The Closing Educational Gap in E-privacy Management in European Perspective

Maineri, Angelica M.; Achterberg, Peter; Luijkx, Ruud

Veröffentlichungsversion / Published Version
Zeitschriftenartikel / journal article

Empfohlene Zitierung / Suggested Citation:
Maineri, A. M., Achterberg, P., & Luijkx, R. (2021). The Closing Educational Gap in E-privacy Management in European Perspective. *Sociological Research Online*, *28*(1), 37-57. https://doi.org/10.1177/13607804211023524

Article

SRO

Sociological Research Online
2023, Vol. 28(1) 37–57

Article reuse guidelines:
sagepub.com/journals-permissions
DOI: 10.1177/13607804211023524
journals.sagepub.com/home/sro

The Closing Educational Gap in E-privacy Management in European Perspective

Angelica M Maineri
Tilburg University, The Netherlands

Peter Achterberg
Tilburg University, The Netherlands

Ruud Luijkx
Tilburg University, The Netherlands; University of Trento, Italy

Abstract

Educational gaps are increasingly salient as skills and knowledge gain prominence in digital societies. E-privacy management, namely, the ability to control the flow of information about the self, is an important asset nowadays, since a skillful use of digital technologies enables full participation in social life and limits the exposure to unwarranted algorithmic processes. We investigate whether and why education affects e-privacy management, and whether the educational gaps vary following a country's degree of digitalization. We empirically test two sets of mechanisms, one derived from the digital divide and diffusion of innovations theories and the other from the reflexive modernization theory. The study employs Eurobarometer 87.1 data ($N = 21{,}177$), collected in 2017 among representative samples from 28 European countries, and uses multilevel linear regression model. Findings suggest that the years spent in education positively affect e-privacy management, and that this effect is largely mediated by digital skills and Internet use, and to a lesser extent by a reflexive mind-set. The educational gap in e-privacy management narrows in more digitalized countries.

Keywords

diffusion of innovations, digital divide, e-privacy, educational gaps, reflexivity

Corresponding author:
Angelica M Maineri, Department of Sociology, Tilburg University, Warandelaan 2, 5037 AB Tilburg, The Netherlands.
Email: a.m.maineri@tilburguniversity.edu

Introduction

Due to the centrality of knowledge and information in contemporary societies, education has become a powerful indicator of social position (Bovens and Wille, 2017). Economic theories, for example, the skill-biased technological change, explained how technological change aggravates inequalities by taking over tasks from the unskilled workers and favoring workers with higher skills (Acemoglu, 2002). At the individual level, the complexity of the technologies that increasingly mediate daily lives is more easily handled by more educated people (Cruz-Jesus et al., 2016). The educational inequalities arising in the digital, information-intense environment hence become important factors in the reproduction of social inequalities in contemporary societies. In this study, we analyze a potential expression of educational inequalities in digital societies, namely, the educational gap in e-privacy management and its configuration in European countries.

Privacy describes the boundaries between the self and society (Anthony et al., 2017; Marx, 2016), and plays an important role for social order by involving monitoring and social control (Anthony et al., 2017). Broadly intended, privacy means 'the access of one actor (individual, group, or organization) to another' (Anthony et al., 2017: 251). Privacy decisions depend upon the context (Nissenbaum, 2010; Park and Shin, 2020), for example, who is going to have access and for what purposes, and privacy norms define what is appropriate in terms of access in different situations (Anthony et al., 2017). One's ability to control access to the self as well as the capability to access others is defined as privacy management (Anthony et al., 2017). For individual citizens, (information) e-privacy management concerns the control of the flow of information about the self that is released online (Blank et al., 2014; Cho and LaRose, 1999; Kokolakis, 2017; Park, 2015): it is not about releasing information *per se*, but about knowing what information is released, to whom, and for which purposes. E-privacy is not uniquely rooted in the digital sphere, since the large amount of personal information exchanged online as well as the far-reaching consequences of a breach of privacy online make it a key aspect of general privacy protection nowadays.

While previous studies often focused on disclosure behaviors and/or management of privacy settings on social networking sites (SNSs; for example, Bartsch and Dienlin, 2016; boyd and Hargittai, 2010; Debatin et al., 2009; Litt, 2013b; Litt and Hargittai, 2014; Park, 2018), in this study, inspired by the approach of Büchi et al. (2017), we focus on e-privacy management within general Internet use.

One's e-privacy management is increasingly challenged in the digital society as individual characteristics and preferences are monitored and reproduced via computational processes. First of all, in their daily online interactions, Internet users need to release information about the self in exchange for services (Acquisti et al., 2015; Kokolakis, 2017; van Dijck, 2014). This exchange makes data released online a valuable asset, which users rarely acknowledge. For example, social media platforms, such as Facebook, do not directly charge a fee to users, yet generate revenues by selling targeted advertisement space based on the elaboration of users' data. Second, digital technologies enable information collection at little cost and without the monitored subjects necessarily being aware of it. Finally, as more and more information on the self is shared online and easily harvested, there are growing risks of abuse. On one hand, cybercrime is widespread, but, since it often does not have immediate repercussions on victims (e.g. identity theft), it goes unnoticed

and underreported. On the other hand, concerns over discrimination and social sorting (Acquisti et al., 2015; Anthony et al., 2017; Lyon, 2005; Mann and Matzner, 2019) are growing as decision-making processes are increasingly delegated to algorithms.

E-privacy management is a critical resource in contemporary digital societies (Büchi et al., 2017), and as such it is likely to be unevenly distributed, with the risk of leaving some social groups vulnerable to the negative consequences of digitalization (Lupton, 2016). While this is generally attributed to resource constraints (Anthony et al., 2017) or socialization processes (Park, 2018), the mechanisms explaining such unequal distribution are not clear. We draw on literature on the digital divide and diffusion of innovation, and on reflexive modernization, to explain the educational gap in e-privacy management. Whereas the former theory refers to Internet use and digital skills as unevenly distributed resources that could explain differences in e-privacy management, the latter pinpoints the role of knowledge and risks awareness in an increasingly information-intense environment.

Critical resources for a fruitful use of digital technologies tend to be associated with education (Cruz-Jesus et al., 2016). Previous findings on the relationship between education and e-privacy management are mixed. Whereas some studies did not find any significant educational differences in e-privacy control (Cho et al., 2009; Litt, 2013b; Park, 2011, 2013), Park and Chung (2017) highlighted how education positively affects awareness of, interest in, and control of privacy online. We therefore attempt at clarifying this discrepancy, and ask *whether and why higher educated individuals are better equipped in managing their privacy online than the lower educated*. By answering this question, we shed light on new potential stratification mechanisms taking place in the digital society.

Second, we look at the comparison across European countries, which are at different stages of the digitalization process, to evaluate whether the digital (infra)structure in a country leads to a widening or narrowing of the educational gap in e-privacy. We ask *whether the degree of digitalization affects the educational gaps in e-privacy management*. Comparing countries with different degrees of digitalization may help forecasting trends over time, as digitalization processes expand globally.

By engaging with the study of educational gaps in the management of privacy online in comparative perspective, we aim at enriching the insights on e-privacy and on educational inequalities in the digital society. We examine and empirically test two mechanisms that could underlie social inequalities in the management of e-privacy. Although the two perspectives share expectations concerning the educational gap in e-privacy management, they suggest different mechanisms, as well as different trajectories of educational gaps according to the degree of digitalization of the country. Analyzing inequalities in e-privacy management also aims at informing policy makers, as the European Commission's Digital Single Market initiative aims at ensuring that European citizens can fully profit from the opportunities offered by digitalization.

The educational gap in e-privacy management

Diffusion of innovation and digital divide

At the individual level, the existence of digital divides, that is, the inequalities in the access to, use of and gains from the Internet has been largely acknowledged (Hargittai,

2002; Lutz, 2019; Robinson et al., 2015; Scheerder et al., 2017; van Deursen and Helsper, 2015; van Dijk, 2005, 2013). Offline resources determine the extent to which one has access – broadly intended – to digital technologies. It is a cumulative model: when the access gap ('first-level digital divide') is overcome, a skill and use divide emerges ('second-level digital divide'); as the skill divide closes, a gap in the benefits obtained by Internet use arises ('third-level digital divide'). Sources of online divides align with traditional, 'offline' sources of inequalities: educational level, occupational prestige, gender, age, and so on (for extensive reviews of different levels of the digital divide, see Lutz, 2019; Scheerder et al., 2017).

E-privacy management is a critical skill in the digital era (Büchi et al., 2017; Park and Chung, 2017). Privacy is related to power relationship and hence unequally distributed within societies; privacy management additionally requires skills and resources to be enacted (Anthony et al., 2017; Büchi et al., 2017). A Swiss study found that privacy protection is mostly explained by Internet skills, and, to a lesser extent, by privacy concerns, and that a more intense Internet use indirectly affects privacy protection by increasing exposure to privacy breach (Büchi et al., 2017). Park (2011, 2013) found a positive effect of knowledge and familiarity with the Internet on privacy control among US citizens, while Bartsch and Dienlin (2016) found a positive association between time spent online and e-privacy literacy in Germany. In other words, e-privacy management tends to be prevalent among groups that are on average more skilled and familiar with digital technologies, along the lines of the digital divide argument. Hence, we expect that *higher educated individuals manage their privacy online more than the lower educated due to their higher frequency of Internet use* (Hypothesis 1a) *and their stronger digital skills* (Hypothesis 1b).

Digital divides follow the model sketched by Rogers (2003) in his theory on the diffusion of innovations. Accordingly, an innovation (e.g. a new technology) is progressively adopted by five groups of people, ranging from the first to adopt the innovation to the last ones: innovators, early adopters, early majority, late majority, and laggards. These groups display systematic differences (Neuman et al., 2011), and early adopters tend to be more educated and be in higher social strata compared with late adopters (Rogers, 2003), therefore generating inequalities, such as the digital divide. However, as the innovation is adopted over time by an increasingly larger portion of the population, socio-economic factors become weaker predictors of an innovation's adoption. This theory would explain why digital divides – as the educational gap in e-privacy management – should be smaller in countries that have a higher degree of digitalization: in countries where a large portion of the population is interested by technological developments, individuals lower educated are likely to catch up with a skillful use of technologies. We hence expect that *the positive effect of education on e-privacy management is weaker in more digitally advanced societies* (Hypothesis 2).

Digital risks and reflexive modernization

According to Beck (1992), as technology advances, the more hazards and insecurities come with it. Hence, inextricably linked to modernization is risk – a 'systematic way of dealing with hazards and insecurities induced and introduced by modernization itself'

(Beck, 1992: 21). Along these lines, the emergence of digital technologies, while offering many potential benefits and possibilities, produces new harms that can quickly escalate due to the pervasiveness in people's daily lives (Lupton, 2016). Unlike traditional risks (e.g. natural catastrophes), people tend not to be physically damaged by digital risks (Beck, 2013), which makes their timely acknowledgment even more critical.

In modern societies, risk is a relevant element in stratification processes (Beck, 1992), for many reasons. First, risks affect some groups in society more than others, and this may run along 'traditional' social-class lines. Moreover, risks depend upon knowledge about them, and knowledge is not equally distributed within societies, hence it follows that those who are aware of risk are those who are more educated and/or informed (Beck, 1992).

To understand how people cope with and analyze risk we use the theory of reflexive modernization (Beck, 1992). This theory describes how modern societies started to question their own modern advances and technological solutions. The central claim is that in modern countries there is a strong emphasis on the idea that the typical risks in these societies are 'manufactured' or produced by modern technological innovations. Pointing to newly emerging, and largely unforeseen risks, in reflexively modern societies, people perceive these modern solutions as sources of newly emerging problems. Reflexively modern individuals soon start to analyze all risks they face, including those potentially produced by technological innovations. In these reflexively modern societies, it is implausible that technology is embraced without reservation (Lupton, 1997). While societies increasingly rely on scientific and technological advances, science and technology become also increasingly targets of reflexive criticism (Nettleton and Burrows, 2003; Price and Peterson, 2016).

Theorizing on reflexive modernization emphasizes two aspects. First, the advancement of information and knowledge is one of its central features (cf. Makarovs and Achterberg, 2017; Price and Peterson, 2016). Because of the widely accessible information and knowledge, people can analyze the unintended and latent consequences of technological interventions. Second, some individuals in these societies are better able to analyze the risks brought by technological innovations (Achterberg et al., 2017; Makarovs and Achterberg, 2017). Accordingly, it can be expected that, because of their reflexive mind-set, and their cognitive abilities, the higher educated are more concerned about the introduction of newly emerging technologies and are more inclined to actively protect their e-privacy. We hence expect that *the higher educated manage their privacy online more than the lower educated because of their reflexive mind-set* (Hypothesis 3).

As the technological advancements progress alongside hazards, risk becomes increasingly salient as a stratification mechanism, and modern information and communication technologies (ICTs) constitute the very infrastructure for the reflexive attitude to flourish (Nettleton and Burrows, 2003). Consequently, the reflexive attitude becomes a stronger driver of inequalities in online privacy management in countries that are at a later stage of digitalization. We hence expect that *the positive effect of education on e-privacy management is stronger in more digitally advanced societies* (Hypothesis 4).

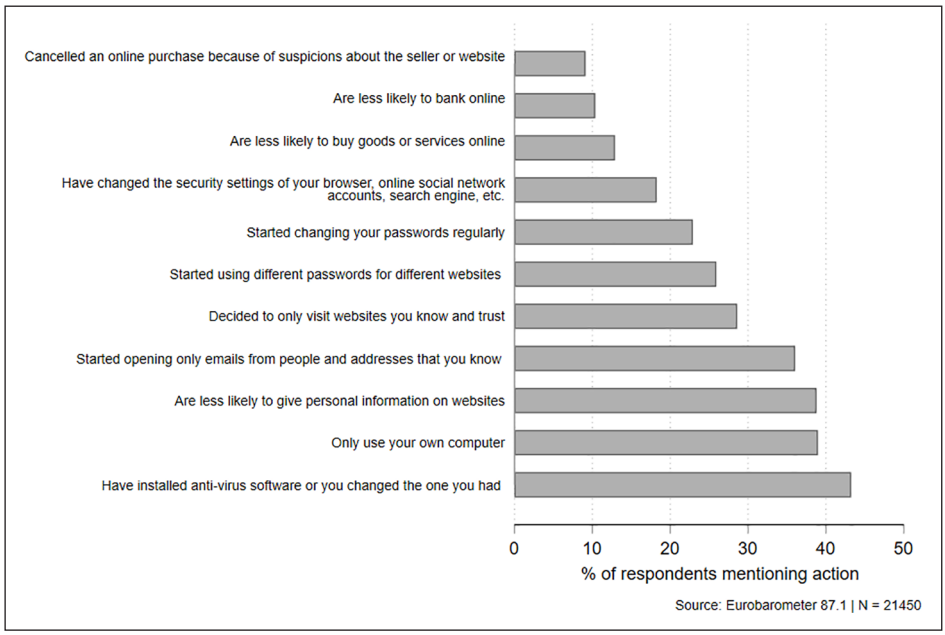

Figure 1. Percentage of mentions for each e-privacy management action.

Data and methods

To address the research questions and test the hypotheses, we used data from the Eurobarometer 87.1 (European Commission and European Parliament, 2017) which investigated e-privacy and cybersecurity issues. The questionnaire was fielded in 28 European Union Member states in 2017 via face-to-face computer-assisted personal interviews (CAPI) to representative samples of the population above 15 years old.

Respondents not using the Internet were not asked questions about e-privacy, hence our study is restricted to Internet users only. In the Supplementary materials, we address the individual characteristics of those not using the Internet and provide a brief description of how prevalent they are in each country.

Individual-level variables

To measure *e-privacy management*, respondents indicated whether in the last three years, because of security and privacy issues,[1] they performed a series of actions, listed in Figure 1. Only one out of ten respondents had ever canceled an online purchase, and more than two out of five respondents mentioned they installed or changed anti-virus software.

To create a single measure of e-privacy management, we performed a principal components factor analysis on the matrix of tetrachoric correlations among the dichotomous items. We adopted an exploratory approach, since – to our knowledge – the quality of

Table 1. Factor loadings and uniqueness of principal components factor analysis ($N = 21{,}450$).

Variable	Factor	Uniqueness
Less personal information	0.67	0.55
Security settings	0.70	0.51
Only trusted websites	0.52	0.73
Different passwords	0.75	0.44
Reject unknown emails	0.69	0.51
Anti-virus software	0.71	0.49
Cancel online purchase	0.55	0.69
Regularly change passwords	0.60	0.63
Explained variance	43%	

this measurement instrument has not been previously assessed. We excluded the three items ('Less online purchases', 'Less online banking', and 'Only use own computer') that performed poorly[2] with the others. This choice is also justified by a critical assessment of the content, as these three items refer to general actions, in contrast with the remaining items that explicitly mention privacy-related actions, for example, changing passwords or disclosing personal information. Eight items with factor loadings > 0.5 on the first factor (which explains 43% of the variance) were retained (see Table 1). The eight items formed a sufficiently reliable index (Kuder–Richardson's formula $20 = 0.66$). Although the items mostly refer to a specific computer-related use of the Internet which, with the spread of mobile devices, is not completely up-to-date, this measure is comparable with one of the dimensions of e-privacy behaviors Cho et al. (2009) found, and labeled as proactive protecting behaviors. An unweighted sum score was computed on the eight items, and correlated strongly (rho = 0.99) with the factor score. See Table 2 for the descriptive statistics of this variable.

Education is based on the age at which full-time education was completed.[3] For those who are still studying, the age at finishing education was imputed as the current age.[4] We subtracted the age at which school starts in each country (cf. Sharp, 2002), which resulted in a measure of years spent in full-time education. Respondents marked up to 79 years spent in full-time education, which is an extremely high value probably due to a misinterpretation of the question. The value corresponding to the 95th percentile, 22 years, is a good approximation for someone who has reached a PhD degree. Hence, we truncated the distribution and assigned the value of 22 years spent in education to all values above the 95th percentile. In this way, the range of years spent in education was more plausible, and fewer respondents were excluded from the analyses. Figure 2 displays the distribution of the years spent in education across countries and shows that, on average, respondents from Northern European countries tend to spend more time in education than respondents in Southern countries, aligning with the statistics on tertiary education attainment in Europe (Eurostat, 2020).

As for *Internet use*, an index measuring the frequency of performing several activities of the Internet (e.g. use Internet at home, at work, using social media, etc.) was available in the dataset. After excluding those never using the Internet, the index consists of five

Table 2. Descriptive statistics of individual characteristics ($N = 21,177$).

Variable	Mean	Std. dev.	Min.	Max.
E-privacy management	2.25	1.91	0	8
Years spent in full-time education	14.09	3.92	0	22
Digital skills	3.13	0.77	1	4
Internet use	3.77	0.70	0	4
Variable	**Proportion**		**Min.**	**Max.**
Climate change own responsibility	0.27		0	1
Unemployed	0.07		0	1
Student	0.08		0	1
Female	0.54		0	1
Age			0	1
15–24	0.11			
25–34	0.17		0	1
35–44	0.19		0	1
45–54	0.19		0	1
55–64	0.17		0	1
65–74	0.13		0	1
75 +	0.04		0	1
Settlement type				
Rural area or village	0.31		0	1
Small- or middle-sized town	0.40		0	1
Large town	0.29		0	1

categories, ranging from '(Almost) everyday' to 'Less often (than two/three times a month)'. Values were recoded so that high values indicate more Internet use. We measured self-reported *digital skills* by the question 'You consider yourself to be sufficiently skilled in the use of digital technologies . . .' for several domains: in one's daily life, to do a job, to do a future job, to use online public services and to benefit from digital learning opportunities. Answers ranged on a 4-point scale from 'totally agree' to 'totally disagree'. The items form a reliable scale (Cronbach's alpha = 0.90), and a principal components factor analysis revealed one factor capturing 73% of the variance. Some of the items were only administered to selected respondents (e.g. 'skills in one's job' are only measured among those who are currently employed), hence average scores on the items were computed taking into account only the items administered to each respondent.

We used a dichotomous item measuring the belief that it is the respondent's personal responsibility to tackle climate change as an indicator of a *reflexive mind-set*. The question taps on the acknowledgment of the man-made nature of contemporary risks. Even though the focus on climate change only is suboptimal, data limitations did not allow for

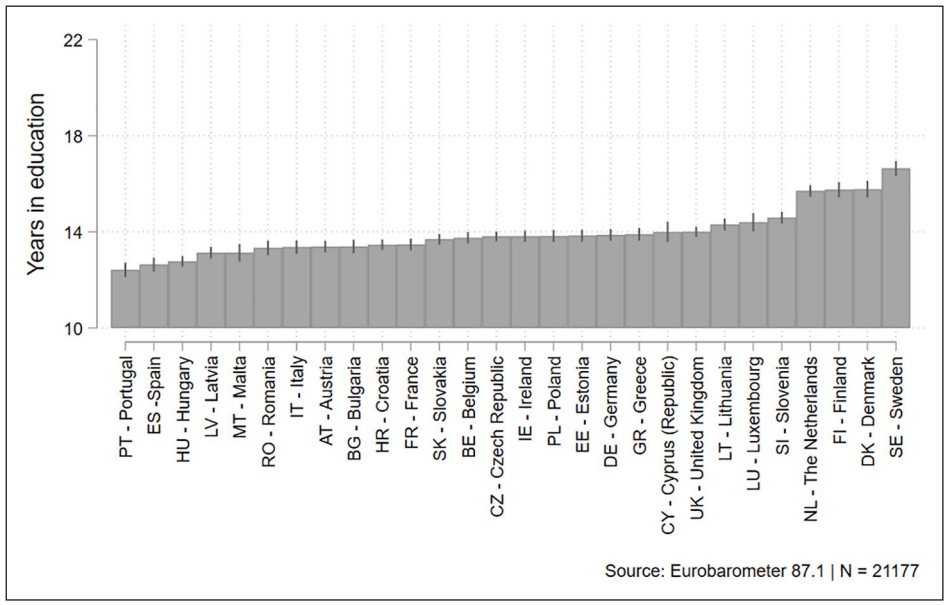

Figure 2. Mean of years spent in education by country (error bars represent 95% confidence intervals).

a more refined measurement. An alternative measure for this concept is shown in the Supplementary Materials, and yielded similar results.

In the analyses, we controlled for socio-demographic characteristics that are usually associated with e-privacy management, such as gender, age, unemployment status, being a student and the settlement type. Age is particularly relevant because previous studies found that e-privacy management is more common among young people (Blank et al., 2014; Litt, 2013b). Findings on gender are mixed: whereas Park (2011, 2015) found that men are more protective, Litt (2013b) found that women tend to enact more diverse privacy management behaviors on SNSs. Finally, e-privacy management is also common practice among university students, despite a general feeling of inevitability of data breach (Hargittai and Marwick, 2016). See Table 2 for the descriptive statistics of all variables used in the models.

In the analyses, all continuous independent variables have been centered around the grand-mean (cf. Hox, 2002: 54–58). We deleted the missing values listwise, leaving 21,177 observations, nested in 28 EU countries. Countries' sample sizes range from 310 respondents in Malta to 1187 in Germany.

Country-level variables

For the *degree of digitalization* we used the digital economy and society index (DESI). The DESI is developed within the context of the Digital Single Market initiative of the European Commission. This index considers the countries' digital performance in five

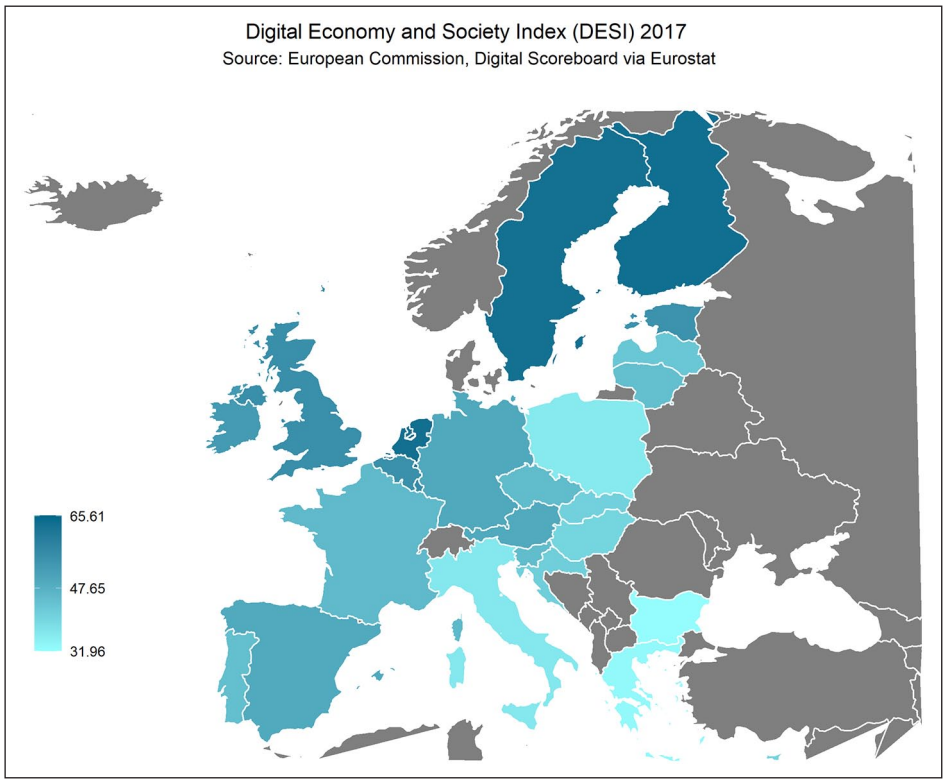

Figure 3. Distribution of DESI across EU countries.

different areas: connectivity, digital skills, Internet use, integration of digital technologies, and digital public services.[5] Consequently, the DESI does not only reflect the prevalence of Internet use among the population, but also it captures the permeation of the digital services among private enterprises and public institutions. Higher scores stand for more digitalization of a country. We retrieved results from 2017 to match the data collection period of the Eurobarometer. The DESI ranges from 31.9 (Romania) to 65.6 (Denmark) and is shown in Figure 3. *Per capita GDP* in Purchasing Power Standards for 2017, retrieved from Eurostat (reference: PRC PPP IND), is used as a country-level control variable. This metric, expresses a countries' per capita GDP in relation to the EU average GDP per capita (=100). The variable ranges from 49 (Bulgaria) to 253 (Luxembourg), with a mean of 99.9 and a standard deviation of 41.2. For the purposes of the analyses, the DESI and GDP have been centered around the mean.

Analytical strategy

To test the hypotheses, we estimated multilevel linear regression models, with 21,177 respondents nested in the 28 EU countries. First, we fitted an empty model allowing an estimation of the amount of variance at the country level. Second, we estimated the fixed

Table 3. Multilevel linear regression analyses of e-privacy management on individual characteristics (N = 21,177).

Variables	M0	M1	M2	M3	M4	M5
Fixed effects	*b*	*b*	*b*	*b*	*b*	*b*
Years in education[a]		0.07***	0.06***	0.04***	0.06***	0.04***
Female		–0.12***	–0.12***	–0.07**	–0.14***	–0.09***
Age categories						
15–24		0.14*	0.08	0.05	0.14*	0.02
25–34		0.01	–0.02	–0.05	0.01	–0.07+
35–44 (Ref.)						
45–54		–0.04	–0.001	0.03	–0.04	0.05
55–64		–0.15***	–0.06	–0.001	–0.14**	0.05
65–74		–0.24***	–0.14*	–0.04	–0.22***	0.02
75 +		–0.64***	–0.46***	–0.29***	–0.61***	–0.19*
Student (full time)		0.15*	0.15*	0.09	0.15*	0.10
Unemployed		–0.09+	–0.02	–0.04	–0.09+	0.001
Rural area or village (Ref.)						
Small/middle town		–0.05+	–0.06+	–0.05+	–0.05	–0.06*
Large town		0.04	0.01	–0.00	0.04	–0.01
Internet use[a]			0.44***			0.31***
Digital skills[a]				0.60***		0.52***
Climate change: own responsibility					0.33***	0.29***
Constant	2.19***	2.34***	2.30***	2.27***	2.25***	2.18***
Random effects						
var(Country)	0.37***	0.37***	0.32***	0.29***	0.33***	0.24***
Pseudo $R^2_{country}$		1.1%	12.9%	22.1%	11.8%	34.5%
var(Individual)	3.23***	3.12***	3.04***	2.95***	3.10***	2.89***
Pseudo $R^2_{individual}$		3.4%	6.1%	8.8%	4.0%	10.4%
Model fit						
Conditional likelihood ratio (LR chi^2) test		740.7***	591.3***	1214.1***[b]	134.3***[b]	1608.6***[b]
Δ *df*		12	1	1	1	3
–2 log likelihood	85,067.5	84,326.8	83,735.4	83,112.7	84,192.5	82,718.2

[a]Centered variable.
[b]Nested in M1.
+ $p < 0.10$; * $p < 0.05$; ** $p < 0.01$; *** $p < 0.001$.

effects at the individual level models including a random intercept at the country level. By adding independent and mediating variables stepwise, these models test Hypotheses 1 and 3. The hypotheses involving the contextual level (Hypotheses 2 and 4) are tested by adding contextual information in the fixed effects part, by allowing a random slope for education to vary across countries, and adding a covariance term between the random slope and the random intercept. In these last models, individual-level control variables are included, but only the direct effect of education (without mediation) is estimated.

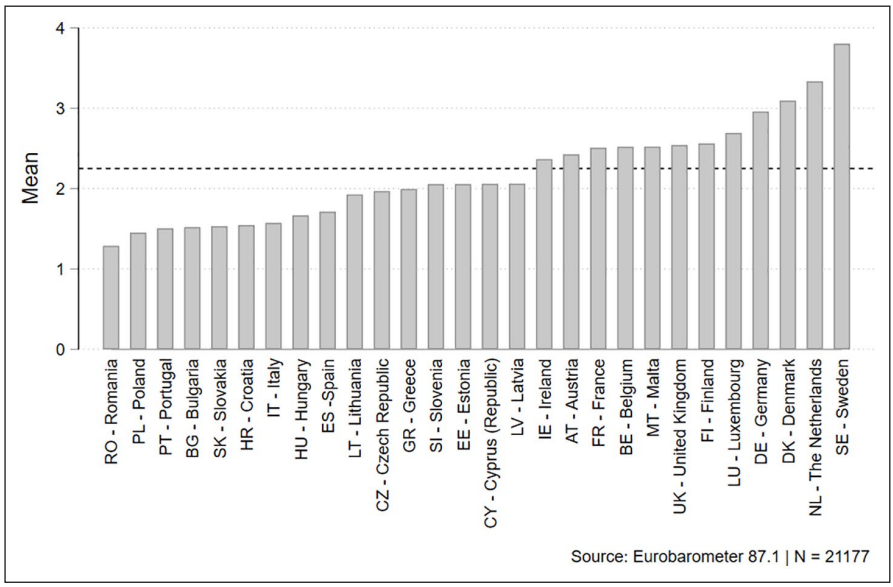

Figure 4. Average number of e-privacy management activities by country. The dotted line represents the grand-mean across countries.

Models are evaluated by means of variations in the explained variance (compared with the variance in the empty model), –2 log likelihood and by the likelihood ratio test (which compares nested models, usually the previous model unless differently specified).

All the analyses are performed with StataMP 16 (StataCorp, 2019) using the package *polychoric* (Kolenikov and Angeles, 2004); the map in Figure 3 was produced with R (R Core Team, 2013) using the packages *ggplot2* (Wickham, 2016), *mapproj* (McIlroy et al., 2018), and *rworldmap* (South, 2011).

Results

The empty model (M0 in Table 3) suggests that the country level accounts for 10% of the total variance of e-privacy management (intraclass correlation coefficient = 0.102). Figure 4 shows the distribution of the average number of e-privacy management activities for each country.

The first part of the analyses is reported in Table 3. Education appears to have a small yet significant and positive effect on managing privacy, as hypothesized, and although the coefficient decreases in size when adding the mediating variables, it holds across models. Taking M1, the increment in e-privacy management activities at each additional year spent in education is small in size ($b = 0.07$, $p < 0.001$), yet the difference between the lowest (0) and highest (22) amount of years in education reaches about 1.5 activity (out of 8). The models account for variation at the country level, due to composition effects. At the individual level, education and the control variables only explain 3.4% of

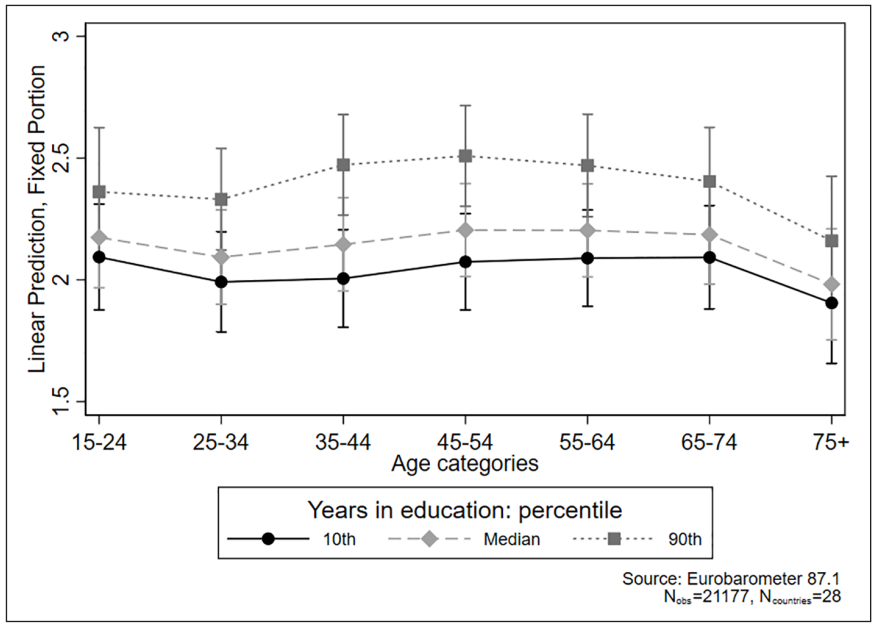

Figure 5. Predicted values of e-privacy management and 95% confidence intervals by 10th, 50th, and 90th percentiles of years spent in full-time education and age categories (controlling for all variables included in M5).

the variance; the final model (M5), which also includes the mediating variables, explains in total 10.4% of the variance at the individual level.

Hypotheses 1 and 3 are supported, since all the mediating effects play a role in the relationship between education and e-privacy management: frequency of Internet use and digital skills, and the reflexive mind-set, all display significant and positive coefficients. Digital skills account for the strongest reduction in the effect of education, and explain more variance at the individual level compared with the variance explained by Internet use. As for reflexive modernization, albeit own responsibility to tackle climate change shows a significant and positive impact on e-privacy management, it accounts for a small reduction in the direct effect of education. An alternative operationalization of reflexive mind-set yields very similar results (see Table A2 in Supplementary Materials).

The change in standard deviations of the outcome variable at each 1-standard deviation increase in the predictor is obtained by standardizing the *b*-coefficients. This allows to directly compare the strength of the coefficients of different predictors within a model. The standardized coefficients (beta) in M5 show that digital skills have a stronger impact (beta = 0.21) on e-privacy management compared with believing that it is one's own responsibility to tackle climate change (beta = 0.06) and Internet use (beta = 0.11). All coefficients, anyway, remain significant, positive, and substantial.

With respect to the control variables, women are consistently less prone to manage their privacy than men; the negative effects of age and unemployment, as well as the

Table 4. Multilevel linear regression analyses of e-privacy management on individual and country characteristics ($N = 21{,}177$).

Variable	M6	M7	M8
Fixed effects	*b*	*b*	*b*
Years in education[a]	0.07***	0.07***	0.07***
DESI[a]	0.05***	0.05***	0.05***
GDP per capita[a]		0.002	0.002
DESI × years in education			–0.001 +
Control variables omitted from output			
Constant	2.35***	2.35***	2.35***
Random effects			
var(Years in education)	0.001***	0.001***	0.001***
var(Country)	0.10***	0.10***	0.10***
Pseudo R^2	71.9%	73.0%	73.0%
Covariance years in education with country	0.05	0.05	0.04
var(Individual)	3.11***	3.110***	3.11***
Pseudo R^2	3.8%	3.8%	3.8%
Model fit			
Conditional likelihood ratio (LR chi^2) test	70.8***[b]	1.1	3.0 +
Δ *df*	3	1	1
–2 log likelihood	84,255.9	84,254.4	84,251.9

GDP: gross domestic product.
[a]Centered variable.
[b]Nested in M1.
+ $p < 0.1$; * $p < 0.05$; *** $p < 0.001$.

positive effect of being students are also explained by the digital divide, as their coefficients drop in size when adding Internet use and/or digital skills to the models. The type of settlement only has limited impact on the tendency to manage privacy.

To explore the residual direct effect of education on e-privacy management, we break it down by age groups (see Figure 5). Even net of digital skills and Internet use, it is mostly among the adult age groups (35–54 years old) that the highest educated (90th percentile) individuals tend to enact significantly more e-privacy protection activities compared with the lowest educated (10th percentile). That is, the relative gain of having pursued higher education on e-privacy-savviness is stronger for those who are in their working age. One possible explanation is that higher educated adults are more likely to work in the tertiary sector, which – compared with manual jobs – may actively require e-privacy management. There is no educational gap among the elderly, for whom digital technologies were hardly available during their formation years. For the younger cohorts, an explanation of the lack of the educational gap in e-privacy management may be due to the fact that digital training in school occurs earlier compared with previous cohorts, diminishing the relative gain of each additional year spent in education.

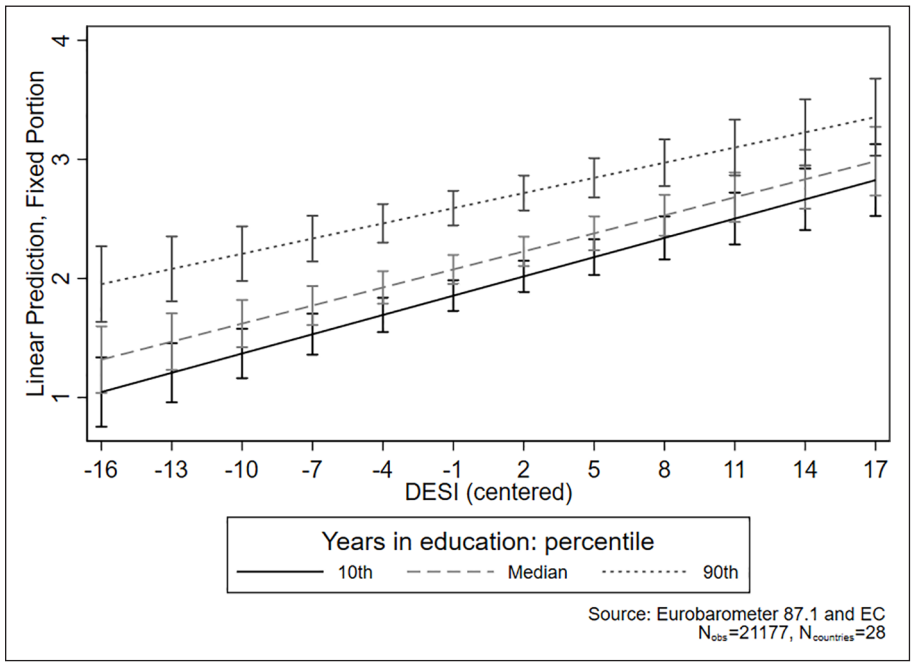

Figure 6. Predicted values of e-privacy management and 95% confidence intervals by 10th, 50th and 90th percentiles of years spent in full-time education and DESI.

Turning to the country-level models, a country's degree of digitalization has a significant positive effect on e-privacy management, indicating an overall higher tendency to manage privacy online in more digitalized countries; the effect holds also when a country's GDP per capita is added to the model. A large portion of variance (70%) at the country level is explained when adding DESI (M6 in Table 4). GDP does not contribute to improve the model, and further inspection shows high collinearity with the DESI index (rho = 0.61).

As concerns the differential effect of education across countries, the random slope for education is small in size, yet statistically significant, and the likelihood-ratio test suggests an improvement in the model (M6 compared with M1): this indicates that the effect of education varies across countries.

The coefficient for the cross-level interaction between DESI and years spent in education proves significant at the 90% level, and there is only a small improvement from previous models according to the Likelihood-ratio test. However, by plotting the marginal effects (see Figure 6), it can be seen that at lower values of DESI there is a significant difference between those in the 90th percentile of years in education and those in the 10th and median cutoffs. However, this difference disappears at higher values of DESI, suggesting that in countries that underwent stronger digitalization processes the educational gap in e-privacy narrows (supporting Hypothesis 2). These results also lead to reject the expectation that the educational gap in e-privacy would be larger in more digitally advanced countries (Hypothesis 4).

Summary of findings and discussion

Digital transformations have made privacy a key issue of our time. In this study, we departed from the idea that the level of education – one of the strongest factors of stratification nowadays (cf. Bovens and Wille, 2017) – affects the extent to which individuals protect their privacy online, potentially generating inequalities in the exposure to unwarranted algorithmic processes and cybercrime. Earlier studies yielded mixed findings, and the theoretical links underlying such relationship remained unexplained. To tackle this gap, we tested two potential mechanisms explaining the effect of educational level on e-privacy management, and studied whether this educational gradient varied across more and less digitalized countries.

Our main finding, that is, the positive and significant association between education and enacted e-privacy protecting activities, aligns with the findings of Park and Chung (2017), who found a positive association between the level of education and e-privacy control among US adults. Although the studies by Park (2011, 2013) did not detect a direct effect of education on e-privacy skills, he found an effect of technical knowledge on e-privacy skills, which is similar to our next set of findings.

Our results indicate that the digital divide theory is highly relevant when it comes to e-privacy management, since both frequency of Internet use and digital skills positively affect e-privacy management (cf. Bartsch and Dienlin, 2016; Büchi et al., 2017; Park, 2011, 2013) and mediate the effect of education. The lower educated (and also elderly and unemployed) are less equipped to deal with the challenges of advanced digitalization. Due to their lower digital skills and their lower tendency at protecting personal information online, the lower educated result more vulnerable to 'offline' consequences, such as (cyber)crime or unwarranted algorithmic profiling. In light of this finding, the emerging new research on algorithmic skills (Hargittai et al., 2020) and, more generally, on digital inequalities in the algorithmic era (Lutz, 2019), constitute a promising venue for future research.

Theorizing on reflexive modernization only proves partially useful to explain the educational gap in e-privacy management. At the individual level, even though the reflexive mind-set positively affects e-privacy management, the evidence of the mediation is weak, and the predictions related to the differences across countries do not hold. Beyond the limitations of the operationalization of the reflexive mind-set, there are theoretical aspects to consider. Reflexive modernization theory posits that those who possess more knowledge are better equipped to analyze the risks of modernity itself; in turn, we considered risk awareness as a motivation to engage with privacy management. However, many studies suggested a privacy paradox, which entails a discrepancy between the strong privacy concerns of people and their low tendency to actively protect their privacy online, especially among young people (Acquisti et al., 2015; Blank et al., 2014; Büchi et al., 2017; Hargittai and Marwick, 2016; Kokolakis, 2017; Park and Shin, 2020). This paradox may offer an alternative explanation as to why the perception of modern risks does not translate into more e-privacy management even among tech-savvy social segments.

Another reason why the expectations derived from reflexive modernization theory fail to find confirmation here may be the selection of countries. This study focused on countries within the European Union, which – differences notwithstanding – may all be considered to be reflexively modern. Setting aside potential limitations in data collection, expanding

to countries with varying levels of Internet freedom and online governmental censorship may offer opportunities to investigate the impact of different kinds of digital risks, and the unequal perception thereof, on e-privacy control in a more comprehensive way.

Our findings support the diffusion of innovation theory, and showed that higher and lower educated tend to protect their online privacy to a similar extent in countries where digital processes are widespread, such as Nordic countries (Scandinavia and the Netherlands). In Southern/Eastern countries (e.g. Romania, Italy), the educational gap in e-privacy management persists. What remains unclear is which of the many factors constituting the digital readiness of a country drives the narrowing of the educational divide across contexts. Educational systems may play a role, since in countries where schools (and not only universities) are equipped with digital devices and training, digital skills may spread more easily across different social strata. Although in 2019, nearly, all EU countries included digital competences at each of the three main educational levels (Bourgeois et al., 2019), differences among countries persist (European Commission, 2019). Future research should focus on this aspect, considering also the accelerating effect that the COVID-19 pandemic is bringing to the digitalization processes by, for example, forcing online education at all school levels.

The diffusion theory also posits that the diffusion process repeats itself at the introduction of each new successful innovation (Rogers, 2003). This means that even in highly digitalized countries, new divides may open up as old ones close. In this study, the measure of e-privacy management refers to rather general behaviors that may have normalized over the years. Recent studies invite to continue to research the topic because, even in digitalized countries, divides in privacy-related behaviors, such as disclosing sensitive information or unknowingly giving up personal data, may occur. For instance, Park (2018) found that disclosure of political views on social media – and the consequent ability to engage in online communities – was more frequent among younger and higher-educated men. Another study found that younger people and those with higher income and education had a higher likelihood to employ apps for health-related issues: compared with one-to-one exchanges, for example, emails and texts to the GP, those systems involve the release of personal information to a third party, which may expose users to unwanted consequences (Park and Shin, 2020).

This issue of the opening of new divides when new technologies are introduced warns caution in interpreting the finding that education does not affect e-privacy management among younger cohorts. As technologies evolve, so do systems to harvest personal data. Today's youth will probably need advanced digital skills to effectively manage their privacy as tomorrow's adults, it may be that the general notions learnt in school to protect e-privacy in this moment will not suffice in the future, exacerbating divides between those who pursued higher/specialized education and those who did not.

Our study presents some limitations in terms of measurements. First, the measures of e-privacy management refer to a rather general use of the Internet and/or to the use of pcs. Although a general measure can work well in general-purpose surveys such as the Eurobarometer, it also does not fully account for the diffusion of mobile devices, which constitute the primary access to Internet for many people in lower social strata nowadays. This may lead to an underestimation of the e-privacy management activities among lower educated people. Moreover, our study is limited to a specific type

of e-privacy management linked to cybersecurity. A more encompassing measure of e-privacy management should take into account the communication and social aspects of disclosing personal information on apps and social media. Second, the measure of education as the number of years spent in education does not allow to properly distinguish among levels of educational achievements, endangering comparability across countries. Finally, some studies found discrepancies between self-reported and observed digital skills, and also, more importantly, showed that these discrepancies depended on socio-demographic characteristics, for example, gender and income (see review by Litt, 2013a). Systematic bias in this instance may lead to serious flaws in any study tackling the digital divide using self-reported measures, and invites more research to assess and improve the quality of the measurement while maintaining feasibility, especially in general-purpose surveys.

In conclusion, in our study, we showed that there are educational gaps in e-privacy among the European general population and that they mostly pass through inequalities in the (skillful) use of Internet and not through risk awareness. In addition, however, we also found that a higher level of digitalization in a country smoothens educational differences in e-privacy management. Our findings indicate that effective policies to tackle the reproduction of inequalities in the digital environment should focus on strengthening citizens' digital competences (Büchi et al., 2017). This should not be left to individual initiative and resources, but be part of a larger collective effort, so that everyone can profit from, and possibly contribute to, the digital developments of a country.

Acknowledgements

The authors are grateful to the co-editor and the reviewers for their valuable comments on the manuscript. They are also thankful for the comments received at the conferences and workshops where earlier versions of this work were presented.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

ORCID iD


Angelica M Maineri https://orcid.org/0000-0002-6978-5278

Supplemental material

Supplemental material for this article is available online.

Notes

1. Exact wording of question QD17 'Among the following possible actions you might have undertaken in the last three years because of security and privacy issues when using the Internet please select those that apply to you?' – multiple answers.
2. The three items displayed factor loadings below 0.40 and, the uniqueness (unexplained variance) was 0.84 and above.
3. A measure of the highest attained level of education was not available.

4. To control for this, a dummy indicating whether respondents are students is employed in the models.
5. Retrieved from https://ec.europa.eu/digital-single-market/en/news/digital-economy-and-society-index-desi2017.

References

Acemoglu D (2002) Technical change, inequality, and the labor market. *Journal of Economic Literature* 40(1): 7–72.

Achterberg P, de Koster W and van der Waal J (2017) A science confidence gap: Education, trust in scientific methods, and trust in scientific institutions in the United States, 2014. *Public Understanding of Science* 26(6): 704720.

Acquisti A, Brandimarte L and Loewenstein G (2015) Privacy and human behavior in the age of information. *Science* 347(6211): 509–514.

Anthony D, Campos-Castillo C and Horne C (2017) Toward a sociology of privacy. *Annual Review of Sociology* 43(1): 249–269.

Bartsch M and Dienlin T (2016) Control your Facebook: An analysis of online privacy literacy. *Computers in Human Behavior* 56: 147–154.

Beck U (1992) *Risk Society: Towards a New Modernity*. London ; Newbury Park, CA: SAGE.

Beck U (2013) The digital freedom risk: Too fragile an acknowledgment. Available at: https://www.opendemocracy.net/en/can-europe-make-it/digital-freedom-risk-too-fragile-acknowledgment/ (accessed 22 October 2019).

Blank G, Bolsover G and Dubois E (2014) A new privacy paradox : Young people and privacy on social network sites. In: *Annual meeting of the American Sociological Association*, San Francisco, CA, 17 August.

Bourgeois A, Birch P and Davydovskaia O (2019) Digital education at school in Europe. *Eurydice Brief*. 1–28. DOI: 10.2797/339457

Bovens M and Wille A (2017) *Diploma Democracy: The Rise of Political Meritocracy*. Oxford: Oxford University Press.

boyd D and Hargittai E (2010) Facebook privacy settings: Who cares? *First Monday* 15(8): 1–11.

Büchi M, Just N and Latzer M (2017) Caring is not enough: The importance of Internet skills for online privacy protection. *Information Communication & Society* 20(8): 1261–1278.

Cho H and LaRose R (1999) Privacy issues in Internet surveys. *Social Science Computer Review* 17(4): 421–434.

Cho H, Rivera-Sanchez M and Lim SS (2009) A multinational study on online privacy: Global concerns and local responses. *New Media & Society* 11(3): 395–416.

Cruz-Jesus F, Vicente MR, Bacao F, et al. (2016) The education-related digital divide: An analysis for the EU-28. *Computers in Human Behavior* 56: 72–82.

Debatin B, Lovejoy JP, Horn AK, et al. (2009) Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication* 15(1): 83–108.

European Commission (2019) *2nd Survey of Schools: ICT in Education Objective 1: Benchmark Progress in ICT in Schools*. Luxembourg: European Commission.

European Commission and European Parliament (2017) *Eurobarometer 87.1 (2017). TNS opinion, Brussels* [producer]. GESIS Data Archive, Cologne. ZA6861 (Data file Version 1.2.0). Available at: https://dbk.gesis.org/dbksearch/SDesc2.asp?DB=E&no=6861

Eurostat (2020) Population by educational attainment level, sex and age (%) – main indicators (online data code: EDAT_LFSE_03). Available at: https://ec.europa.eu/eurostat/databrowser/view/EDAT_LFSE_03__custom_665742/default/table?lang=en (accessed 10 March 2021).

Hargittai E (2002) Second-level digital divide : Differences in people's online skills. *First Monday* 7(4–1): 1–19.

Hargittai E and Marwick A (2016) 'What can I really do?' Explaining the privacy paradox with online apathy. International Journal of Communication 10(0). University of Southern California's Annenberg Center for Communication: 21. Available at: http://ijoc.org/index.php/ijoc/article/view/4655/1738 (accessed 2 November 2017).

Hargittai E, Gruber J, Djukaric T, et al. (2020) Black box measures ? How to study people's algorithm skills. *Information, Communication & Society* 23: 764775.

Hox JJ (2002) *Multilevel Analysis: Techniques and Applications*. Mahwah, NJ: Lawrence Erlbaum.

Kokolakis S (2017) Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security* 64: 122–134.

Kolenikov S and Angeles G (2004) *The use of discrete data in principal component analysis with applications to socio-economic indices*. Working paper No. WP-04-85. Available at: https://www.measureevaluation.org/resources/publications/wp-04-85

Litt E (2013a) Measuring users' internet skills: A review of past assessments and a look toward the future. *New Media & Society* 15(4): 612–630.

Litt E (2013b) Understanding social network site users' privacy tool use. *Computers in Human Behavior* 29(4): 1649–1656.

Litt E and Hargittai E (2014) A bumpy ride on the information superhighway: Exploring turbulence online. *Computers in Human Behavior* 36: 520–529.

Lupton D (1997) Consumerism, reflexivity and the medical encounter. *Social Science & Medicine* 45(3): 373–381.

Lupton D (2016) Digital risk society. In: Burgess A, Alemanno A and Zinn J (eds) *The Routledge Handbook of Risk Studies*. London: Routledge, pp. 301–309.

Lutz C (2019) Digital inequalities in the age of artificial intelligence and big data. *Human Behavior and Emerging Technologies* 1(2): 141–148.

Lyon D (2005) *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination* (ed. Lyon D). London; New York: Routledge.

McIlroy D, Brownrigg R, Minka TP, et al. (2018) mapproj: Map projections. Available at: https://rdrr.io/cran/mapproj/

Makarovs K and Achterberg P (2017) Contextualizing educational differences in 'vaccination uptake': A thirty nation survey. *Social Science & Medicine* 188: 1–10.

Mann M and Matzner T (2019) Challenging algorithmic profiling : The limits of data protection and anti-discrimination in responding to emergent discrimination. *Big Data & Society*. Epub ahead of print 16 December. DOI: 10.1177/2053951719895805.

Marx GT (2016) *Windows into the Soul: Surveillance and Society in an Age of High Technology*. Chicago, IL; London: The University of Chicago Press.

Nettleton S and Burrows R (2003) ICTs and processes of reflexive modernization. *Critical Social Policy* 23(2): 165–185.

Neuman WR, Bimber B and Hindman M (2011) The Internet and four dimensions of citizenship. In: Shapiro R and Jacob R (eds) *The Oxford Handbook of American Public Opinion and the Media*, pp. 22–42 Oxford: Oxford University Press.

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

Park YJ (2011) Digital literacy and privacy behavior online. *Communication Research* 40(2): 215–236.

Park YJ (2013) Offline status, online status: Reproduction of social categories in personal information skill and knowledge. *Social Science Computer Review* 31(6): 680–702.

Park YJ (2015) Do men and women differ in privacy? Gendered privacy and (in)equality in the Internet. *Computers in Human Behavior* 50: 252–258.

Park YJ (2018) Social antecedents and consequences of political privacy. *New Media & Society* 20(7): 2352–2369.
Park YJ and Chung JE (2017) Health privacy as sociotechnical capital. *Computers in Human Behavior* 76: 227–236.
Park YJ and Shin D (2020) Contextualizing privacy on health-related use of information technology. *Computers in Human Behavior* 105: 106204.
Price AM and Peterson LP (2016) Scientific progress, risk, and development: Explaining attitudes toward science cross-nationally. *International Sociology* 31(1): 57–80.
R Core Team (2013) *R: A Language and Environment for Statistical Computing*. Vienna, Austria: R Foundation for Statistical Computing.
Robinson L, Cotten SR, Ono H, et al. (2015) Digital inequalities and why they matter. *Information, Communication & Society* 18(5): 569–582.
Rogers EM (2003) *Diffusion of Innovations*. 5th ed. New York: Free Press.
Scheerder A, van Deursen A and van Dijk J (2017) Determinants of Internet skills, use and outcomes. A systematic review of the second- and third-level digital divide. *Telematics and Informatics* 34: 16071624.
Sharp C (2002) School starting age : European policy and recent research. *LGA Seminar 'When Should Our Children Start School?'*, November. Available at: http://www.emie.co.uk/nfer/publications/44414/44414.pdf%5Cnhttp://www.nfer.ac.uk/nfer/publications/44414/
South A (2011) rworldmap: A new R package for mapping global data. *The R Journal* 3(1): 35–43.
StataCorp (2019) *Stata Statistical Software: Release 16*. College Station, TX: StataCorp.
van Deursen A and Helsper EJ (2015) The third-level digital divide: Who benefits most from being online? *Communication and Information Technologies Annual*, pp. 29–52. Available at: https://www.emerald.com/insight/content/doi/10.1108/S2050-206020150000010002/full/html
van Dijck J (2014) Datafication, dataism and dataveillance : Big Data between scientific paradigm and ideology. *Surveillance & Society* 12(2): 197–208.
van Dijk J (2005) *The Deepening Divide: Inequality in the Information Society*. Thousand Oaks, CA: SAGE.
van Dijk J (2013) A theory of the digital divide. In: Ragnedda M and Muschert GW (eds) *The Digital Divide: The Internet and Social Inequality in International Perspective*. New York: Routledge, pp. 29–51.
Wickham H (2016) Ggplot2: Elegant graphics for data analysis. Available at: https://ggplot2.tidyverse.org

Author biographies

Angelica M Maineri is a PhD student and assistant of the Methodology Group of the European Values Study. Her substantive research mostly focuses on privacy and surveillance in the digital era, and she also works on (Web) survey methodology.

Peter Achterberg is a professor of Sociology at the Department of Sociology, at Tilburg University. He is a cultural sociologist with a general interest in studying cultural, political, and religious change in the West.

Ruud Luijkx is Associate Professor at Tilburg University and Visiting Professor at the University of Trento. He is the Chair of the Executive Committee and Methodology Group of the European Values Study. His research interests revolve mostly around social stratification and mobility.

Date submitted 20 November 2020
Date accepted 13 May 2021