesh et al. 2012, Eaton et al. 2018, Echikson 2020). We therefore formulate:

> *Hypothesis 1.11 – Usability:* The higher respondents' perceived usability, the higher will be acceptance of a digital identity solution.

2.3 Acceptance of FRT for authentication purposes

Authentication is only one of many possible uses of FRT. While increasingly common, it is not the most discussed or the controversial use of FRT. Indeed scholarship and public debate have focused on acceptance of FRT for security and law-enforcement purposes, and on commercial uses connected to tracking the public at large (e.g. for advertisement purposes within a shopping mall). Only a few studies have also addressed acceptance of FRT for authentication. (Acceptance of) FRT for law enforcement or commercial tracking presents different issues than FRT for authentication. Nevertheless, these studies too can shed light on possible factors driving acceptance, and we therefore consider these studies as well as what literature is available on FRT for authentication.

Kostka et al. (2021) study acceptance of FRT for security and law enforcement among respondents in Germany, China, the US and UK, and provide an overview of recent research on the topic. With some exceptions, the effect of most socio-demographic variables seems to be ambiguous, with different studies finding the same variable to correlate positively, negatively or not at all with acceptance. A possible explanation for this phenomenon could be country effects (see below). One effect that does find relatively consistent support is that of income. Both Kostka et al. (2021) and Fletcher et al. 2017 (discussed in Kostka et al.) find that acceptance increases with income.

Evidence is more ambiguous for age, gender and education: Fletcher et al. (2017) find gender not to be significant, Trüdinger and Steckermeier (2017, discussed in Kostka et al.), find German women to be more accepting than German men, while Kostka et al. (2021), to the contrary, find German *men* to be more accepting than German women, and Chinese *women* more accepting than Chinese men. (The variable is not significant for respondents from the US and UK.). Higher age is a (weakly) significant predictor of acceptance among Kostka et al.'s (2021) respondents from the USA, but not elsewhere. Age is also not significant in Fletcher et al.'s (2017) study, but higher age *is* associated with greater acceptance in a Pew Centre study (2017, discussed in Kostka). That older people (or women) should be *more* accepting of FRT than younger people (or men) may seem counter-intuitive, given the general association of technology acceptance with youth and male gender. However, this could be explained by women and older people being (or perceiving themselves to be) at greater risk of violent crime than younger men – after all, the technology in question here is FRT *for security and law enforcement*. How these results might translate to FRT used *for authentication* is less clear, however. Plausibly, older people might struggle more with usernames and passwords than younger people, and thus be more open to using FRT as an alternative. Yet, it is also possible that older people are less open to new technology in general, and thus are also less open to FRT for authentication. Indeed, the data on acceptance of digital identity technology discussed above suggests just that. Similarly, in as far as men tend to be more open to new technology in general and of digital identity systems in particular, they could be more accepting of FRT for authentication.

On balance, we thus hypothesise:

> *Hypothesis 2.1 – Age*: The older respondents are, the lower will be acceptance of FRT for authentication.
>
> *Hypothesis 2.2 – Gender*: Women will be less likely to accept a digital identity solution than men.
>
> *Hypothesis 2.3 – Income*: The higher respondents' income, the higher acceptance of FRT for authentication.

Findings for education are ambiguous as well. Among German respondents, Kostka et al. find that higher levels of education predict greater acceptance but Trüdinger and Steckermeier (2017) find the opposite, and the variable is again not significant for Kostka et al.'s respondents from China, the UK and the USA. Fletcher et al. (2017) do however find higher levels of education to predict greater acceptance. For higher levels of education to go together with greater levels of acceptance would also be in line with the general findings on technology acceptance. On balance, we thus hypothesise:

> *Hypothesis 2.4 – Education*: The higher the level of respondents' education, the higher will be acceptance of FRT for authentication.

Kostka et al. (2021) is the only study known to us to explore the effects of place of abode on acceptance. They find that living in a city increases the likelihood of acceptance for respondents from Germany, but not for the other countries. This could be related to urban dwellers being more exposed to crime than those in rural areas, but it could also reflect a greater a technological openness among urbanites in general, as supported also by the TUM/Initiative D21 studies. The latter would lead us to expect greater urban than rural acceptance also for FRT for authentication. We thus hypothesise:

> *Hypothesis 2.5 – Place of abode*: Respondents who live in villages or small towns will be less likely to accept FRT for authentication than respondents who live in major urban areas.

Kostka et al. (2021) find country effects to be highly significant. How people in general and subpopulations (e.g. women) reaction to FRT seems shaped in important ways by national differences. This may explain the other variables' frequent inconsistency across countries. We thus formulate:

> *Hypothesis 2.6 – Country effects*: Respondents' country origin will affect acceptance of FRT for authentication.

A similar ambiguity as with place of abode relates to ethnic minority status. The variable is not significant in Kostka et al.'s study, but the Pew Center study finds that minorities are less accepting of FRT, at least in a law enforcement context, as does a study of the Ada Lovelace Institute (2019). Given historical experiences of discrimination, this is not surprising, and plausibly it could translate to a greater scepticism of FRT uses in general. We thus hypothesise:

> *Hypothesis 2.7 – Ethnic minority status*: Respondents indicating to be part of ethnic minorities will be less likely to accept FRT for authentication compared to non-minority respondents.

Turning to attitudinal variables, none of the studies we surveyed checked for the effects of technology affinity. Nevertheless, it is very plausible that people with higher technology affinity will be more accepting. We thus hypothesise:

> *Hypothesis 2.8 – Technology Affinity:* The higher respondents' affinity for new technology, the higher acceptance of FRT for authentication.

What the surveyed studies mostly examined, were the effects of privacy concerns. These were consistently found to negatively impact acceptance, both of FRT for authentication and for law enforcement (Kostka et al. 2021, Fletcher et al. 2017, Zimmermann and Gerber 2020, Morales et al. 2010, Ada Lovelace Institute 2019, Krol et al. 2019, Hu et al. 2021). This is intuitively plausible, and thus we hypothesise:

> *Hypothesis 2.9 – Privacy Concerns:* The higher respondents' privacy concerns, the lower acceptance of FRT for authentication.

A further factor consistently found to increase acceptance is prior experience and habituation: people who have previously used or otherwise experienced a given technology are more likely to accept it when presented with it in the future. This effect has been documented for numerous technologies, and in particular also for FRT, both for law enforcement and for authentication (Kostka et al. 2021, Morales et al. 2009, Krol et al. 2019, TUM/Initiative D21 2020, TUM/Initiative D21 2021). We thus hypothesise:

> *Hypothesis 2.10 – Prior Use of FRT:* The higher respondents' prior experience with FRT, the higher acceptance of FRT for authentication.

One so far still open question is whether the prior-experience effect holds only for the identical technology, or whether prior experience of a related technology can also increase acceptance. I.e. can only prior experience of FRT (potentially) increase acceptance of FRT, or could prior experience of other biometric technologies do so too? Since the risks associated with FRT (privacy, false negatives/false positives, etc.) exist also for other biometric technologies, it is plausible that prior experience of these too might translate into higher acceptance of FRT. We thus hypothesise:

> *Hypothesis 2.11 – Prior Use of other biometric technologies:* The higher respondents' prior use of biometric technologies other than FRT (e.g. fingerprint recognition), the higher acceptance of FRT for authentication.

3 Methodology[3]

3.1 Method and sample collection

We use the case of a novel smartphone- and facial recognition-based digital identity solution called "IMPULSE" to test the hypotheses, with data from an online survey. IMPULSE was developed

[3] This section is loosely based on Martin and Metzger 2024, pp. 13–15. Some sentences may be lifted from that text.

and trialled as a prototype in the eponymous Horizon 2020 project[4], during which the survey was also conducted.

IMPULSE is described in detail below, but from the user's perspective, it is a smartphone application. Using IMPULSE, the user can register and subsequently authenticate to online services, which she or he accesses via her browser. Authentication is done with FRT, using the smartphone camera. Credentials are stored in a digital wallet that is part of the app. IMPULSE is thus a rather typical instantiation of the core features of the novel, smartphone- and biometrics-based digital identity solutions coming on the market today. Unlike some commercial offerings, though, the IMPULSE prototype and use case presented to survey respondents was focused exclusively on authentication, without any further services or benefits (e.g. loyalty rewards). While the question of how generalisable results are that derive from the IMPULSE case necessarily presents itself, the "bare bones"-nature of the IMPULSE solution somewhat reduces the risk of false inferences.[5]

The survey analysed here was conducted to collect data on likely levels of user acceptance of IMPULSE, but also included general (i.e., not IMPULSE-specific) questions about willingness to use FRT for authentication, as well as collecting a wide range of attitudinal, behavioural and socio-demographic data (see below).

We next describe the survey, the IMPULSE solution, and the data set. In the subsequent sections, we present the results of our analysis with respect to the research questions. The survey data was analysed descriptively and with regression analysis, using Ordinary Least Squares and Logit regression analyses. These were performed with the R software package. Detailed information on the dependent and explanatory variables used in regression analyses and how they were constructed from the survey data is provided below, in the chapter on the results of the regression analyses.

The survey ran from February to June 2023. The survey link was initially disseminated through the personal and professional networks of the researchers and staff members from the IMPULSE consortium's 15 partner institutions in their countries (Germany, Spain, Italy, Denmark, Iceland, Bulgaria, Finland and France). Respondents were asked to pass the survey on further in their own personal networks (convenience sampling). This dissemination method was chosen as financial constraints prevented the use of e.g. a survey company. To incentivise participation, a donation of €2 to charitable organisations was promised per completed survey, up to a total of €500.

The survey instrument is presented in Appendix A. It was given to respondents in their native languages (i.e. Spanish, German, etc.). Respondents were first asked for various socio-demographic and attitudinal data; viz. their age, gender, ethnicity, education, income (by quintile), and place of abode (village or rural area, small/medium-sized town, major metropolitan area), affinity for novel technology, and privacy concerns. For "technology affinity", respondents were given the statement "I enjoy trying out new technologies" and asked to record their disagreement/agreement with it on a Likert scale running from 1 ("strongly disagree") to 5 ("strongly agree"). For privacy concerns, respondents were told that "people have different views on privacy" and then asked, "in general, how concerned are you about your privacy when you access services on the internet?" with answers again recorded on a 5-point Likert Scale (1 = "very concerned", 5 = "not concerned at all").

[4] IMPULSE – Identity Management in PubLic SErvices (www.impulse-h2020.eu) was an EU Horizon 2020-funded project (European Commission Grant Agreement 101004459). It ran from 02/2021 to 01/2024 and aimed to develop a smartphone-based SSI-style identity solution, trialling this in six pilots mostly in local public administrations across Europe. The authors, and the Fraunhofer Society, participated as partners in the project, responsible mainly for social-political and economic impact assessments, standardisation and roadmapping. Fraunhofer and the authors have no commercial or financial interest in the IMPULSE solution.

[5] See further discussion in chapter 6.3 "Limitations"

Next, they were shown a five and a half minute long animated video explaining the "IMPULSE" digital identity solution.[6] The film used the example of online banking to illustrate how IMPULSE works and how one could use it to sign up and log in to online services. The film presented IMPULSE as an alternative to traditional digital identity systems based on passwords and usernames, noting the problem that people often choose weak passwords. It was careful to describe IMPULSE in neutral terms, and concentrated on laying out the concrete process of signing up and logging in with IMPULSE as well as the associated data flows. Promotional language, in particular about e.g. usability, privacy friendliness or data control, was carefully avoided.

After watching the video, respondents were asked, "would you use IMPULSE instead of the digital identity (log-in) systems that you currently use (like username/password, smartcard, PIN, etc.), if IMPULSE were available?" Answers were recorded on a 5-point Likert Scale (1 = "certainly not", 5 = "certainly yes"). Those respondents who selected "1" or "2" on the Likert scale (which we may interpret as "certainly not" and "probably not") were then asked why they would not use IMPULSE.[7] This was followed by a question about which online services respondents considered appropriate use cases for IMPULSE. Eight different services were listed (plus "Other/please specify" and "None"), ranging from services involving very sensitive data (e-health, online banking) to less sensitive use cases (e.g. social media). Finally, respondents were given 18 different words and phrases and asked to choose all that "you feel describe IMPULSE". These included nine positive phrases (e.g. "convenient", "saves time", "makes logging in easier", "interesting" etc.) and seven negative phrases (e.g. "complicated", "surveillance", "dangerous", "unnecessary", etc.), plus two further descriptors suggesting that IMPULSE would give users data sovereignty.[8]

Later in the survey, respondents were asked about their experience with and preference for different kinds of authentication technologies. They were given a list of technologies – username and password, smartcard and PIN, NemID/MitID (only in the Danish survey), PIN/TAN, fingerprint recognition, facial recognition, voice recognition, iris (eye) recognition, and "other/please specify" – and asked whether they had used each of these technologies, heard about them, or not heard about them. Then they were given the same list, and asked to select those three technologies that they preferred to use for authentication.

The survey also asked other questions not analysed here, including about respondents' use of public and private online services, their understanding of the concept of "data sovereignty", views on and experience with using multiple digital identities and passwords.

3.2 The IMPULSE solution

The IMPULSE digital identity solution works as an application that the user installs on her smartphone. This will enable her to access a larger ecosystem of online service providers (e.g. banks, healthcare providers, e-commerce sites, government services etc.) who use IMPULSE for authentication.[9] The video shown to the survey respondents described the process by which users onboard to online services using IMPULSE and later authenticate to the service (once onboarded).

[6] The film can be viewed at https://www.youtube.com/@impulse_EU

[7] Respondents were offered a list of seven possible reasons (multiple answers possible), plus "Other, please specify" with a free text box. The list of reasons offered focused on smartphone dependence, security-related concerns, concerns over FRT, usability, and lack of need.

[8] "IMPULSE gives me control over my data", "With IMPULSE, I can decide who gets my data"

[9] At this stage, IMPULSE exists only as a prototype and is not yet in production. Survey respondents were told that the system is currently under development by a consortium of European scientists, and all descriptions and questions were carefully phrased to make clear that the system is not currently in production and the questions concern a hypothetical future state where it is.

The following presents an extended and more technical description of how the system functions than given to the survey respondents in the video; the core information however is the same.[10]

With IMPULSE, the first step on the user's onboarding journey is to navigate to the online service's website using a browser on her smartphone and click on a "sign up with IMPULSE" button on the service website. This opens the IMPUSE app on their phone. The user now takes a photo of the front and back of her state ID card or passport, and a selfie. These are uploaded to the IMPULSE enterprise module installed in the service provider's IT system via an encrypted peer2peer channel.[11] Prior to upload, a module integrated in the IMPULSE app creates a biometric profile of the user from the selfie and stores this profile in the user's smartphone, for use when she authenticates to the online service the next time, after onboarding. The profile is not shared with the enterprise module. The enterprise module (on the online service provider side) of IMPULSE then uses artificial intelligence to check that the selfie and the user's picture on her ID card match and verifies the authenticity of the ID documents. This user verification can be fully automated, but for compliance with EU eIDAS regulation, IMPULSE foresees a human in the loop (a worker on the online service provider side who manually confirms that the photos match). Next, such data as the online service requires are automatically extracted from the ID card photos (e.g. name, date of birth, address). Additional data not contained on the ID card that may be needed (e.g. bank details) are entered manually by the user. These are encoded in a digital credential (a so-called "verifiable credential" or VC) that the service provider creates for the user (to be read out later by the service provider's system when the credential is presented during authentication) and/or stored directly by the service provider in their systems. With verification of the user completed, all photos are erased, and the service provider creates the credential (VC) for the user and sends this her, to be stored in the IMPULSE app digital wallet on her smartphone. The user is now onboarded to the online service provide.

When the user next wishes to authenticate to the service to use it, she again goes to the service provider's webpage, chooses "log in with IMPULSE", which opens the IMPULSE app on her smartphone. To access the authentication credential (the VC) from the service provider that is stored in her app, she must again take a selfie, which is checked via facial recognition against the biometric profile that is also stored on her Smartphone. Provided the selfie and the profile match, the authentication credential is automatically presented to the service provider. The service provider verifies the credential against its own systems and authenticates the user. She can now use the service. The entire process should only take a few moments. In the video in the survey, the process of was explained to users in a slightly simplified fashion and in non-technical language, using the example of an online bank.

3.3 Dataset

After excluding missing values, there were 651 responses to the survey. Table 3 shows the country breakdown. Just over two-thirds of respondents are from Germany, Spain and Italy, with the other countries accounting for between 3% and 8% of respondents each. Respondents' age ranged from 18 to 82 years (average 42.2; median 40), with 65% of the respondents drawn from the prime working-age population (30–59 years age). This distribution is also found in most of the country cohorts, with the notable exception of Germany (only 41% between 30 and 59; instead greater share aged 60 and over) and Denmark (only 53 percent between 30 and 59; instead greater share younger than 30). Respondents were disproportionately well-educated (87% had or

[10] This following two paragraphs are taken from Martin and Metzger 2024, pp. 15–17, with some minor modifications.

[11] Technically, this is a DID (decentralised identifier) channel.

were currently in university education) and affluent (by income, 53% belonged to the top-20% of income earners; a further 16% to the top 60-80%), and 93.5% white (3% self-declared as ethnic minority, 3.5% chose the option to refuse an answer). The biases towards more highly educated and towards more affluent respondents are found throughout the country cohorts, with the partial exceptions of Bulgaria and Denmark, where "only" 72% (Bulgaria) and 68% (Denmark) had university educations (Figure 5 and Figure 6 in Appendix B).

Conversely, the gender split was almost exactly 50-50 (50.7% female, 48.8% male, rest diverse). 57.4% of respondents live in small or medium-sized towns; 25.5% in major cities, 17% in villages. Evidently, the survey population is not representative of the general population, as was to be expected given the dissemination strategy. The implications thereof for the external validity of the following analysis are discussed in closing.

Table 2. Breakdown of survey respondents by country.

Country	Number of respondents	Share of sample (%)
Germany	175	27
Spain	173	27
Italy	102	16
Denmark	53	8
Iceland	51	8
Bulgaria	40	6
Finland	35	5
France	22	3
Total	651	100

Respondents mostly self-described as having a high affinity for technology. 74.2% agreed or strongly agreed with the statement "I enjoy trying out new technologies". This high openness to new technology is broadly shared across most but not all country samples (Figure 7 in Appendix B): While the average technology-affinity Likert value for respondents from Bulgaria, Iceland, Italy and Spain is between 4.3 and 4.4, the average score for respondents from Finland, Denmark, and Germany is somewhat lower, between 3.5 and 3.8, with France in the middle at 4.1. (Average Likert-scale score across the entire survey population: also 4.1).

The respondents were also quite sensitive to online privacy. 60.5% were "concerned" (Likert value of 4) or even "very concerned" (Likert value of 5) about their privacy online (Figure 8 in Appendix B), though slightly larger variations across country samples can be observed. While Bulgarian respondents registered the highest privacy concerns, with a score of 4.6 on average, Danish respondents registered an average score of only 3.1. (Figure 8 in Appendix B). Interestingly, elevated privacy concerns do not seem to preclude respondents simultaneously having a high technology affinity: thus the Bulgarian respondents register both the highest privacy concerns, and a very high interest in new technology, while Finnish, German and especially Danish respondents register relatively low values on both on average.

4 Results: Acceptance of a new digital identity system

4.1 Descriptive analysis

After viewing the video, respondents were asked whether they would use IMPULSE instead of their current digital identity system, should it become available, to be answered on a Likert scale.

As Figure 1 shows, a narrow majority (336 respondents, or 51.6%) chose 4 or 5 on the Likert scale, which may be interpreted as "would or would certainly switch to IMPULSE", while 23.6% (154 respondent) chose 1 or 2 ("would not/certainly not"). The remaining 24.7% (161 respondents) chose 3, which may be understood as a neutral "maybe". Evidently, IMPULSE appealed to a substantial fraction of respondents, but by no means to everyone.

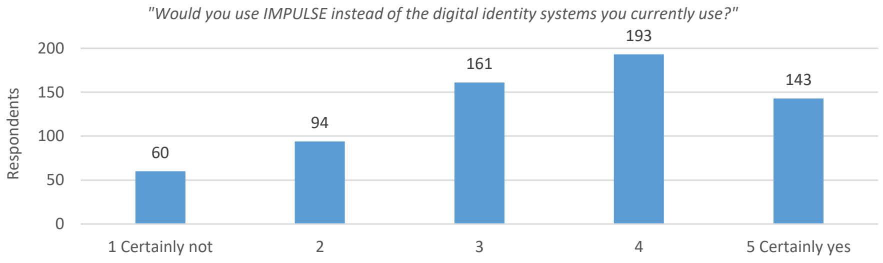
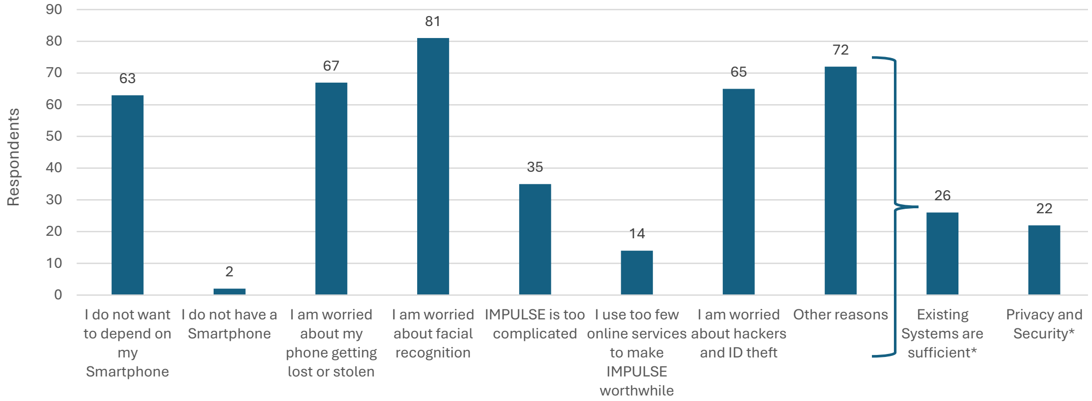


Figure 1. Intention to use IMPULSE across the survey population

Figure 9 in Appendix B shows in more detail the distribution of "would use", "would not use" and "maybe" responses across the surveyed countries. What stands out is the very high share of "would use IMPULSE"-responses from Bulgaria and secondarily from Spain. Conversely, the largest proportions of "would *not* use"-respondents are found in Iceland and Denmark. Due to the heterogeneity of the survey population and the fact that none of the country samples are nationally representative, these numbers must be interpreted very cautiously – in particular before statistical analysis. However, a plausible explanation for these patterns could relate to the fact that both Denmark and Iceland have established, very widely used digital identity systems – thus reducing the need for a system like IMPULSE – while in Bulgaria and Spain no established nationwide system exists. Instead, in both countries users confront fragmented eID landscapes, with multiple, often region-, municipality- or service-specific digital ID systems. Free text responses to the question of why respondents would *not* use IMPULSE (discussed further below) indeed provide some support for this speculation, in as far as a number of Danish and Icelandic respondents noted that due to the existing, established systems in their countries, they had no need for IMPULSE. At the same time, it is clear that this cannot be all that is going on, since Germany has a similarly fragmented digital ID landscape as Bulgaria, but the German respondents nevertheless manifested the third-lowest share of "would-use"-responses.

154 respondents selected a 1 or a 2 ("would not"/"would certainly not use IMPULSE"). These people were then asked why they would not do so (multiple answers possible). Figure 2 shows the results. Concern over the solution's use of facial recognition technology (FRT) is the single most-often chosen reason, with other security-related factors figuring too. This is also borne out by the free-text responses to this question, as well as the answers to the subsequent question about which terms best described IMPULSE (discussed next below). Collectively, these indicate that at least a small subset of the respondent population perceived IMPULSE quite negatively, with concerns over privacy, security and inappropriate collection of sensitive data top of mind, prompting sometimes vituperative reactions.[12] Conversely, (poor) usability and little need for the solution were rarely cited.

[12] Thus one respondent wrote that "it [IMPULSE] is most stupid thing and not secure as you say it is! That alone is a fact just look to the news it is made for others to steal from the person, Fact!" Another argued that it



Multiple answers possible
*imputed from free-text responses

Figure 2. Reasons for not using IMPULSE

As noted above, the respondents were given a list of positive and negative, as well as more neutral, terms, and asked to select all that they felt described IMPULSE (Figure 10 in Appendix B). While positive descriptors were chosen significantly more often than negative ones, no term garnered more than a plurality of votes. Nevertheless, the various descriptors related to *good* usability and convenience were each chosen by between ~27% and ~37% of respondents. Conversely, negative descriptors related to *poor* usability and lack of usefulness were chosen only by between ~5% and ~12% of respondents. Notable is the divergence in views related to safety and privacy guarantees. While 32.9% (214 respondents) felt that "safe" described IMPULSE well, and 28.4% (185 respondents) believed this of "privacy friendly", 6.5% (42 respondents) conversely thought that "dangerous" was a good descriptor, and 9.2% (60 respondents) believed this of "surveillance". Inspection of the raw data reveals that those who chose "safe" or "privacy friendly", and those who chose "dangerous" or "surveillance", are almost completely separate groups of respondents. Finally, 5.7% and 5.2% of respondents felt that "creepy" or "weird" described IMPULSE, which may be understood as indicating a general discomfort with the system. In total 211 respondents (32.4%) chose *at least one* of the negative descriptors (dangerous, surveillance, creepy, weird, unnecessary, complicated, not useful), while 554 respondents (85%) chose *at least one* of the positive descriptors (convenient, easy to use, saves time, makes signing up/logging in easier, exciting, safe, privacy friendly, interesting).

Finally, the two descriptors suggesting that IMPULSE would give users data sovereignty – "IMPULSE gives me control over my data" and "with IMPULSE, I can decide who gets my data" – were felt by 82 (12.6%) and 89 (13.7%) respondents, respectively, to be good descriptors of the system. While the objective validity of these claim that a system like IMPULSE can give users data sovereignty, and thus the accuracy of these descriptors, is questionable, the particular family of digital identity solutions that IMPULSE belongs to (so-called "self-sovereign identity solutions", SSI) is often marketed as giving users data sovereignty / "control over their data" (Martin and Metzger 2024). However, whether objectively correct or not, evidently these claims sounded plausible to a subset of the survey respondents.

was "subjectively dangerous if Selfies are online or transmitted", and a further claimed that "Again you are making people more slaves than it has been. So you are working with slavery to all human kind. Stop this nonsense and let people have there one right to choose!"

As noted, we further asked respondents what use cases they regarded as appropriate for IMPULSE (data not shown). Respondents tended to see IMPULSE as more appropriate for online services handling relatively sensitive data like e-health and finance-related services (banking, taxes). Conversely, less sensitive services, like social media or state registration (as is required in some European states) seemed to be regarded as less fitting. A possible explanation for this could be that IMPULSE itself uses quite sensitive data (facial biometrics) and while this increases the level of security, respondents regarded using such sensitive data for authenticating to social media or email as inappropriate "overkill".

4.2 Regression analysis

To understand the individual-level determinants of (non-) acceptance of the IMPULSE system, we conducted regression analysis. We estimated three models each for two different dependent variables (DVs), using a battery of explanatory variables. We next describe the dependent and the explanatory variables, and then turn to the results.

Dependent variables

The first DV is *Positive Perceptions of IMPULSE*. This is an ordinal variable constructed from the nine different positive descriptors of IMPULSE, with a value running from 0 to 9. It took a value of 0 if the respondent had not selected *any* of the positive descriptors as good descriptions of IMPULSE, 1 if she or he had selected one positive descriptor, 2 if two, through to 9 if they had chosen all nine positive descriptors as good descriptions of IMPULSE.

The second DV was *Intention to Adopt IMPULSE*, viz. the respondent's self-reported likelihood of switching to IMPULSE, were the system to become available. This too was an ordinal variable running from 1 (if they had selected 1 on the Likert scale, i.e. "certainly not") to 5 ("certainly yes").

The logic of using these two distinct DVs to understand the acceptance of the IMPULSE digital identity solution is that they capture somewhat distinct information. The question whether people would switch to using IMPULSE instead of their present digital identity system, were it to become available, tells us about how they evaluate IMPULSE *relative to their current system*, and about their willingness to bear the switching costs of a change (acquiring the new system, learning how to use it, updating service information, etc.). This is important information for someone wanting to evaluate the market potential of a new system, but the variable thus also captures information extraneous to the IMPULSE solution itself – for instance, whether or not someone has already just bought a new solution, and is thus less motivated to shoulder new switching costs, or whether someone is already looking around for a new system (and thus perhaps more inclined to pay switching costs). Conversely, the question of how positively or not someone perceives IMPULSE tells us much less about their willingness to pay switching costs or the strength of their inclination to actually change to the new system. However, this measure is also less influenced by information about their satisfaction with their current system, etc. To get a good measure of acceptance, we thus use both measures in separate regressions. Of course, positive perception and intention to switch should logically be closely correlated and driven by the same variables – if it turns out that they are *not*, this would raise questions about the quality of these measures. Regressing them on the same explanatory variables thus also provides a reliability check for the analysis.

Explanatory variables

We use the following explanatory variables in the regressions:[13]

- *Age*: a continuous variable running from 18 to 82, capturing the respondents' age.
- *Gender_Male:* a dummy variable with value 1 if the respondent is female, and 2 if male.
- *Education*, a categorical variable with value 1 if the respondent has completed high school (but not attended university), and value 2 if the respondent has completed or is attending university. The value 0 is given if the respondent has not completed high school, and is the reference category. R reports the coefficients for each value that the variable takes separately in the regression table (except the reference category). Thus the table includes *Edu_HighSchool* (when the education variable has the value 1) and *Edu_University* (educational variable value of 2).
- *Income:* a categorical variable with values 1–5, corresponding to the income quintile (based on EuroStat data) that the respondent's self-reported income is in. (I.e., value = 2 if the respondent's income situates them in the second quintile; value = 3 for the third income quintile, etc.). The reference category is the first quintile. R again reports the coefficients for each value that the variable takes on separately (except for the reference category), viz. *Income_Q2* for second quintile, *Income_Q3* for third quintile, etc.
- *Place of Abode*: a categorical variable with value = 1 if the respondent reports themselves to live in a village or rural area, value = 2 if they report to live in a small or medium town, and = 3 for major city. The reference category is 1. R reports the coefficients for value = 2 (*SmallMedium_Town*) and = 3 (*City*) separately.
- *Ethnicity*: a categorical variable with value = 1 if the respondent self-reported to be "white" (reference category), value = 2 if the respondent self-reported to belong to an ethnic minority, and = 3 if he or she refused to report their ethnic identity. The reference category is 1; R reports the coefficients for Ethnicity = 2 (*Ethnic_Minority*) and = 3 (*Ethnicity_Refuse*) separately.
- *TechAffinity:* an ordinal variable running from 1 to 5, capturing the respondent's self-reported enjoyment of new technology[14].
- *PrivacyConcern:* an ordinal variable running from 1 to 5, capturing the respondent's self-reported level of concern over their online privacy.
- *Usability:* an ordinal variable running from 0 to 5, with 1 point added for each of the descriptors "convenient", "easy to use", "makes signing up for services easier", "makes logging in easier" that the respondent ticked. This variable was not included in the models taking *Positive Perceptions of IMPULSE* as DV, since it is constructed from some of the same items as that DV.
- *DataSovereignty_Perception:* an ordinal variable with values 0, 1, 2, that captures whether respondents ticked none, one or both of the "control over/get to decide who gets my data"-descriptors.

[13] Most of the following descriptions of the variables are taken from Martin and Metzger 2024 where we ran regressions using many of these same variables (albeit to answer a different research question).

[14] The survey item asked respondents where they stood with regard to the statement "I enjoy trying out new technologies" (Likert scale 1 ("strongly disagree") to 5 ("strongly agree").

- *Country*: a categorical variable with country coding for Bulgaria (reference category), Denmark, Finland, France, Germany, Iceland, Italy, Spain.
- An *interaction term* between the *Country* variable and *PrivacyConcern.*

Results

For each of the two DVs, we estimated three models. For both *Positive Perceptions* (i.e. DV 1) and *Intention to Adopt* (i.e. DV 2), the first respective models (i.e. Model 1.1 [DV 1] and Model 1.4 [DV 2]) take *Age*, *Gender*, *Education, Income*, *Place of Abode*, *Ethnicity*, *TechAffinity*, *PrivacyConcern* and *DataSovereignty_Perception* as explanatory variables. For *Intention to Adopt*, Model (1.4) additionally also takes *Usability* as explanatory variable.[15] In Models (1.2) [DV 1] and (1.5) [DV 2], *Country* is added, to control for country effects. In Models (1.3) and (1.6), the *Country-PrivacyConcerns interaction term* is added too. The results are shown in Table 3 (DV *Positive Perceptions*) and Table 4 (DV *Intention to Adopt*). Because both sets of regressions capture important information related to acceptance, we discuss them together.

Table 3. Linear regression for positive perceptions of IMPULSE (DV 1).

	Model (1.1)	Model (1.2)	Model (1.3)
Age	-0.025^{***} (0.007)	-0.020^{***} (0.007)	-0.018^{**} (0.007)
Gender	0.043 (0.199)	−0.050 (0.196)	−0.017 (0.195)
$\text{Edu}_{\text{HighSchool}}$	−0.098 (0.443)	−0.095 (0.447)	−0.089 (0.447)
$\text{Edu}_{\text{University}}$	−0.239 (0.364)	−0.252 (0.373)	−0.252 (0.370)
Income_{Q2}	1.427^{***} (0.545)	1.106^{**} (0.539)	1.294^{**} (0.541)
Income_{Q3}	−0.020 (0.500)	−0.135 (0.503)	−0.042 (0.503)
Income_{Q4}	1.099^{**} (0.456)	0.788^{*} (0.458)	0.900^{*} (0.460)
Income_{Q5}	0.828^{**} (0.413)	0.629 (0.415)	0.745^{*} (0.418)
$\text{Income}_{\text{Refuse}}$	0.415 (0.493)	0.144 (0.492)	0.297 (0.491)
$\text{Place}_{\text{SmallMedium\_Town}}$	0.0004 (0.268)	0.066 (0.265)	0.006 (0.264)
$\text{Place}_{\text{City}}$	−0.188 (0.302)	0.090 (0.310)	0.005 (0.311)
$\text{Ethnicity}_{\text{Minority}}$	-1.304^{**} (0.581)	-1.335^{**} (0.579)	−0.697 (0.600)
$\text{Ethnicity}_{\text{Refuse}}$	-1.666^{***} (0.538)	-1.393^{***} (0.532)	-1.275^{**} (0.527)
TechAffinity	0.386^{***} (0.103)	0.357^{***} (0.104)	0.345^{***} (0.104)
PrivacyConcern	−0.066 (0.096)	-0.218^{**} (0.101)	1.158^{**} (0.513)
DataSovereigntyPerception	1.702^{***} (0.169)	1.624^{***} (0.169)	1.665^{***} (0.168)
$\text{Country}_{\text{Denmark}}$		-2.354^{***} (0.536)	2.403 (2.550)
$\text{Country}_{\text{Finland}}$		−0.946 (0.582)	5.954^{**} (2.866)
$\text{Country}_{\text{France}}$		-1.527^{**} (0.652)	6.842^{*} (3.546)

[15] *Usability* is *not* included in the regressions with *Positive Perceptions* as DV, because it was constructed using some of the same survey items as *Positive Perceptions*.

	Model (1.1)	Model (1.2)	Model (1.3)
Country$_{\text{Germany}}$		−1.587*** (0.458)	5.638** (2.466)
Country$_{\text{Iceland}}$		−1.887*** (0.538)	6.316** (2.665)
Country$_{\text{Italy}}$		−1.546*** (0.469)	6.212** (2.611)
Country$_{\text{Spain}}$		−0.793* (0.447)	3.859 (2.510)
PrivacyConcern:Country$_{\text{Denmark}}$			−0.864 (0.589)
PrivacyConcern:Country$_{\text{Finland}}$			−1.547** (0.685)
PrivacyConcern:Country$_{\text{France}}$			−1.891** (0.811)
PrivacyConcern:Country$_{\text{Germany}}$			−1.644*** (0.543)
PrivacyConcern:Country$_{\text{Iceland}}$			−1.884*** (0.596)
PrivacyConcern:Country$_{\text{Italy}}$			−1.750*** (0.577)
PrivacyConcern:Country$_{\text{Spain}}$			−0.937* (0.549)
Constant	1.289 (0.832)	3.224*** (0.951)	−3.235 (2.477)
Observations	651	651	651
R^2	0.232	0.269	0.295
Adjusted R^2	0.212	0.241	0.26
Residual Std. Error	2.423 (df = 633)	2.377 (df = 626)	2.348 (df = 619)
F Statistic	11.268*** (df = 17; 633)	9.606*** (df = 24; 626)	8.348*** (df = 31; 619)

Note: * p<0.1; ** p<0.05; *** p<0.01; standard errors in parentheses

Table 4. Linear regression for the intention to adopt IMPULSE (DV 2).

	Model (1.4)	Model (1.5)	Model (1.6)
Age	0.004 (0.003)	0.007** (0.003)	0.007** (0.003)
Gender	−0.116 (0.084)	−0.166** (0.082)	−0.147* (0.082)
Edu$_{\text{HighSchool}}$	−0.467** (0.188)	−0.384** (0.188)	−0.383** (0.190)
Edu$_{\text{University}}$	−0.342** (0.154)	−0.273* (0.157)	−0.269* (0.157)
Income$_{Q2}$	0.464** (0.232)	0.314 (0.227)	0.342 (0.230)
Income$_{Q3}$	0.080 (0.212)	−0.030 (0.211)	−0.043 (0.213)
Income$_{Q4}$	0.203 (0.194)	0.034 (0.193)	0.045 (0.196)
Income$_{Q5}$	0.339* (0.175)	0.198 (0.174)	0.197 (0.178)
Income$_{\text{Refuse}}$	0.291 (0.209)	0.134 (0.206)	0.146 (0.208)
Place$_{\text{SmallMedium\_Town}}$	−0.148 (0.113)	−0.123 (0.111)	−0.128 (0.112)
Place$_{\text{City}}$	−0.127 (0.128)	−0.001 (0.130)	−0.011 (0.132)
Ethnicity$_{\text{Minority}}$	−0.065 (0.246)	−0.072 (0.243)	0.061 (0.254)

	Model (1.4)	Model (1.5)	Model (1.6)
Ethnicity$_{\text{Refuse}}$	−0.631*** (0.228)	−0.521** (0.224)	−0.495** (0.224)
TechAffinity	0.233*** (0.044)	0.205*** (0.044)	0.202*** (0.045)
PrivacyConcern	−0.049 (0.041)	−0.133*** (0.042)	0.256 (0.218)
DataSovereigntyPerception	0.336*** (0.072)	0.314*** (0.071)	0.326*** (0.071)
Usability	0.345*** (0.027)	0.322*** (0.027)	0.309*** (0.028)
Country$_{\text{Denmark}}$		−1.000*** (0.229)	0.936 (1.082)
Country$_{\text{Finland}}$		−0.698*** (0.245)	1.429 (1.220)
Country$_{\text{France}}$		−0.711*** (0.274)	1.573 (1.507)
Country$_{\text{Germany}}$		−0.880*** (0.193)	1.018 (1.051)
Country$_{\text{Iceland}}$		−0.927*** (0.228)	0.962 (1.135)
Country$_{\text{Italy}}$		−0.535*** (0.199)	1.886* (1.111)
Country$_{\text{Spain}}$		−0.329* (0.189)	0.910 (1.065)
PrivacyConcern:Country$_{\text{Denmark}}$			−0.444* (0.250)
PrivacyConcern:Country$_{\text{Finland}}$			−0.492* (0.292)
PrivacyConcern:Country$_{\text{France}}$			−0.516 (0.345)
PrivacyConcern:Country$_{\text{Germany}}$			−0.426* (0.232)
PrivacyConcern:Country$_{\text{Iceland}}$			−0.418 (0.255)
PrivacyConcern:Country$_{\text{Italy}}$			−0.558** (0.246)
PrivacyConcern:Country$_{\text{Spain}}$			−0.248 (0.233)
Constant	2.062*** (0.354)	3.074*** (0.404)	1.294 (1.051)
Observations	651	651	651
R^2	0.329	0.373	0.382
Adjusted R^2	0.31	0.348	0.35
Residual Std. Error	1.026 (df = 632)	0.997 (df = 625)	0.996 (df = 618)
F Statistic	17.221*** (df = 18; 632)	14.858*** (df = 25; 625)	11.933*** (df = 32; 618)

Note: * $p<0.1$; ** $p<0.05$; *** $p<0.01$; standard errors in parentheses

Age is significant in the regressions related to perceptions of IMPULSE (Table 3), with the negative sign expected by our *Hypothesis 1.1 Age*. Older people at least have a more negative *perception* of IMPULSE, which supports our hypothesis that they would be less likely to *accept* a new digital identity solution. However, in the following set of regressions that explore the decision whether or not to *switch to* IMPULSE (DV2, Table 4), the coefficient of Age becomes *positive* and once country effects are controlled for, it also becomes significant at the $p<0.05$ level. (Conversely, in the regressions related to perception, the statistical significance of Age *declined* once country effects are controlled for).

It is difficult to know how to interpret these somewhat inconsistent results. We suggest that they may best be taken to indicate that the explanatory power of *Age* for decisions surrounding acceptance/adoption is relatively small. In line with this, the coefficients of *Age* in both sets of regressions are small, meaning the variable's effect size is small. We therefore reject *Hypothesis 1.1 Age*. It is worth noting that age has no statistically significant effect on acceptance of FRT, either (see below).

Gender is not significant in the perception-regressions (Table 3) though it has a negative sign, which would be inconsistent with *Hypothesis 1.2 Gender*, that men are more likely to accept the new technology. It becomes weakly significant in the regressions about switching to IMPULSE ($p<0.1$, $p<0.05$) once country effects are controlled for (Table 4), which would likewise be contrary to *Hypothesis 1.2* since it implies that women, not men, are more likely to adopt the technology. One way to rationalise this result could be to argue that if men indeed are more likely to adopt new technology than women (as much IS research suggests) then there is a higher chance that they *already* possess digital identity solutions they are happy with, in turn making them less likely to adopt a new one that may not be that much more advanced than their present solution. That said, given the inconsistent and relatively weak significance levels, we reject the hypothesis. Again, *Gender* proves statistically not significant for acceptance of FRT (see below).

Education. In the perception-regressions (DV 1; Table 3), education is not significant, but in the adoption-regressions (DV 2; Table 4) it is statistically significantly and negatively associated with adopting IMPULSE for both high school-only ($p<0.05$) and university ($p<0.05$, falling to $p>0.1$ when country effects are controlled for). The somewhat higher significance level and slightly larger coefficients for high school education than university education in Models (1.4), (1.5) and (1.6) (adoption, DV 2) could be read as supporting *Hypothesis 1.4 Education*, that people with lower levels of education would be less likely to accept a new digital identity solution. However, in Models (1.1), (1.2) and (1.3) (perception, DV 1) the coefficient size is the reverse (larger negative coefficients for university than high school). More fundamentally, there is no obvious substantive explanation for why education should only negatively impact adoption, but not also perception. On balance, we therefore reject *Hypothesis 1.4 Education*. Education will also prove statistically not significant for the acceptance of FRT.

Income. Income at the level of the second quintile is statistically significantly and positively associated with a *positive perception* of IMPULSE (DV 1; $p<0.01$, falling $p<0.05$ with country effects), as is income at the fourth quintile level and the fifth quintile (though only in two models). Income at the third quintile level has no statistically significant effect. In the adoption-regressions (DV 2), only the second and fifth quintile are significant, and only when country effects are not controlled for. Refusal to disclose income is never significant. (In the regressions for FRT acceptance below, income is never significant.) In short, the income variable is only inconsistently significant – something for which there is no obvious substantive theoretical reason – and the strongest significance is at a relatively low level of income (second quintile), not the higher levels of income (fourth or fifth quintile) as *Hypothesis 1.3. Income* would predict. We therefore reject the hypothesis.

Place of abode is consistently not significant, across all models related to acceptance. We thus reject *Hypothesis 1.5 Place of abode*: We had expected people who live in villages or small towns to be less likely to accept a novel digital identity technology than people who live in major urban areas, but this is not supported by the data. At least in this data set, we find no evidence for a distinct effect of rurality. As we will see below, this also goes for acceptance of FRT: here too, rurality has no statistically significant effect. This suggests that apparent correlations between rurality and non-acceptance such as found in prior – non-statistical – studies like the TUM/Initiative D21 surveys may be spurious and driven by rurality correlating with other factors.

Ethnicity. Ethnic minority status (*Ethnicity_Minority*) as such is somewhat inconsistently significant. In the regressions for positive perception of IMPULSE, it is significant at the $p<0.05$ level in Model (1.1) and Model (1.2), and carries the negative sign predicted by *Hypothesis 1.7 Ethnic minority status*, that members of ethnic minorities should be less likely to accept a new digital identity solution. Once the *Country-PrivacyConcern interaction term* is added in Model (1.3) however, it ceases to be significant (though it retains the negative sign). In the regressions for the intention to adopt IMPULSE, ethnic minority status (*Ethnic_Minority*) is never significant. (It is also never significant in the FRT-acceptance regressions below). Conversely, *refusal* to disclose ethnic status (*Ethnicity_Refuse*) *is* consistently highly significant across the regressions and always carries a negative sign. In the perception-regressions, *Ethnicity_Refuse* is significant at the $p<0.01$ level in Models (1.1) and (1.2), falling to $p<0.05$ in Model (1.3); in the intention to adopt-regressions it is significant at the $p<0.01$ level in Model (1.4) and at the $p<0.01$ level in Models (1.5) and (1.6). (It is never significant in the FRT-acceptance regressions).

We interpret these results as follows: Refusal to disclose one's ethnicity cannot tell us anything about the ethnicity of the refuser. It therefore cannot provide evidence for or against *Hypothesis 1.7 Ethnic minority status*. Rather, refusal to disclose ethnicity reveals something about the respondent's attitudinal preferences, perhaps a particularly strong concern for privacy and suspicion of individuals or institutions who ask them to reveal sensitive data.[16] That *Ethnicity_Refuse* is significant across all the models thus indicates that to have this particular attitudinal preference reduces the acceptance of IMPULSE. That *Ethnicity_Minority* – which *does* measure minority status – is only inconsistently significant, conversely, suggests that this has at best weak explanatory power. We thus reject *Hypothesis 1.7. Ethnic minority status*.

Technology Affinity. Consistent with *Hypothesis 1.8. Technology Affinity*, the variable *TechAffinity* is significant at the $p<0.01$ level across all regressions related to acceptance of IMPULSE, with a positive sign. This provides strong evidence in favour of the hypothesis, and we thus accept it. (*TechAffinity* is also significant at the $p<0.01$ and $p<0.05$ level in several of the FRT-related regressions, something discussed further below.)

Privacy Concern is not significant in Model (1.1) and Model (1.4) of either the *Positive Perception* or the *Intention to Adopt* regressions. Once country effects are controlled for (Models 1.2 and 1.5) *PrivacyConcern* becomes significant, at the $p<0.05$ level for *Positive Perception* and the $p<0.01$ level for *Intention to Adopt*, with the negative sign predicted by *Hypothesis 1.9 Privacy Concern*. Substantively, we can interpret this as follows: contrary to *Hypothesis 1.9*, privacy concerns by themselves are *not* predictive of reduced acceptance of IMPULSE. Rather, in some country populations, privacy concerns go together with reduced acceptance of IMPULSE (i.e. here greater privacy concern reduces the likelihood of acceptance, as *Hypothesis 1.9* predicted), but in other country populations, high privacy concerns do not go together with reduced acceptance. This is supported also by the qualitative data, which suggests that at least in Bulgaria, high privacy concern can go together with high acceptance.[17] We thus do not accept Hypothesis 1.9.

To explore the country-specific structures further, we add the *Country-PrivacyConcern interaction term* (Models 1.3 and 1.6). Now the sign on *PrivacyConcern* becomes *positive* (in the *Positive Perception* regression, it also remains significant at the $p<0.05$ level). The interaction term itself is always negatively signed, and in the *Positive Perception* regressions, significant for all countries except Denmark. In the *Intention to Adopt* regression (Table 4), the interaction term

[16] Indeed, respondents who refused to disclose their ethnicity have an average privacy concerns score of 4.2, while the average score across the entire population of survey respondents is 3.7.

[17] Thus, Bulgarian respondents express both the highest intention to adopt IMPULSE, and the highest privacy concern.

is significant for Denmark, Finland, Germany and Italy. *Country,* meanwhile, turns positive and significant for most countries.

Understood literally, the negative and significant interaction term implies that being German, Icelandic, Italian, French, etc., *while also* having increased privacy concern, leads to lower acceptance of IMPULSE, while the positive sign on *Country* means that "just" being German, etc., without privacy concerns, leads to *increased* acceptance of IMPULSE, and the positive sign on *PrivacyConcern* implies that with all country effects netted out, "just" having greater privacy concern leads to greater acceptance of IMPULSE, too. Of course, these statistical results should *not* be taken so literally. Respondents who "just" have privacy concerns without also having a nationality (i.e. being German, French, Bulgarian, etc.) do not exist. Rather, these effects should be understood as indicating two things. Firstly, on the most general level, they show that no specific response to the question of acceptance follows systematically from heightened privacy concerns: evidently, these can go together both with acceptance and non-acceptance. Secondly, the results indicate that the effect of privacy concerns on acceptance seems to be heavily moderated by "country effects", i.e. something like nationally-specific cultures, experiences or discourses about privacy and new technologies.

Data Sovereignty. Consistent across all models and for both DVs, *DataSovereignty_Perception*, i.e. the belief that IMPULSE gives the user control over their data, is significant ($p<0.01$) with a positive sign and a large coefficient. Evidently, the belief that IMPULSE gives users sovereignty over their data strongly increases the likelihood of acceptance. We thus accept *Hypothesis 1.10 Data Sovereignty*.

Usability. Consistent with *Hypothesis 1.11 Usability*, the variable *Usability* is significant at the $p<0.01$ level across all regressions for the DV *Intention to Adopt* (Table 4). (In the *Positive Perception* regressions the Usability variable is not used, as it was constructed using several of the same items as the *Positive Perception* DV.) We thus accept *Hypothesis 1.11*.

Country Effects. In Models (1.2) and (1.5) for both *Positive Perception* and *Intention to Adopt*, the country variable is always negatively signed, and significant for Denmark ($p<0.01$ for both DVs), Finland (not significant in Model (1.4); significant at $p<0.01$ in Model (1.5)), France ($p<0.05$ and $p<0.01$), Germany (both $p<0.01$), Iceland (both $p<0.01$), Italy ($p<0.01$ for both), and Spain ($p<0.1$ for both). In Models (1.3) and (1.6), when the *Country-PrivacyConcern interaction effect* is added, *Country* itself becomes positive, but – except for Italy – is only still significant in the *Perception* regression (Model 1.3), and here for all countries except Denmark and Spain. Finally, it should be noted that in all the regressions, the coefficients on *Country* are always among or even the largest of all variables' coefficients, meaning that the statistical effect is big. Put together, these results mean firstly that we can accept *Hypothesis 1.6. Country effects*: country effects do impact acceptance in large and statistically significant ways. Secondly, the negative signs mean – both statistically and substantively – that, other things equal, respondents from Denmark, Finland, France, Germany, Iceland, Italy and Spain are less likely than respondents from Bulgaria to accept IMPULSE, something borne out also by the qualitative data which showed that Bulgarians expressed the highest average intention of switching to IMPULSE (cf. Figure 1). In other words, country effects matter, but their direction seems to be country-specific.

5 Results: Acceptance of facial recognition technology (FRT)

5.1 Descriptive analysis

As we have seen, for a subset of the respondent population, IMPULSE's use of FRT was at least one factor prompting them to reject adopting IMPULSE. But what of respondents' general acceptance/rejection of FRT as an authentication technology and its determinants? As noted, to explore this, we first asked respondents whether they had used different authentication technologies, including FRT, and then asked them to select their three preferred technologies. In Figure 3 we show for each technology how many respondents had used it, and how many selected it as one of their three preferred technologies (multiple answers possible). For each technology, we next calculate the "rejection rate", namely the percentage of respondents who have had experience using it who did *not* select it as one of their preferred technologies (Figure 4). We may understand this percentage as an indicator of how positive the usage experience for each technology seems to be: the better the average user experience, the smaller the "rejection rate" is be expected to be. Conversely, the *higher* this percentage, the *fewer* users the technology can evidently convince. As can be seen, iris and facial recognition have the *lowest* rejection rates, followed by fingerprint recognition and username/password solutions. Conversely, voice recognition, smartcard/PIN and PIN/TAN have the highest rejection rates.

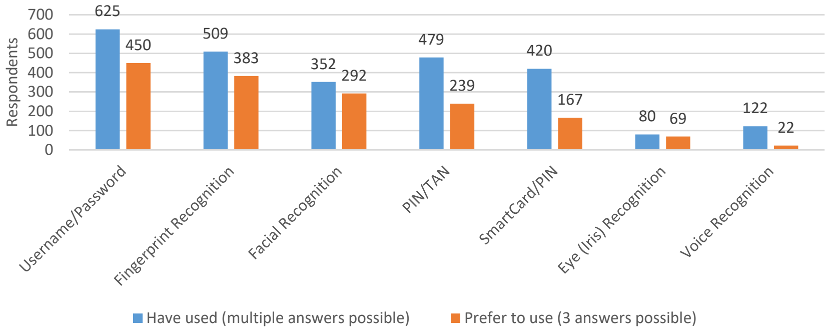


Figure 3. Experience and usage preferences for different authentication technologies

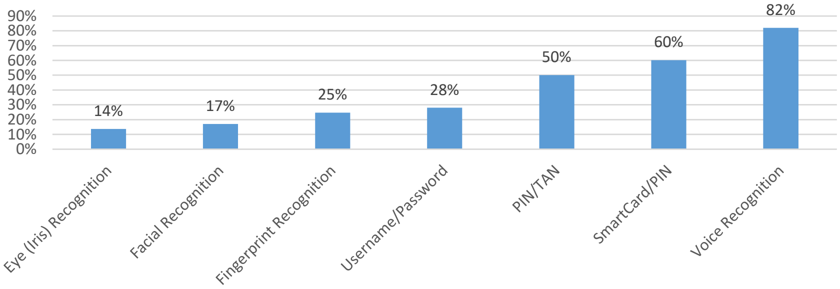


Figure 4. Rejection rate for different authentication technologies

Evidently, username and password is the most widely used authentication technology among the survey population, followed by fingerprint recognition, PIN/TAN, smartcard/PIN, and facial recognition. Significantly fewer respondents had experience with voice or iris recognition (Figure 3). As regards their popularity as measured by the share of rejecters, iris and facial recognition stand out as the most popular, with only 14% and 17% rejecters, respectively. Username/password comes in third, at 28% rejecters. Conversely, voice recognition records the highest share of rejecters (i.e., seems to be the least popular), 82%, followed by smartcard/PIN (60%) and PIN/TAN (50%).

5.2 Regression analysis

We next conducted regression analysis of the determinants of acceptance of FRT, using logit regression.

Dependent variable

The dependent variable, *Preference for Facial Recognition*, is a binary variable that takes the value of 1 if a respondent had selected FRT as one of their preferred authentication technologies, and 0 if they had not.

Explanatory variables

The explanatory variables are the same as used in the previous regressions, plus three additional variables

- *FacialRecognition_Exp:* a binary variable that takes the value of 1 if the respondent has used FRT, and 0 if they have not.
- *FingerPrint_Exp:* a binary variable that takes the value of 1 if the respondent has used fingerprint recognition, and 0 if they have not.
- *AnyBiometric_Excpt_FRT:* a binary variable that takes the value of 1 if the respondent has used any of the biometric technologies other than FRT, and 0 if they have not.

Results

Table 5 presents the results. The socio-demographic variables – *Age, Gender, Education, Income, Place of Abode, and Ethnic Minority* – are not significant across all models. We thus reject *Hypotheses 2.1* (age), *2.2* (gender), *2.3* (income), *2.4* (education), *2.5* (place of abode) and *2.7* (ethnic minority status).

The country variable is significant at the $p<0.05$ and $p<0.01$ levels, respectively, for France, Germany, Iceland, Italy and Spain, across all models. In other words, the respondents from these countries are significantly less likely to accept FRT for authentication than respondents from Bulgaria are. We therefore accept *Hypothesis 2.6*, that country effects are often strong and significant. Interestingly, the country variable is *not* significant for Denmark and Finland (though it remains directionally negative in most specifications), indicating that statistically, these respondents are *not* more unlikely than the Bulgarian respondents to accept FRT for authentication.

In Model (2.1), *Technology Affinity* is significant at the $p<0.01$ level, with a positive coefficient. However, once prior use with FRT (*FacialRecognition_Exp*) is controlled for in Model (2.2), *Technology Affinity* ceases to be significant, though its coefficient remains positive. Interestingly, once prior experience with FRT is replaced with prior experience with fingerprint recognition (*FingerPrint_Exp*) (Model 2.3), *Technology Affinity* again becomes significant, albeit only at the $p<0.05$ level and with a slightly smaller coefficient compared to Model (2.1). The same is true when prior experience with FRT is replaced with prior experience with any other biometric (*AnyBiometric_Excpt_FRT*) (Model 2.4). A plausible explanation for this could be that the people with high tech affinity are also disproportionately likely to have *already* used FRT (precisely because they are keen on new technology). While in a statistical sense, prior experience with FRT (*FacialRecognition_Exp*) thus soaks up much of the statistical significance of the *Technology Affinity* variable, substantively, the causality is more likely to run from tech affinity to prior experience (to acceptance). In other words, substantively, tech affinity is still likely to be doing much of the causal work. We therefore accept *Hypothesis 2.8* that people with a greater affinity for new technology are more likely to accept FRT for authentication than people without or with less of such an affinity.

PrivacyConcern is consistently significant throughout all models at the p<0.05 level, with the negative sign expected by *Hypothesis 2.9*. We therefore accept *Hypothesis 2.9*, stipulating that greater privacy concern lowers acceptance of FRT.

Table 5. Logit regression for decision to use facial recognition technology (FRT).

	Model (2.1)	Model (2.2)	Model (2.3)	Model (2.4)	Model (2.5)	Model (2.6)
Age	−0.007 (0.007)	−0.001 (0.007)	−0.002 (0.007)	−0.002 (0.007)	−0.0001 (0.008)	−0.0003 (0.008)
Gender	−0.036 (0.176)	0.041 (0.192)	−0.024 (0.178)	−0.022 (0.178)	0.041 (0.192)	0.041 (0.192)
Edu$_{\text{HighSchool}}$	−0.180 (0.413)	−0.254 (0.441)	−0.201 (0.417)	−0.189 (0.417)	−0.254 (0.441)	−0.254 (0.441)
Edu$_{\text{University}}$	0.497 (0.343)	0.402 (0.366)	0.504 (0.345)	0.510 (0.345)	0.405 (0.366)	0.406 (0.366)
Income$_{Q2}$	0.164 (0.501)	0.397 (0.536)	0.252 (0.507)	0.297 (0.507)	0.402 (0.536)	0.410 (0.537)
Income$_{Q3}$	0.391 (0.466)	0.410 (0.504)	0.461 (0.475)	0.454 (0.473)	0.414 (0.504)	0.416 (0.504)
Income$_{Q4}$	−0.041 (0.428)	−0.091 (0.461)	−0.059 (0.435)	−0.031 (0.433)	−0.096 (0.462)	−0.089 (0.461)
Income$_{Q5}$	0.444 (0.388)	0.388 (0.418)	0.396 (0.396)	0.422 (0.394)	0.378 (0.419)	0.386 (0.418)
Income$_{\text{Refuse}}$	0.313 (0.456)	0.278 (0.495)	0.339 (0.463)	0.368 (0.462)	0.276 (0.495)	0.284 (0.495)
Place$_{\text{SmallMedium\_Town}}$	−0.097 (0.238)	−0.232 (0.261)	−0.132 (0.242)	−0.119 (0.242)	−0.234 (0.261)	−0.231 (0.261)
Place$_{\text{City}}$	0.196 (0.280)	0.123 (0.305)	0.173 (0.284)	0.180 (0.283)	0.120 (0.305)	0.122 (0.305)
Ethnicity$_{\text{Minority}}$	0.005 (0.549)	−0.229 (0.593)	0.052 (0.551)	0.075 (0.552)	−0.221 (0.594)	−0.218 (0.594)
Ethnicity$_{\text{Refuse}}$	−0.589 (0.551)	−0.752 (0.591)	−0.515 (0.561)	−0.499 (0.563)	−0.747 (0.592)	−0.745 (0.592)
TechAffinity	0.297^{***} (0.096)	0.150 (0.104)	0.236^{**} (0.098)	0.238^{**} (0.098)	0.144 (0.105)	0.145 (0.105)
PrivacyConcern	$−0.223^{**}$ (0.091)	$−0.202^{**}$ (0.098)	$−0.212^{**}$ (0.092)	$−0.205^{**}$ (0.092)	$−0.201^{**}$ (0.098)	$−0.201^{**}$ (0.098)
Country$_{\text{Denmark}}$	0.004 (0.488)	−0.402 (0.534)	−0.116 (0.497)	−0.109 (0.498)	−0.415 (0.535)	−0.412 (0.535)
Country$_{\text{Finland}}$	−0.420 (0.517)	−0.261 (0.566)	−0.569 (0.530)	−0.564 (0.531)	−0.290 (0.569)	−0.284 (0.569)
Country$_{\text{France}}$	$−1.602^{***}$ (0.598)	$−1.660^{**}$ (0.656)	$−1.733^{***}$ (0.611)	$−1.737^{***}$ (0.612)	$−1.673^{**}$ (0.657)	$−1.672^{**}$ (0.657)
Country$_{\text{Germany}}$	$−1.631^{***}$ (0.417)	$−1.711^{***}$ (0.460)	$−1.619^{***}$ (0.427)	$−1.657^{***}$ (0.428)	$−1.710^{***}$ (0.461)	$−1.716^{***}$ (0.461)
Country$_{\text{Iceland}}$	$−1.232^{**}$ (0.481)	$−1.694^{***}$ (0.527)	$−1.360^{***}$ (0.492)	$−1.393^{***}$ (0.493)	$−1.704^{***}$ (0.528)	$−1.707^{***}$ (0.529)
Country$_{\text{Italy}}$	$−1.254^{***}$ (0.421)	$−1.453^{***}$ (0.468)	$−1.389^{***}$ (0.433)	$−1.392^{***}$ (0.433)	$−1.471^{***}$ (0.470)	$−1.468^{***}$ (0.470)
Country$_{\text{Spain}}$	$−0.865^{**}$ (0.401)	$−1.003^{**}$ (0.444)	$−0.934^{**}$ (0.412)	$−0.949^{**}$ (0.413)	$−1.013^{**}$ (0.446)	$−1.014^{**}$ (0.446)
FacialRecognition_Exp		1.835^{***} (0.197)			1.795^{***} (0.211)	1.802^{***} (0.212)
FingerPrint_Exp			0.997^{***} (0.251)		0.146 (0.284)	
AnyBiometric_Excpt_FRT				1.037^{***} (0.266)		0.123 (0.303)
Constant	0.022 (0.862)	−0.431 (0.924)	−0.708 (0.892)	−0.792 (0.897)	−0.519 (0.941)	−0.514 (0.947)
Observations	651	651	651	651	651	651

	Model (2.1)	Model (2.2)	Model (2.3)	Model (2.4)	Model (2.5)	Model (2.6)
Log Likelihood	-408.356	-359.437	-399.852	-400.008	-359.304	-359.354
Akaike Inf. Crit.	864.711	768.875	849.703	850.016	770.608	770.709

Note: * $p<0.1$; ** $p<0.05$; *** $p<0.01$; standard errors in parentheses

Prior use experience of FRT (*FacialRecognition_Exp*) is strongly significant across all models in which the variable appears, at the $p<0.01$ level and with a large coefficient and a positive sign. We thus accept *Hypothesis 2.10*, that prior use of FRT makes people more likely to accept FRT.

Conversely, prior use experience of fingerprint recognition (*FingerPrint_Exp*, Model 2.3) and of other biometrics except FRT (*AnyBiometric_Excpt_FRT*, Model 2.4) are significant only until Prior use experience of FRT (*FacialRecognition_Exp*) is included in the model (Models 2.5 and 2.6). In other words, the significance of *FingerPrint_Exp* and *AnyBiometric_Excpt_FRT* in Models (2.3) and (2.4) seems to have been largely due to these variables including significant numbers of people who had also had prior experience of FRT, which was doing the causal work. We interpret that as suggesting that respondents do *not* in fact treat the different biometric technologies as in some sense part of a single class, with (positive) usage experiences "translating" between technologies. Having used one biometric technology does not seem to make a respondent more likely to accept a different biometric technology. We thus reject *Hypothesis 2.11*.

6 Concluding discussion

6.1 Theoretical contributions

This paper has examined the factors determining whether individuals will adopt a new digital identity technology (RQ 1) and adopt facial recognition technology (FRT) for authentication (RQ 2). To do so, the paper analysed survey data collected as part of the IMPULSE project. We formulated hypotheses to direct our research. Final results of the hypotheses formulated are presented in Table 6. Our contributions are as follows.

Table 6. Hypotheses results overview

Explanatory Variables	Dependent Variables	Acceptance of digital identity solution: Hypothesis number and expected relationship	Acceptance of FRT: Hypothesis number and expected relationship
Socio-demographic variables	Age	1.1 (−) rejected	2.1 (−) rejected
	Gender	1.2 (women: −) rejected	2.2 (−) rejected
	Income	1.3 (+) rejected	2.2 (+) rejected
	Education	1.4 (+) rejected	2.4 (+) rejected
	Place of abode	1.5 (rural: −) rejected	2.5 (rural: −) rejected
	Country effects	1.6 (▪) accepted	2.6 (▪) accepted
	Ethnic minority status	1.7 (minority: −) rejected	2.7 (−) rejected
Attitudinal variables	Technology affinity	1.8 (+) accepted	2.8 (+) accepted
	Privacy concerns	1.9 (−) rejected	2.9 (−) accepted

Explanatory Variables	Dependent Variables	Acceptance of digital identity solution: Hypothesis number and expected relationship	Acceptance of FRT: Hypothesis number and expected relationship
	Data sovereignty	1.10 (+) accepted	N.A.
	Usability	1.11 (+) accepted	N.A.
	Prior Use of FRT	N.A.	2.10 (+) accepted
	Prior use of other biometric technologies	N.A.	2.11 (+) rejected

Note: “ ▪ “ means that while we expect the variable to be significant, no prediction as to the direction of the effect seemed possible

Firstly, we find that socio-demographic variables (age, gender, education, income, place of abode and ethnicity) had little explanatory power. They were never significant for FRT, and only occasionally and inconsistently so for adoption of new digital identity technology. This runs counter to prior work, which has repeatedly suggested that these are important factors for driving adoption. It is unclear what accounts for this difference in findings. One possibility is that it is largely an effect of poor-quality data (see Limitations below), and that a fully representative sample would come to different conclusions. But it is also possible that these factors simply are not that important, at least in comparison to attitudinal and experiential variables as well as usability. It is notable, for instance, that socio-demographic variables are only inconsistently significant in Kostka et al. (2021) cross-country analysis of acceptance of FRT for law enforcement.

Secondly, we find that, on the contrary, it is precisely attitudinal and experiential variables, and usability, that are consistently significant. Technology affinity, perceptions of gaining data sovereignty and usability (in the case of the digital identity solution) as well as prior usage experience (in the case of FRT) are consistently highly significant across all our regressions. For developers this underscores the importance of user-friendly design and of facilitating (and advertising) the degree to which their solutions provide users with real control over their data. For governments and others wishing to encourage uptake of new technology, it emphasises the importance of encouraging positive views and interest in technology in general (technology affinity). For companies, it indicates the importance of providing (potential) users with low-threshold opportunities to try out new tech and thus gain usage experience.

Thirdly, we find that privacy concerns have surprisingly weak and country-dependent statistical effects on the acceptance of new digital identity solutions, though the effect is stronger for FRT. This is somewhat counter-intuitive, as one might expect individuals who are strongly privacy-conscious to be more cautious about adopting new-fangled identity solutions (especially if they also utilise FRT, as was the case here). Yet this is not quite what the regressions find. Rather, privacy concerns seem to be filtered through some form of country effects, with high privacy concern – at least in some countries – apparently going together with enthusiasm for new digital identity solutions. This suggests a larger point: “privacy” is a complex, multi-faceted and situational concept (Nissenbaum 2004). Digital technology and the contexts in which it is used, too, have become very complex and varied. Thus it would not be surprising if people interpret the meaning and implication of privacy concerns as they pertain to a new technology differently depending on their (national) context. That context should vary *nationally* in this regard is not surprising, since the public and everyday cultures and discourses by which people make sense of their lives, and the institutional framework conditions that shape them, remain heavily national.

Fourthly, we find that country effects matter, across all regressions. Respondents from different countries manifested varying levels of interest in adopting new digital identity technology, and varying levels of acceptance of FRT for authentication. It is unclear what is driving these variations or rather, what is going on "under the hood" of "country effects". The "country" variable is a compound item[18], that can in principle capture many different factors that vary nationally in some way. That could include, for example, (different) public discourses about the threats and opportunities presented by novel technologies, varying attitudes towards and trust in the state and public and private institutions as well as society at large, diverging positive and negative historical experiences with state power and state capacity in general, different prior experiences of digital technology and ecosystems, and different perceptions of need. As our data is not fine-grained enough to disentangle what the "country effects" variable is capturing, we can only speculate. As noted above for example, it is possible that lower interest in adopting the IMPULSE system in Finland, Denmark and Iceland compared to Bulgaria or Spain, is related to the existence of established digital identity systems in the former countries, and lack thereof in the latter. Conversely, the relatively low levels of privacy concerns (Figure 4) manifested by Scandinavian and Finnish respondents and comparatively less-negative reaction to FRT for authentication of Danish and Finnish respondents in particular could plausibly be linked to the relatively high levels of trust in institutions found in these countries (European Commission 2024). However, this deserves further study.

Fifthly and finally, we find that prior experience does not seem to "travel" between different biometric technologies. While prior experience with FRT has a strongly significant impact on the decision whether to want to use FRT in future, prior experience with other biometric technologies does not seem to have this effect. In other words, while analysts frequently discuss biometric technologies *as a class* of closely related technologies – which implies that often, what goes for one technology that is a member of this class, may go for other members too – users may draw sharper contrasts between them. Rather than to form views about biometric technologies *in general*, *as a class*, users may tend to form views about individual biometric technologies, without necessarily applying a view formed about one of these technologies to another.

6.2 Managerial and policy implications

Across the regressions, six variables stand out as particularly important for driving adoption of the IMPULSE solution and acceptance of FRT for authentication: technology affinity, data sovereignty, usability, prior experience with biometric technology and country effects. For business, this has implications for go-to-market strategies and value proposition. Several of these implications are truisms, albeit truisms frequently overlooked at considerable financial cost: the importance of careful market research prior to entering new countries as receptiveness to a product can vary sharply; the role of technophile early adopters for driving initial sales, and of usability.

Perhaps less obvious is the implication of the critical role of prior experience: it suggests that when marketing a novel technology, giving the public at large ample opportunities to just play around and become familiar with the technology may be critical for reducing fears and making people open to adopting the technology. Also maybe less obvious, given the well-attested privacy paradox in consumer behaviour (Adjerid et al. 2018) is the high value people seem to place on having "control" (sovereignty) over their data and the degree to which it may drive purchasing decisions. This suggests that a potentially lucrative market niche may exist for "data sovereign" products. Yet given the ambiguities surrounding notions of data sovereignty (Martin and Metzger

[18] We thank an anonymous reviewer for making this point.

2024) and the difficulty for consumers to track what is really happening with their data, it is critical that businesses exploit this niche responsibly. Among other things, that means not making attractive-sounding but effectively fallacious claims (ibid.). The same applies to policy makers, especially in the European Union, which is currently promoting digital identity solutions with reference to data sovereignty.

The role of country effects suggests a further implication for EU and European policy makers: So far, efforts to create a single digital market in Europe have mainly focused on creating common institutions and regulations. Yet cross-country divergencies in attitudes and behaviour towards novel digital technologies may also constitute important hindrances to market integration and the economic and technological dynamism that the EU hopes to thus unlock. Better understanding the causes of these divergencies thus appears worthwhile. It may be that beyond institutional and regulatory harmonisation, fostering a common digital culture may also be needed to make a truly integrated single digital market possible.

6.3 Limitations and future work

The research presented here has at least three important limitations, which all relate to the underlying data. One is the technique by which the data was collected, namely convenience sampling, and the resultant biases in the data. As discussed, the sample was disproportionately drawn from more educated and more affluent respondents. But there may also be other, more hidden biases that we are unaware of. At the same time, the chosen analytical method – regression analysis – helps to somewhat counterbalance this problem, since statistical analysis does not assume a perfectly representative data set.

Secondly, the study revealed country-specific effects to be important but was itself not fine-grained enough to analyse these more deeply. As the purpose of controlling for country-specific effects is to avoid unobserved factors biasing results, this is not per se a problem for the analysis. However, clearly it would be desirable to know much more about what is going on here, and this is an important avenue for further research.

The third limitation in the data concerns the fact that it was drawn from a survey asking respondents for their views of a specific digital identity solution (IMPULSE), and the analytical conclusions are extrapolated from this. On the one hand, this is hard to avoid: digital identity solutions *are* specific, concrete hardware/software artefacts, and thus to get data on user adoption decisions, one must present users with concrete instantiations of such digital identity solutions. Moreover, given the cost involved in building such solutions – and the time and respondent attention span required to describe different digital identity solutions to survey respondents – it is usually not feasible to present users with more than one or at most a couple of such solutions. That however means that survey respondents are then not answering questions about digital identity solutions *in general*, but about one or a few specific systems, that have particular attributes and lack other attributes. The researcher then has the challenge of abstracting from these solution-specific responses to digital identity solutions in general. This implies that the insights gained and presented in this study might only travel to a limited extent to digital identity solutions other than IMPULSE. That said, IMPULSE instantiates core features of the novel digital identity solutions coming onto the market today (i.e., smartphone app, digital wallet, biometric recognition usually based on FRT). It therefore appears likely that the conclusions drawn in this paper from the survey about IMPULSE will apply more broadly, to other digital identity solutions also. Of course, more developed commercial offerings in particular may also include additional features that may impact user adoption (e.g. loyalty rewards, further services, gamification, . . .). The present paper can tell us little about the effects of such (hypothetical) additional features. But conversely, such additional features are likely to become increasingly product-specific (their point being after all to *differentiate* the offering), in turn complicating generalisation and complicating inference.

The paper indicates several avenues for future work. For one, variations in how people in different national or other contexts understand privacy and privacy risks/concerns, and how these in turn affect possibly diverging patterns of technology acceptance and adoption deserve further empirical study. In particular, it is interesting that at least among respondents from certain countries, high affinity for new technology and openness to new solutions using sensitive data (i.e., facial recognition) seems to go together with high privacy concerns. This appears paradoxical, as conventionally privacy concerns and openness to new and "risky" technology are thought of as opposites. More broadly, the way that national contexts ("country effects") may shape diverging responses to new technology provides an interesting avenue for further work. These could also be important avenues for qualitative research focused on teasing out the different narratives and logics by which people make sense of novel technology and its risks, and the institutional and historical contexts these are grounded in.

Acknowledgements

We would like to acknowledge and thank Thomas Jackwerth-Rice, formerly of Fraunhofer ISI, and Diana Silvestru, formerly of AEI Austria, for contributing to the design of the survey instrument, and the members of the IMPULSE project consortium for support with disseminating the survey. We would also like to thank three anonymous reviewers for their comments, and the editors of JIM for excellent support with finalising the manuscript.

Funding disclosure

This research was supported by the European Commission, Grant Agreement 101004459, as part of the Horizon 2020 Identity Management in PubLic SErvices (IMPULSE) Project (www.impulse-h2020.eu).

7 References

Ada Lovelace Institute (2019). Beyond face value: public attitudes to facial recognition technology. https://www.adalovelaceinstitute.org/report/beyond-face-value-public-attitudes-to-facial-recognition-technology/

Adjerid, I., Peer, E., & Acquisti, A. (2018). Beyond the Privacy Paradox. Objective Versus Relative Risk in Privacy Decision Making, *MIS Quarterly, 42*(2), 465-488.

Barth, S., & De Jong, M. D. (2017). The privacy paradox–Investigating discrepancies between expressed privacy concerns and actual online behavior–A systematic literature review. *Telematics and informatics, 34*(7), 1038-1058.

Hu, Bo and Liu, Yu-li & Yan, Wenjia, Should I Scan My Face? The Influence of Perceived Value and Trust on Chinese Users' Intention to Use Facial Recognition Payment. In *23rd Biennial Conference of the International Telecommunications Society (ITS): "Digital societies and industrial transformations: Policies, markets, and technologies in a post-Covid world", Online Conference / Gothenburg, Sweden.* Available at SSRN: https://ssrn.com/abstract=4061630 or http://dx.doi.org/10.2139/ssrn.4061630

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS quarterly, 13*(3), 319-340.

Eaton, B., Hedman, J., & Medaglia, R. (2018). Three different ways to skin a cat: financialization in the emergence of national e-ID solutions. *Journal of Information Technology, 33*(1), 70-83.

Echikson, W. (2020). Europe's Digital Identification Opportunity. *The Centre for European Policy Studies (CEPS)*

European Commission (n.d.). Electronic Identities - a brief introduction. European Commission. Brussels https://ec.europa.eu/information_society/activities/ict_psp/documents/eid_introduction.pdf

European Commission (2024). Public opinion in the European Union. EuroBarometer Report April-May 2024. https://veriangroup.com/hubfs/BE/Eurobarometer/Standard-101-Spring%202024.pdf

Felden, F., Zelt, T., Bauer, P., Siegert, S., Einaste, T., Müller, M., ... & Hoffmann, T. (2020). Zehn Jahre elektronischer Personalausweis; Wie Deutschland ein erfolgreiches eID-Ökosystem aufbauen kann. Boston Consulting Group and Nortal.

Fletcher, J., Howard, P., Mody, D., Vyas, A., & Eng, H. (2017). A study of biometric security technology acceptance and primary authentication. *Proceedings of student-faculty research day*. https://www.semanticscholar.org/paper/A-Study-of-Biometric-Security-Technology-Acceptance-Fletcher-Howard/2c91e7c778d6dd92729a408d983314aa5fc56118

Förster, Katrin (2024). Extending the technology acceptance model and empirically testing the conceptualised consumer goods acceptance model, In: *Heliyon 10*(6), pp. 1-13.

Gritzalis, S., & Lambrinoudakis, C. (2008). Privacy in the digital world. In *Encyclopedia of Internet Technologies and Applications* (pp. 411-417). IGI Global Scientific Publishing.

Gustafsson, M., & Elin, W. (2013). Safe Online e-Services Building Legitimacy for E-government. A Case Study of Public E-services in Education in Sweden. *JeDEM-eJournal of eDemocracy and Open Government, 5*(2), 155-173.

Hedström, K., Wihlborg, E., Gustafsson, M. S., & Söderström, F. (2015). Constructing identities–professional use of eID in public organisations. *Transforming Government: People, Process and Policy, 9*(2), 143-158.

Hilowle, M. M., Yeoh, W., Grobler, M., Pye, G., & Jiang, F. (2022). Towards Improving the Adoption and Usage of National Digital Identity Systems. In *Proceedings of the 37th IEEE/ACM International Conference on Automated Software Engineering* (pp. 1-6).

Horvath, L., Banducci, S., Blamire, J., Degnen, C., James, O., Jones, A., ... & Tyler, K. (2022). Adoption and continued use of mobile contact tracing technology: multilevel explanations from a three-wave panel survey and linked data. *BMJ open, 12*(1), e053327.

Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. *IEEE Transactions on circuits and systems for video technology, 14*(1), 4-20.

Korir, M., Parkin, S., & Dunphy, P. (2022). An empirical study of a decentralized identity wallet: Usability, security, and perspectives on user control. In *Eighteenth symposium on usable privacy and security (SOUPS 2022)* (pp. 195-211).

Kostka, G., Steinacker, L., & Meckel, M. (2021). Between security and convenience: Facial recognition technology in the eyes of citizens in China, Germany, the United Kingdom, and the United States. *Public Understanding of Science, 30*(6), 671-690.

Krol, K., Parkin, S., & Sasse, M. A. (2016). "I don't like putting my face on the Internet!": An acceptance study of face biometrics as a CAPTCHA replacement. In *2016 IEEE International Conference on Identity, Security and Behavior Analysis (ISBA)* (pp. 1-7). https://doi.org/10.1109/ISBA.2016.7477235

Mahula, S., Tan, E., & Crompvoets, J. (2021, June). With blockchain or not? Opportunities and challenges of self-sovereign identity implementation in public administration: Lessons from the Belgian case. In *Proceedings of the 22nd Annual International Conference on Digital Government Research* (pp. 495-504).

Martin, N., & Metzger, F. M. (2024). The chimera of control: Self-sovereign identity, data control, and user perceptions. *Human Technology, 20*(2), 183-223.

Martin, N., Pullmann, L., & Blind, K. (2023). *D4.4 Economic Benefits of the IMPULSE Approach – V2*, Deliverable No. 4.4, submitted as part of the IMPULSE project. Available at https://www.impulse-h2020.eu/public-deliverables/

Morales, A., Ferrer, M. A., Travieso, C. M., & Alonso, J. B. (2010). About user acceptance in hand, face and signature biometric systems. *Jornadas de Reconocimiento Biometrico de Personas*

Mühle, A., Grüner, A., Gayvoronskaya, T., & Meinel, C. (2018). A survey on essential components of a self-sovereign identity. *Computer Science Review, 30*, 80-86.

Naik, N., & Jenkins, P. (2020). Governing principles of self-sovereign identity applied to blockchain enabled privacy preserving identity management systems. In *2020 IEEE International Symposium on Systems Engineering (ISSE)* (pp. 1-6). IEEE.

Nissenbaum, H. (2004). Privacy as Contextual Integrity, *Washington Law Revie, 79*(1). Available at: https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10

NIST (n.d.). Authentication. NIST (Computer Security Resource Center Glossary) https://csrc.nist.gov/glossary/term/authentication, accessed 03.01.2023.

PricewaterhouseCoopers (PWC) (2021). Der Online-Ausweis auf dem Smartphone und die digitale Brieftasche.

Pöhn, D., Grabatin, M., & Hommel, W. (2021). eID and self-sovereign identity usage: an overview. *Electronics, 10*(22), 2811.

Rouidi, M., Hamdoune, A., Choujtani, K., & Chati, A. (2022). TAM-UTAUT and the acceptance of remote healthcare technologies by healthcare professionals: A systematic review. *Informatics in Medicine Unlocked, 32*, 101008.

Spiekermann, S., & Korunovska, J. (2017). Towards a value theory for personal data. *Journal of Information Technology, 32*(1), 62-84.

Trüdinger, E. M., & Steckermeier, L. C. (2017). Trusting and controlling? Political trust, information and acceptance of surveillance policies: The case of Germany. *Government Information Quarterly, 34*(3), 421-433.

TUM/Initiative D21 (2018): eGovernment MONITOR 2020. Staatliche Digitalangebote – Nutzung und Akzeptanz in Deutschland, Österreich und der Schweiz. Initiative D21 & Technische Universität München

TUM/Initiative D21 (2019). eGovernment MONITOR 2020: Staatliche Digitalangebote – Nutzung und Akzeptanz in Deutschland, Österreich und der Schweiz. Initiative D21 & Technische Universität München

TUM/Initiative D21 (2020). eGovernment MONITOR 2020: Staatliche Digitalangebote – Nutzung und Akzeptanz in Deutschland, Österreich und der Schweiz. Initiative D21 & Technische Universität München

TUM/Initiative D21 (2021). eGovernment Monitor 2021: Staatliche Digitalangebote - Nutzung und Akzeptanz in Deutschland, Österreich und der Schweiz. Initiative D21 & Technische Universität München

TUM/Initiative D21 (2022). eGovernment Monitor 2022: Nutzen und akzeptieren Bürger*innen die digitale Verwaltung? Die deutschen Bundesländer, Deutschland, Österreich und die Schweiz im Vergleich. Initiative D21 & Technische Universität München

TUM/Initiative D21 (2023). eGovernment MONITOR 2020: Staatliche Digitalangebote – Nutzung und Akzeptanz in Deutschland, Österreich und der Schweiz. Initiative D21 & Technische Universität München

Vassil, K. (2015). Estonian e-Government Ecosystem: Foundation, Applications, Outcomes. In: *World Development Report 2016*. [online] Available at: http://pubdocs.worldbank.org/en/165711456838073531/WDR16-BPEstonian-eGov-ecosystem-Vassil.pdf

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view, *MIS Quarterly, 27*(3), pp. 425-478.

Venkatesh, V., Thong, J. Y., & Xu, X. (2012). Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology. *MIS quarterly, 36*(1), 157-178.

White, O., Sperling, O., Madgavkar, A., Manyika, J., Bughin, J., Mahajan, D., McCarthy, M. (2019). Digital identification: A key to inclusive growth. McKinsey Global Institute. https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20identification%20A%20key%20to%20inclusive%20growth/MGIDigital-identification-Report.ashx

Woolley, K. E., Bright, D., Ayres, T., Morgan, F., Little, K., & Davies, A. R. (2023). Mapping inequities in digital health technology within the World Health Organization's European region using PROGRESS PLUS: scoping review. *Journal of medical Internet research, 25*, e44181. https://doi.org/10.2196/44181

World Bank Group (2019). Global ID Coverage, Barriers, and Use by the Numbers: World Bank, Washington, DC

Zimmermann, V., & Gerber, N. (2020). The password is dead, long live the password–A laboratory study on user perceptions of authentication schemes. *International Journal of Human-Computer Studies, 133*, 26-44.

8 Appendix

8.1 Appendix A: Survey Instrument

The text was translated into the languages of the countries surveyed.

Introduction

Thank you for your help!

This survey is conducted by a group of researchers at institutes and universities in Finland, Germany and Austria. Our survey is for a scientific project funded by the European Union. We want to understand what people think about online public services, computers and smartphones, and how they use them. This will help us develop new technology and improve public services online.

By taking the survey, you provide really important input for our research!

The survey is completely anonymous. No information you share can be traced to you, nor can you be traced by any information you provide. You can also withdraw from the survey at any point.

For each completed survey, we will donate 2€ to one of several charities (you can pick!), up to a total of €500 Euros.

Let me thank you again for support

Nicholas Martin, Fraunhofer ISI, Germany

If you have any questions, please feel free to contact me at nicholas.martin@isi.fraunhofer.de

To learn more about our research project, visit https://www.impulse-h2020.eu/

Section 1: Demographics

To understand survey results better, we would first like to collect some background information.

Q1. How old are you?

- Free text box

Q2. What is your gender

- Female
- Male
- Diverse

Q3. What is your highest level of education?

- Completed primary school
- Completed secondary school
- Completed post-secondary school vocational training
- Completed university
- Currently at university
- Currently in post-secondary school vocational training

Q4: What is your annual household income, after tax?

(country-specific quintiles, based on Eurostat data)

- Less than X
- X+1 to XX
- XX+1 to XXX
- XXX+1 to XXXX
- More than XXXX+1
- Prefer not to answer

Q5. What is your citizenship?

- Citizen of [*survey country*]
- Permanent resident of [*survey country*]
- Migrant / non-permanent residency
- Prefer not to answer

Q6. Due to discrimination and for other reasons, minority groups often have distinct views about technology. To help us develop genuinely inclusive technology, we would therefore like to ask you for your ethnicity.

- White
- Minority
- Prefer not to answer

Q7. Do you live in a. . .

- Rural area or village
- Small or middle-sized town
- Major city [country-specific population number based on size of ~top 5 cities]

Q8. I enjoy trying out new technologies

> *Strongly Disagree . . . Strongly Agree.*
>
> *1 2 3 4 5*

Q9. People have different views on privacy. In general, how concerned are you about your privacy when you access services on the internet?

> *Very Concerned . . . Not Concerned at All*

1 2 3 4 5

Section 2: IMPULSE

We are developing a new Log-In system for online services. We would like to get your feedback on it. Please watch the video, which shows the basic elements of our system.

Video here

Qu. 10. Would you use IMPULSE instead of the digital identity (log-in) systems you currently use (like username/password, smartcard, PIN, etc.), if IMPULSE were available?

Certainly not . . . Certainly yes

1 2 3 4 5

Qu. 11. *Only for "NOs" (1, 2) at Qu. 9*. **Why would you not use IMPULSE instead of the digital identity (log-in) systems you currently use? Tick all that apply**

- I do not want to depend on my Smartphone
- I do not have a Smartphone
- I am worried about what happens if I lose my Smartphone or it is stolen
- I am worried about facial recognition technology
- IMPULSE is too complicated
- I use too few online services to make IMPULSE worthwhile
- I am worried about hackers and identity theft

Qu. 12. For which online services do you think it would be most sensible to use IMPULSE? Please select no more than five

- Online banking
- eHealth (e.g. electronic communication with a doctor to get a prescription instead of going in person)
- Digital vaccination certificate for Covid or other diseases
- Social media
- E-commerce (e.g. Amazon, Airbnb)
- Completing tax returns online
- Registering for social services online
- Email
- Other (free text box)
- None

Qu 13. Please choose all of the following words and phrases that you feel describe IMPULSE.

Convenient ; Easy to use ; Saves time ; Makes signing up for services easier ; Makes logging in easier ; Exciting ; Safe ; privacy-friendly ; interesting ; Unnecessary ; weird ; Complicated ; Creepy ; IMPULSE gives me control over my data ; Dangerous ; Surveillance ; Not useful ; With IMPULSE, I can decide who gets my data ; Other *(free text box)*

Qu 14. Today, many people have multiple digital identities (log-ins), with different usernames/passwords. People have different views and experiences of this. Please tell us which statements you agree with

Strongly Disagree . . . Strongly Agree

1 2 3 4 5

- Using multiple digital identities is a hassle, but sensible

- I would prefer to have a single digital ID for all online services and accounts
- I sometimes forget my username/password, or forget which identity to use for a service or account
- I sometimes don't use a service because the sign-up process (when you enter information like your name and address and create a username/password or similar) is too much hassle
- Managing multiple digital identities and ways of identifying myself overtaxes me
- If signing up for services were easier and faster, I would use more services
- If I had only one single, secure digital ID, that I could use for all online services, I would use more services

Qu. 15. With IMPULSE, you create a new digital identity for each online service, and store these identities on your phone, in the IMPULSE App. As we saw in the video, you create these digital identities with photos of your state identity card, but then the photos are deleted. No record of your identity card is kept.

Some European governments have proposed an alternative system: a digital version of your state identity card, that you store on your phone and can use as a single, universal digital identity for all online services – instead of having multiple digital identities like with IMPULSE.

Which system would you prefer to use? *Choose One*

- IMPULSE: multiple digital identities stored on your phone but no record of your ID card kept on your phone
- Alternative: digital version of your identity card stored on your phone that serves as a single, universal digital identity

Qu. 16. For many people, it is very important to have "control over their data". Having "control over your data" has many dimensions. Below is a list of some dimensions. *Please choose the three most important in your view.*

- Online service providers have to ask for my consent before collecting or using my data
- Online service providers must provide a short, easy-to-understand privacy policy explaining how they use my data
- Online service providers cannot demand more data from me than necessary to make the service work
- Online service providers cannot refuse me their service unless I allow them to use my data for advertising
- Online service providers cannot use website lay-out and other tricks that manipulate me to give them extra data or data-use permissions
- Online service providers must delete my data if I ask them to

Section 3: Experience with eID and & Digital Experience

Qu 17. Some people are very skilled with computers and smartphones; others are just getting to know them. Please tell us about your skills

Strongly Disagree . . . Strongly Agree

1 2 3 4 5

I know how to. . .

- . . . use Google or other internet search engines
- . . . find relevant information on websites of state agencies or the municipal government
- . . . use email or social media
- . . . save or store files (documents, music etc.) on my device and retrieve them when I want them
- . . . use Cloud Applications like Dropbox, iCloud, Google Drive, or SharePoint to store and share documents
- . . . use online services like online banking, e-government or e-health
- . . . use Word or Powerpoint or similar applications
- . . . read a simple computer code and make basic changes to it
- . . . re-install or update computer programs

Qu. 18. There are many different technologies to give users a digital identity to log in to an online service, computer or smartphone, like username and password, PIN/TAN, Smartcard etc. Please tell us which ones you have used or heard about

	I have used this technology	I have heard about this technology	I have not heard about this technology
User Name + Password			
SmartCard + PIN-Number			
NemID / MitID (Denmark only)			
PIN / TAN			
Fingerprint recognition			
Face recognition			
Voice recognition			
Eye [iris] recognition			
Other [please specify]			

Qu. 19. From the list below, please choose the 3 digital identity (log-in) technologies that you prefer to use for your log-ins. Don't worry if you have not used some of the technologies yet.

- User Name + Password
- SmartCard + PIN-Number
- PIN / TAN
- Fingerprint recognition
- Face recognition
- Voice recognition
- Eye [iris] recognition
- NemID / MitID *(Denmark only)*
- Other [please specify]

Qu. 20. Many online services require you to use a digital identity (log-in), like a username/password, PIN/TAN, Smartcard/PIN or biometric recognition

> **Please estimate how many *private-sector* online services you regularly use that require a digital identity (log in), like online banking, social media, insurance, Amazon/online shopping, Airbnb, Booking.com, . . .**

Don't worry if you are not 100% sure, just give us your best guess.

Freetext box

> **Please estimate how many public-sector online services you use that require a digital identity (log in), like completing tax returns online, Covid App, registering a car or your residency, participating on a public discussion forum, registering online for a government service, . . .**
>
> **Don't worry if you are not 100% sure, just give us your best guess.**

Freetext box

Section 4: Experience with eGovernment

eGovernment means digitising public services, so citizens can do them online: for example complete tax returns, pay municipal bills, register a car or residence, or apply for social benefits.

Q. 21. Have you used eGovernment services (online public services)?

- Yes
- No

Q.22a. *For "Nos".* Please tell us about why you have not used eGovernment services, and your views about eGovernment in general.

Tick all that apply

- I am not aware of any eGovernment services
- The eGovernment services that exist are not relevant to me
- Going to the public administration in person is faster than using eGoverment
- Doing things in person at the public administration is easier than using eGoverment
- eGovernment feels cold and nonpersonal. I prefer having personal interaction with the civil servants
- I am worried about the security of my data if I use eGovernment
- I would be worried to make a mistake if I use eGovernment
- I would use eGovernment if it was fast, simple and I could be sure my data are safe
- Other Free Textbox

Qu.22b. *Only for "Yes" at Qu.21.* Thinking about your experience with eGovernment, what aspects should be improved the most? Please choose the three most important

- Make signing up for eGovernment (creating a digital identity to use for eGovernment) easier and faster

- Make logging-in to eGovernment services easier and faster
- Make more public services available online
- Make finding information about eGovernment services easier
- Improve the layout of eGovernment websites
- Offer more assistance for using eGovernment (e.g. helplines, chatbots)
- Ensure all eGovernment services can be completed fully online (i.e. no need for any offline steps, like providing physical signatures

End

Many thanks for your time and support!

8.2 Appendix B: Supplementary Figures

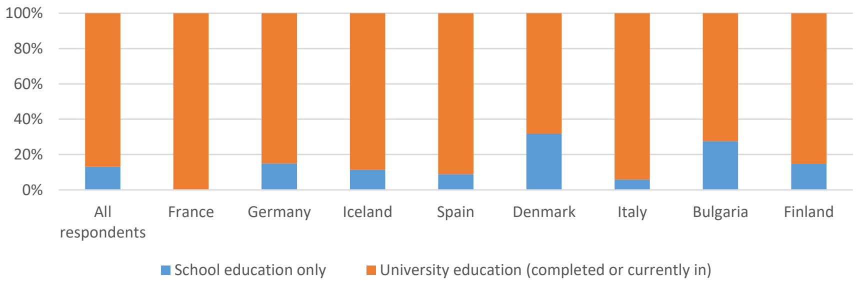


Figure 5. Educational distribution of the survey population by country

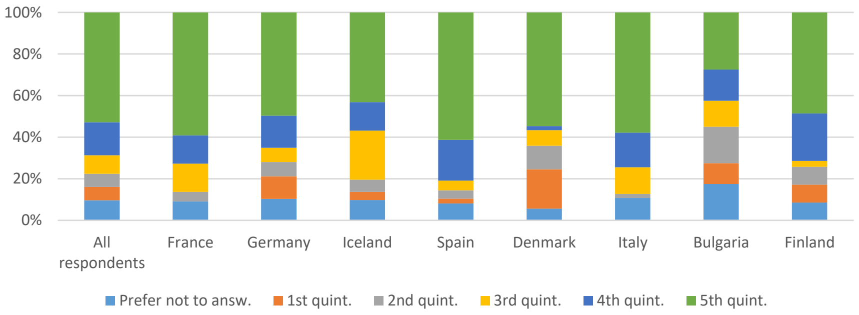


Figure 6. Income distribution of the survey population by country and income quintile

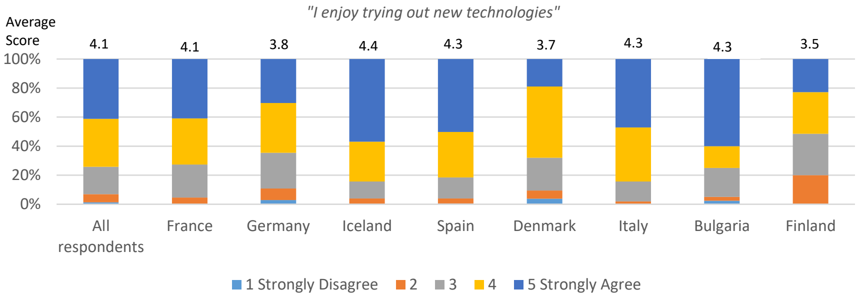


Figure 7. Technology affinity scores across countries

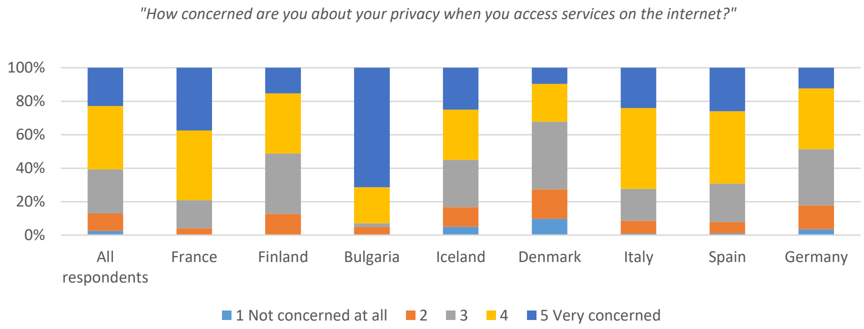


Figure 8. Privacy concern scores across countries

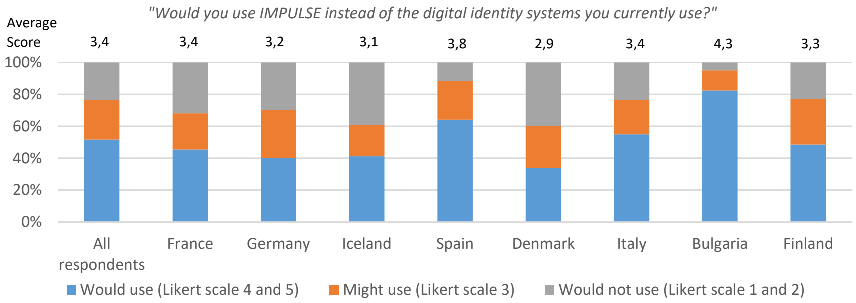


Figure 9. Intention to use IMPULSE across the survey population, by country

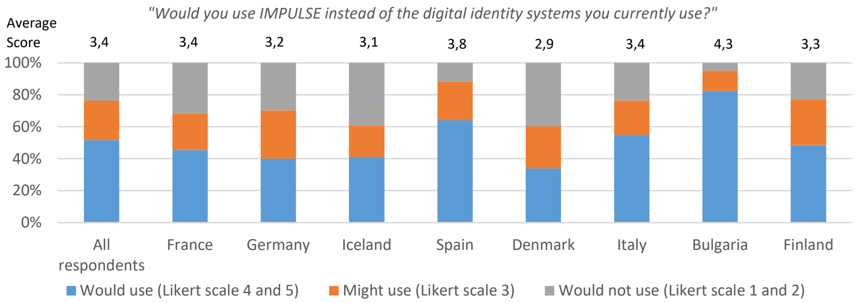


Figure 10. Use cases identified as appropriate for IMPULSE

Biographies

Nicholas Martin. Nicholas Martin is a research scientist at Fraunhofer ISI in Karlsruhe, Germany. His research focuses mainly on industrial and innovation policy, the economic effects of data protection regulation, and the adoption of new technologies. Prior to joining Fraunhofer, he was a management consultant at OC&C Strategy Consultants, and holds a PhD in political science from MIT.
ORCID: https://orcid.org/0000-0002-8739-0165
CRediT Statement: Conceptualisation, Methodology, Investigation, Writing – original draft, Revision.

Frederik M. Metzger. Frederik Metzger is a research scientist at Fraunhofer ISI in Karlsruhe, Germany. His main research focuses on how technology impacts human agency and how value is created through digital data. Prior to joining Fraunhofer ISI, he held positions in technology transfer, startup consulting and agile software management. He holds a doctorate in Business and Management from the University of Mannheim, Germany.
ORCID: https://orcid.org/0000-0002-3082-7047
CRediT Statement: Methodology, Investigation, Formal analysis, Writing – original draft, Revision.