Media and Communication
2026 • Volume 14 • Article 11500
https://doi.org/10.17645/mac.11500

ARTICLE

Open Access Journal

Navigating Digital Surveillance in Later Life: Determinants of Identity Masking and Data Protection Practices

Sara Suárez-Gonzalo [1,2], Joel Peiruza-Parga [2], and Mireia Fernández-Ardèvol [1,2]

[1] Faculty of Information and Communication Sciences, Open University of Catalonia, Spain
[2] Communication Networks & Social Change Research Group (UOC-TRÀNSIC), Open University of Catalonia, Spain

Correspondence: Joel Peiruza-Parga (jpeiruza@uoc.edu)

Submitted: 31 October 2025 **Accepted:** 25 February 2026 **Published:** 2 April 2026

Issue: This article is part of the issue "Digital Resilience Within a Hypermediated Polycrisis" edited by Marc Esteve Del Valle (University of Groningen), Ansgard Heinrich (University of Groningen), and Anabel Quan-Haase (Western University), fully open access at https://doi.org/10.17645/mac.i499

Abstract

Surveillance is a systemic and systematic threat exacerbated by the context of polycrisis. Recent political and economic processes, focused on intensive data collection, have led to multiple agents engaging in both vertical and horizontal forms of surveillance. Within this context, this study addresses a gap in academic research by identifying the determinants of two types of protection practices that demonstrate the ability of older internet users in Spain to exercise resilience against digital surveillance: identity masking and data protection. Through logistic regression models, we analyse responses to an online survey (N = 505) conducted in late 2023 on perceptions and practices regarding surveillance by five agents: corporations, governments, social institutions, individuals, and malicious actors. Results indicate that greater engagement in both identity masking and data protection practices is related to ageist self-stereotypes and problematic conceptions of digital technologies, as well as to high and negative perceptions of surveillance by other individuals. However, perceptions of the remaining agents show no consistent effects on protection practices. These findings generate an interesting dialogue with previous contributions on resilience and surveillance, and invite further qualitative and contextual research into older adults' resilience and resistance to digital surveillance.

Keywords

data protection; digital protection practices; horizontal surveillance; identity masking; older internet users; digital surveillance; resilience to surveillance; vertical surveillance; Spain

1. Introduction

How, why, and by whom surveillance is exercised have all changed drastically over recent decades. Beyond being a source of political power, it has also become a global economic priority, and consequently, a myriad of agents engage in vertical and horizontal forms of surveillance for diverse purposes. As a result, surveillance has become a systemic and systematic threat to fundamental rights, liberties, and social justice (Raab et al., 2015; van Dijck et al., 2018; Zuboff, 2019).

This constant and unavoidable exposure to surveillance threatens fundamental rights such as privacy and data protection (DP). It hinders conscious control over the generation, spread, and use of the data produced by our daily activities, and hyper-exposes our identity by revealing several aspects of our lives to a growing number of social actors. However, research has shown that the perception of digital surveillance is not always related to greater engagement in digital protection practices (Gerber et al., 2018). While this evidence has been widely discussed, the specific case of older adults remains understudied, reinforcing digital ageism (Marciano, 2025).

This study aims to determine the determinants of digital protection practices adopted by older internet users (aged 60 and over) in Spain against surveillance. Spain is particularly relevant for the study of digital surveillance in later life, given the rapid expansion of internet use within this demographic, a process notably accelerated by the Covid-19 pandemic (Instituto Nacional de Estadística, n.d.). The country represents a characteristic instance of a Southern European welfare and digital ecosystem, distinguished by strong familial networks and with a past linked to a dictatorship in which study participants grew up.

To achieve this goal, we analysed data from an online survey as part of the international research project Aging in Data, conducted in late 2023. The project targeted the practices and perceptions of older internet users regarding five different surveillance agents. In addition to a set of articles that focused on each of the five surveillance agents separately across various countries (Fernández-Ardèvol et al., 2026; Gallistl et al., 2025; Léveillé et al., 2026; Nimrod et al., 2025; Rosenberg et al., 2026), this article examines all the agents simultaneously in Spain. Responses ($N = 505$) provide insights into older adults' digital attitudes and usage, as well as perceptions and evaluations of digital surveillance by the five agents. We relied on logistic regression models to analyse the relationship between the variables and two types of digital protection practices that emerged from our study: identity masking (IM) and data protection (DP). The question guiding our analysis is whether there is a distinct relationship (if any) between the high and negative perception of vertical (by institutional agents) and horizontal (by individuals) surveillance and IM or DP practices in later life.

We adopt a gerontoveillance (Marciano, 2025) perspective that incorporates the unique social and cultural dimensions of ageing, rather than framing surveillance merely as a care-related issue in later life. In doing so, we contribute to a much-needed understanding of the intersection of digital ageism and digital resilience to nowadays' pervasive surveillance in increasingly digitised ageing societies. Moreover, the study opens the door to further research that would help to find innovative ways to conceptualise digital resilience and to tackle sociodigital inequalities. The article is structured as follows: This introduction is followed by a review of the most recent and relevant academic literature on the subject. We then elaborate on our methodological approach for an analysis of the survey data, followed by a presentation and discussion of the principal findings. We conclude by acknowledging the limitations of our analysis and outlining potential directions for future research emerging from this work.

2. Older Adults' Resilience to Surveillance in a Polycrisis Scenario

2.1. A New Permanent Digital Surveillance System

In recent decades, a permanent digital surveillance system has been built up with significant implications for people's lives (Snowden, 2019; Zuboff, 2019).

State power has been traditionally linked to surveillance. From the mid-1900s until the fall of the Berlin Wall in 1989, the Stasi spied on the most intimate aspects of ordinary people. A vast network of informants was built, inducing civilians to betray their relatives and friends by reporting almost every aspect of citizens' lives. This was one of the most repressive and aggressive instances of state surveillance to date (Macrakis, 2008; Mayer-Schönberger & Cukier, 2014). In Spain, during Franco's regime (1939–1975), the Social Investigation Brigade was known for its harsh techniques of torture, infiltration, and "permanent and total surveillance" of all "enemies" of the state (Boletín Oficial del Estado, 1941). Years later, the al-Qaeda terrorist attacks in September 2001 constituted a turning point in the scope and scale of surveillance techniques. Already in 2001, Lyon (2001) highlighted an escalation of computer power allowing the storage, matching, retrieval, processing, marketing, and circulation of everyday life data. To prevent such an attack from happening again, the US Intelligence Community boosted a mass surveillance system. The US National Security Agency hired ICT specialists such as Edward Snowden, who, in 2013, overwhelmed by the magnitude of the mass surveillance system he had helped to create, revealed programmes such as PRISM (Snowden, 2019). In parallel, data also became a global economic priority. With the rise of "surveillance capitalism" (Zuboff, 2019), data became a raw material at the centre of a new economic order shaped by the growing influence of big technology corporations. Their ability to develop the technology for gathering and exploiting data, and their determination to commodify it, made these corporations inescapable digital intermediaries (Poell et al., 2019), becoming some of the richest companies in the world ("Fortune global 500," 2025).

As a result of these political and economic processes, Western societies are experiencing a major digital transformation configured around the intensive collection of data (Mayer-Schönberger & Cukier, 2014; van Dijck et al., 2018). Although surveillance—from the French *surveiller*—implies an intrinsic hierarchical superiority of the surveilling agent over the surveilled, the terms "vertical" and "horizontal" are respectively used in academic literature to refer to surveillance carried out by institutional agents (e.g., schools, governments, corporations) and by other individuals (Quinn & Epstein, 2023). Terms such as "lateral surveillance" (Andrejevic, 2002), "participatory surveillance" (Albrechtslund, 2008), "social searching" (Lampe et al., 2006), "social surveillance" (Marwick, 2012), and "intimate surveillance" (Leaver, 2017) refer to peer or horizontal surveillance, with nuances. Regarding parent–child, child–parent, and parent–parent digital surveillance, Mols et al. (2023) advocate for the term "family surveillance."

Surveillance in this context (also known as "dataveillance") is inherent in the daily use of ICTs and has become pervasive, systemic, and systematic (Büchi et al., 2022). Consequently, a wide range of surveillance agents can now gather and process data. Essentially, corporations, governments, social institutions, other individuals, and malicious actors analyse data for a variety of purposes, including political or social control, economic profit, caring for relatives, or a combination of these (Nimrod, 2024).

2.2. Resilience to Surveillance in a Polycrisis Scenario

Resilience is a controversial concept, whose lights and shadows have been discussed by different academic schools of thought (Bourbeau, 2013; Neocleous, 2013). Feminist theory, for example, has criticised how neoliberalism has used it to reframe structural issues as personal, often placing the onus on vulnerable individuals or groups to resolve them (McAfee & Howard, 2023). Raab et al. (2015) critically analyse pertinent contributions to resilience studies and apply them to the context of mass surveillance after Snowden. Drawing on their work, we define resilience to surveillance as the individual or social capacity to cope with, withstand, recover from, or successfully adapt to the impact, stress, and shock caused by surveillance. Resilience is, thus, a prerequisite for resistance, which can be considered a response that focuses on opposing, protesting, or implementing defensive measures to manage current surveillance. In the face of surveillance, digital protection practices are therefore evidence of the capacity for digital resilience.

Surveillance has usually been justified in the name of resilience to security threats, appealing to the traditional trade-off model between security and privacy (Monahan, 2012), as often happens with unpopular and repressive measures (Klein, 2007). Moreover, the current polycrisis scenario (Morin & Kern, 1999)—characterised by intersecting financial, ecological, migratory, geopolitical, and health crises—has recently been highlighted as a growing global risk (Serhan, 2023; Tooze, 2022; World Economic Forum, 2023), thus keeping arguments in favour of surveillance constantly active. Interestingly, Raab et al. (2015) note that, while this praxis has paradoxically forged a public understanding of "surveillance as resilience," the profoundly negative threats of surveillance require characterising and studying "resilience to surveillance." Hence, they conceptualise three fundamental elements of resilience to surveillance: (a) the reference point of normalcy, (b) the timescale, and (c) the role of perception. Firstly, resilience actions may encompass diverse strategies to anticipate, prevent, tolerate, absorb, recover, restore, resist, learn from the past and the present, and plan for the future. Their aim is to return to a previous state of normalcy or evolve towards a new one. Therefore, the reference point of normalcy operates as a driver for resilience. Even so, different social groups may differ in what is or should be "normal," and may evaluate differently the positive or negative nature of a given stress or shock, or the measures to counteract it. Secondly, the timescale of a stressful, aversive change is crucial for examining resilience. If its intensification is too slow, it may go unnoticed and its impacts can be hardly recognisable, thereby failing to prompt conscious and effective resilience. If, on the contrary, it is sudden, its consequences may be more clearly recognisable, which (in principle) facilitates resilience, unless full recovery is slow, partial, or uneven, blurring the effects of resilience and hindering its effectiveness. And thirdly, perception is key. Both the reference point of normalcy and the timescale influence citizens' perception of the situation and, consequently, their disposition for resilience. The perception of a shock-like stress differs strongly from a gradual, incremental, and sustained one. In the first case, the moment of perception is immediate, causing a well-identifiable shock. In the second, it is belated, eroding the reference point of normalcy and causing sustained stress that may be difficult to identify and resist.

Surveillance shocks such as the Snowden case or Cambridge Analytica increased citizens' concerns and led to certain resilience strategies (Boerman et al., 2021). However, they merely allowed a glimpse of a system that has been (and still is) stealthily, ubiquitously, and gradually deployed, with detrimental "chilling effects" that cause the "self-inhibition of (legitimate) behaviours" (Büchi et al., 2022, p. 2), including resilience to surveillance (Raab et al., 2015).

Although surveillance often impacts the whole population, it also tends to particularly harm certain individuals or social groups. This is the case of older adults, who have become the focus of both vertical and horizontal digital surveillance (Berridge & Fox Wetle, 2020). Nevertheless, despite many studies examining perceptions, attitudes, and practices regarding surveillance of younger citizens, or comparing younger and older cohorts, often with a low average age, the relationship between older people and surveillance remains understudied. Apart from some recent contributions (Marciano, 2025), exceptions are limited to the specific field of health and care (Friedman et al., 2022; Gupta & Chennamaneni, 2018; Marston et al., 2019; Morrison et al., 2021; Mortenson et al., 2015). Indeed, studies on the digital practices of older adults are often reduced to whether or not they use digital technologies and tend to present them as a "homogeneous group characterised by technophobia, digital illiteracy, and technology non-use" (Neves et al., 2018, p. 237).

Further emphasising the importance of studying surveillance in later life, research indicates that surveillance resilience is context-dependent and generation-specific. It depends on the exposure to global technological developments and the sociohistorical context in which each generation formed its views on surveillance (Kalmus et al., 2022; Raab et al., 2015). Thus, it is particularly relevant to study citizens' attitudes towards contemporary surveillance among those who experienced totalitarian or authoritarian regimes. Kalmus et al. (2022) demonstrate consistent generation-specific differences in the predictors of tolerance toward state or corporate surveillance by comparing an older cohort that mainly formed their worldviews under authoritarian regimes with a younger group without the same experience. Results indicate higher perceptions of state surveillance among older adults exposed to authoritarian or totalitarian regimes (in this case, Portugal and Estonia), more tolerance toward online state surveillance among the older group, and more tolerance toward corporate surveillance among the younger one. Similarly, Raab et al. (2015) report that citizens who have been exposed to long authoritarian regimes have increased vulnerability and decreased resilience towards new forms and technologies of surveillance. While their suspicion of the state remains high, they are more susceptible to surveillance exerted by private agents who are not perceived as harmful. In this respect, Duffy and Chan (2019, p. 121) note that people's behaviour is influenced by "imagined surveillance" or how they perceive the scrutiny they are subjected to and the opportunities or risks it may present, depending on whom they imagine is watching (Litt & Hargittai, 2016).

Consequently, this article closes a pertinent gap in the literature by concentrating on the factors that influence engagement in digital protection practices and their correlation with perceptions of digital surveillance among adults who are likely to have spent their childhood and youth in Francoist Spain.

2.3. From Perception to Resilience to Surveillance

The threats posed by digital surveillance have been widely discussed in terms of privacy harms. Although some studies confirm a positive correlation, scholars have also highlighted a "privacy paradox" demonstrating that people's digital practices do not necessarily align with their surveillance concerns (Gerber et al., 2018). This evidence underscores the importance of carefully analysing the role of perception in the ability to exercise digital resilience against surveillance through specific digital protection practices. Proponents of the "privacy calculus" approach argue that digital practices reflect a rational calculation of the risks and benefits of using digital technologies, which influences the likelihood of engaging in digital protection practices or leads to non-protective behaviours (Barth & de Jong, 2017; Dienlin, 2023), including among older people (Gupta & Chennamaneni, 2018). The proven discordance between practices and

concerns, which from the privacy calculus perspective is not necessarily paradoxical, has been attributed to informational gaps, cultural backgrounds, or negative privacy experiences (Kalmus et al., 2022), as well as online apathy or digital resignation (Draper & Turow, 2019; Hargittai & Marwick, 2016). Segijn et al. (2022) found a positive relationship between the perceived level of surveillance (PS) and privacy concerns, privacy risk perception, perceived vulnerability, perceived severity, creepiness, surveillance concerns, and perceived personalisation.

Engagement in digital protection practices in the face of surveillance or privacy threats has been linked to privacy and surveillance concerns and attitudes, and to factors often associated with the digital divide. These include digital knowledge, skills, experience, the diversity of internet use, and sociodemographic factors like education, gender, age, and socioeconomic status (Bartol et al., 2024; Büchi et al., 2021; Hänninen et al., 2025). Boerman et al. (2021) contend that individuals are more likely to protect their privacy online when they believe their protective practices are effective, and perceive the collection, use, and sharing of their personal information on the internet as a severe problem. However, their findings did not reveal a connection between perceived susceptibility to online privacy threats and perceived self-efficacy in protecting privacy online. Kalmus et al. (2022) identify self-confidence and functional diversity in internet use, trust in the media, digital skills, attitudes, values, and mindsets as predictors of tolerance toward surveillance. Furthermore, they note that people tend to be more concerned about others receiving sensitive information about them than about algorithms collecting their data. Conversely, Quan-Haase and Ho (2020) argue that older adults are less concerned about social privacy than about security or institutional privacy, and Dombrowski (2023) highlights the social and context-dependent nature of privacy protection.

Regarding older adults, Mariano et al. (2022) highlight that the anxiety linked to the worry of confirming negative age stereotypes about technological inability leads older adults to decrease their use of technology. This is influenced, in turn, by the perceived usefulness and ease of use of technology. Ageist (self-)stereotypes regarding technology use are therefore a relevant factor in understanding older people's digital practices (Köttl et al., 2021; Mannheim et al., 2023). Similarly, in addition to the digital divide, Marston et al. (2019) identify apprehension about digital technology, a lack of interest, and difficulty in learning to use it as detractors of older adults' technology use. Conversely, having access to technology, perceived learning and sharing opportunities, being connected with relatives and friends, or being reachable in case of a health emergency are drivers for technology use in later life. In that regard, Boström et al. (2013) previously noted that older people often have ambivalent feelings and attitudes towards online surveillance: While they highly value privacy, they will accept some surveillance if it ensures security, leading to both positive and negative feelings about surveillance. Trust in the surveillance agent and the perceived need for surveillance have also proven to play a relevant role in its acceptance (Thompson et al., 2020). The term "careful surveillance" acknowledges this conflicting relation between trust and certain horizontal forms of surveillance including self, mutual, everyday, interpersonal, careful, and caring surveillance (Andrejevic et al. 2021).

Finally, studies indicate that surveillance concerns may be addressed differently by diverse types of digital protection practices. Thus, it has been argued that it is crucial to differentiate between practices intended to enhance general caution or limit the self-disclosure of information from those aimed at technically safeguarding privacy (Boerman et al., 2021; Buchanan et al., 2007); as well as between those intended to address the audience, the content, or the connection to one's identity (Duffy & Chan, 2019).

3. Methods

Drawing on the literature discussed, this study focuses on identifying the factors determining the adoption of different digital protection practices by older internet users. Following the surveillance network framework (Marciano, 2019), we analyse the perceived surveillance and the positive or negative evaluation of five agents as identifiers of vertical and horizontal contexts in which surveillance can occur (Quinn & Epstein, 2023). Vertical surveillance originates from commercial corporations and companies (e.g., retailers, department stores, technology companies), government agencies and state or local authorities, social institutions (e.g., non-profit organisations, religious institutions, political movements, social clubs), and malicious actors (e.g., scammers, criminals, entities involved in defrauding or stealing information). Horizontal surveillance originates from individuals (e.g., family members such as children and siblings, close friends). Based on the literature, we additionally consider three other sets of factors expected to influence surveillance acceptance and digital protection practices. The first is attitudes towards digital technology (or digital attitudes): self-stereotypes and the feeling that technologies are problematic may compromise older individuals' adoption of new technologies. The second is whether more digital usage leads to higher digital protective practices, and the last is sociodemographic characteristics such as age, gender, and income.

Analyses were conducted with SPSS v29 (principal components analysis) and R v4.4.1 (logistic regressions—glm function available on the base "stats" package).

3.1. The Sample

Given the relevance of the Spanish context for studying digital surveillance in later life, we analyse data gathered in Spain (N = 505) from a survey conducted in late 2023 across six countries through an opt-in online panel, as part of the Aging in Data project. The questionnaire (available in Nimrod, 2024) was originally written in English and subsequently translated into Spanish by the same research team involved in the project. To fully ensure consistency, an iterative process of back-translation was carried out until the translation accurately matched the original. The questionnaire design operationalises a range of attitudinal factors and self-declared behaviours related to ICT uses, the perceived surveillance by different agents, attitudes and concerns about the use of digital technologies and surveillance outcomes, and online protection practices. It also includes sociodemographics and other potential confounders.

With an average age of 67.89 years (SD 1.16), up to 60% of respondents identified as male, and almost one-third (29.9%) declared educational attainment up to high school. The usual selection biases in online surveys (e.g., Cea D'Ancona, 2025) were influenced by the digital divide affecting later life in the country (Instituto Nacional de Estadística, n.d.). Informed participation in the study required more than basic digital skills, resulting in a sample that was younger and better educated than the average Spanish population aged 60 and over, with an over-representation of male participants. Furthermore, 47.5% of respondents reported living in a large city or its suburbs (only 22% in a rural area), 78% had children, and 62% were retired. Regarding digital practices, one-to-one communication was the most frequent purpose of internet use, with 30% always using the internet for this purpose (57% doing so often). These sociodemographic and sample features will be considered for a more nuanced discussion.

3.2. Key Variables

To measure older adults' digital protection practices, we analysed 14 items with values ranging from 1 (*never*) to 5 (*always*). The data demonstrated the necessary underlying correlation (KMO 0.970, Bartlett's test of sphericity $p < 0.001$). We used a principal components analysis with Varimax rotation of 13 variables (one excluded because of a lack of significant load in the principal components analysis, leading to loads of at least 0.49 for the remaining). To handle missing values, we used mean substitution, a valid approach in social sciences when the underlying correlation is high and missing values are limited (in our case, always below 5% except for one variable, which was 6.6%). The two extracted factors (eigenvalues > 1) explained 55.6% of the variance. Results revealed an underlying structure of two factors which constitute interpretable and meaningful types of protective practices: IM and DP. Drawing on evidence from the aforementioned studies, they are sufficiently relevant to be analysed separately. Given the modest percentage of the explained variance, IM and DP were operationalised as affirmative (value 1) when participants reported undertaking at least sometimes more than half of the practices listed in Table 1 (value 0 otherwise). This threshold acknowledged the impossibility of always implementing the analysed practices and sought to identify cases in which digital protection was varied and, as a result, appeared more integrated into individuals' daily lives. The dichotomisation process also resolved the issue of missing values. Table 1 presents the elements and distribution of each type of protection practice. IM refers to a range of strategies that enable users to protect their personal identity or individual traits through procedures that do not necessarily require advanced digital skills. DP, on the other hand, encompasses a range of practices aimed at protecting data, some of which require a higher degree of digital competence. Notably, IM and DP show distinct patterns of

Table 1. Elements and distribution of IM and DP protective practices (endogenous variables; $n = 503$).

While using the internet, how often do you do the following things? (1 *Never*–5 *Always*).	Mean	*SD**	Missing *N**
Identity masking (IM)			
Decide not to use a website because they ask for your real name	2.53	1.280	13
Delete or edit something you posted in the past	2.16	1.168	18
Use a temporary username or email address	1.95	1.116	9
Use a fake name or untraceable username	1.86	1.130	6
Give inaccurate or misleading information about yourself	1.77	1.046	9
Ask someone to remove something that was posted about you online	1.65	0.987	18
Use a public computer to browse anonymously	1.50	0.937	5
Data protection (DP)			
Clear cookies and browser history	3.28	1.289	8
Restrict the amount of personal data seen by other people in your social media profiles	3.13	1.389	13
Use a pop-up window blocker	2.67	1.367	20
Set your browser to disable or turn off cookies	2.58	1.287	22
Encrypt your communications (or make sure that the communication is encrypted by the app)	2.20	1.248	33
Use services that allow you to browse the web anonymously, such as a proxy server, Tor software, or a VPN	2.02	1.229	22

Note: * Missing values replaced by the respective variable average.

response regarding their frequency. The respondents reported doing DP practices nearly twice as frequently as IM practices on average, although some items in each construct were reported to be performed more frequently than others.

Table 2 shows the variables that we analyse as potential determinants of IM and DP (for a more detailed version, see Table S.1 in the Supplementary File).

Firstly, we examined the perceived surveillance (PS) by the agents in the study: corporations, governments, social institutions, individuals, and malicious actors. Respondents were presented with statements, following

Table 2. Exogenous variables in the logistic models (ordered by variable type) and their distribution ($N = 505$).

Continuous variables	Mean	*SD*
Device usage (number of devices)	2.89	1.156
Self-stereotypes (factor)	0.00	1.000
Problematic conceptions of digital technologies	2.60	0.861
Age	67.9	6.352
Discrete variables	***N***	**%**
Internet usage (weekly usage range, hours)		
0–7	112	22%
8–14	129	26%
15–21	121	24%
22–28	64	13%
>28	76	15%
NA	3	
Perceived surveillance (PS)		
Corporations (high)	342	68%
Governments (high)	256	51%
Social institutions (high)	164	32%
Malicious actors (high)	283	56%
Individuals (high)	88	17%
Negative evaluation of surveillance (NE)		
Corporations (high)	196	39%
Governments (high)	159	31%
Social institutions (high)	114	23%
Malicious actors (high)	253	50%
Individuals (high)	40	8%
Gender identity		
Male	304	60%
Female/Other	201	40%
Income declared		
Below average	368	73%
Above average	137	27%

the scale validated by Segijn et al. (2022). For each agent, respondents were invited to provide information on four dimensions: "To what extent do you believe that on the internet, [this agent is]…watching your every move/checking up on you/looking over your shoulder/entering your private space?" Answers ranged from (1) "strongly disbelieve" to (5) "strongly believe." Those answering (4) or (5) were then asked to evaluate the surveillance by that specific agent. Negative evaluation of perceived surveillance (NE) reflects the perception of those who considered such surveillance as either much more negative or more negative than positive. For the first measure (PS), we dichotomised responses, classifying individuals as having a "high perception" if they answered (4) or (5) on at least one item. The second measure (NE) is also dichotomous, identifying individuals who simultaneously perceived high surveillance and expressed a strong negative assessment of it. The responses for these two variables highlight several points. The agent with the highest level of PS is corporations (68% perceived it as high), followed by malicious actors (56%), and governments (51%). At the other end of the scale, social institutions (32%) and individuals (17%) are less often perceived as surveillance agents. When considering the assessment of surveillance when it is highly perceived, malicious actors are the most negatively evaluated (89%), followed by social institutions (70%), governments (62%), corporations (57%), and individuals (45%). In all cases, almost half of those with a high perception of surveillance by an agent evaluate this surveillance negatively.

Secondly, we analysed the number of devices and the frequency of internet usage. Respondents declared using an average of nearly three devices to access the internet, and half of them spent between eight and 21 hours on the internet per week. Thirdly, there are two indicators concerning attitudes towards technology. The first is age-related self-stereotypes regarding digital technologies ("self-stereotypes") which include three items: "If young people are residents in technology-land, I may be considered an immigrant"; "I am better at understanding and using technology than young people" [reverse coded]; "I am typically behind younger persons in my family in the technologies I use." We operationalised a single continuous measure of this variable using the factor score derived from a principal components analysis (KMO 0.62, Bartlett's test of sphericity $p < 0.001$). Then we operationalised problematic conceptions of digital technologies as an average measure of three statements, after confirming that they shared common variance, measured with values ranging from 1 (*strongly disagree*) to 5 (*strongly agree*). The items were: "The constant developments and upgrades in technologies are a burden for me"; "Technologies make me do things more slowly"; "Technologies create many more problems than I would otherwise experience." Finally, the sociodemographic variables serve as control variables, primarily considering age, gender self-identification and household income.

3.3. Model Specification

In Section 4, we discuss four logistic regression models aimed at explaining IM (Model 1, Model 3) and DP (Model 2, Model 4). Models 1 and 2 focus on PS by the five agents, whereas Models 2 and 4 consider NE of such surveillance. Beyond these, the models have the same structure and include digital attitudes, digital usage, and control variables as explanatory variables (Table 3). Note that previous specifications—not reproduced here—included other key items (mainly self-perceived digital knowledge and privacy risk), which were eventually excluded because they showed no stability across the models and did not improve the overall models' goodness of fit. Besides, the final socioeconomic variables are limited to age, gender, and income because the last two were found to capture other compositional effects (e.g., income captured the educational level)—possibly a consequence of the sample characteristics—and allowed a more straightforward interpretation. This approach

allows a parsimonious evaluation of the distinct effects on IM and DP while comparing differentiated analyses of surveillance perception among the older adults in the sample.

4. Results and Discussion

The four models have pseudo R^2 values ranging from 0.09 to 0.16 and adjust better for IM than for DP. They are also more stable when focused on the same dependent variables (i.e., Models 1 and 3, and 2 and 4). The variance inflation factors were verified, and no relevant multicollinearity was found (see Table S.2 in the Supplementary File). There is a compositional relationship regarding both IM and DP in the sample. Individuals who identified as female or with gender identities other than male are less likely to engage in either type of digital protection practice (coefficients between −0.456 and −0.409, Models 1 to 4). In parallel, higher income levels are negatively associated with IM and DP (coefficients between −0.552 and −0.407, Models 1 to 4).

Models' estimations (Table 3) reveal two robust determinants of both IM and DP. Firstly, age-related self-stereotypes show a significant relationship in the four models, with negative coefficients from −0.397 to −0.431. Secondly, the results are also robust across the four models concerning conceptions of digital technologies. Stronger problematic conceptions of digital technologies are associated with more engagement in IM and DP (parameters between 0.269 and 0.677). These results confirm the powerful role of age-related stereotypes and negative feelings towards digital technologies as mediators of the digital protection practices of older adults in the presence of surveillance (Boström et al., 2013; Mariano et al., 2022; Marston et al., 2019).

The number of devices and the frequency of internet usage have poor explanatory power, as neither yielded statistically significant parameters in any model. Regarding this result, the nuance introduced by Kalmus et al. (2022) enables an insightful interpretation in relation to the problematic conceptions of digital technologies and the role of self-stereotypes, as the relevance of use is not necessarily its intensity but the fact that it is self-confident and functional.

Regarding the influence of PS and NE, the results indicate that individual surveillance agents play a differentiated role. A high level of PS by other individuals, and its NE, are both consistently associated with engagement in digital protection practices across three of the four models. In particular, IM is increased by both PS by other individuals (0.693, Model 1) and its NE (0.943, Model 3), whereas DP is significantly increased by a NE of this agent (0.742, Model 4). Additionally, in Model 1, only PS by commercial corporations shows a significantly NE (−0.580) with IM, suggesting that individuals with higher levels of PS by corporations are less likely to engage in IM practices. Neither PS from other agents, nor their NE, are related to IM or DP.

Responding to our guiding research question, our results indicate a distinct relationship between the PS and NE of vertical and horizontal surveillance and the IM and DP practices of older internet users in Spain. This finding allows for an interesting discussion and several considerations. Firstly, our research demonstrates that, among older internet users in Spain, PS depends on the surveillance agent and, by extension, on the surveillance context (vertical or horizontal; Kalmus et al., 2022; Quan-Haase & Ho, 2020). Moreover, when this perception is high, its evaluation is predominantly negative. Secondly, the differing performance of IM and DP in the models confirms the analytical and conceptual pertinence of studying protection practices

Table 3. Logistic regressions: IM and DP models.

		Model 1 IM	Model 2 DP	Model 3 IM	Model 4 DP
Digital attitudes	Self-stereotypes (factor)	−0.412*** (0.146)	−0.431*** (0.117)	−0.423*** (0.144)	−0.397*** (0.115)
	Problematic conceptions of digital technologies	0.655*** (0.159)	0.269** (0.131)	0.677*** (0.160)	0.277** (0.131)
Digital usage	Internet usage (range of hours)	0.059 (0.087)	0.033 (0.073)	0.065 (0.087)	0.040 (0.072)
	Devices usage (number)	−0.099 (0.108)	0.081 (0.091)	−0.087 (0.107)	0.115 (0.091)
PS & NE of such surveillance, by agent	Corporations (PS)	−0.580** (0.284)	−0.030 (0.231)		
	Corporations (NE)			−0.245 (0.264)	−0.174 (0.215)
	Governments (PS)	0.130 (0.293)	0.193 (0.232)		
	Governments (NE)			−0.040 (0.306)	−0.096 (0.248)
	Social institutions (PS)	0.335 (0.291)	0.236 (0.246)		
	Social institutions (NE)			0.309 (0.321)	0.229 (0.272)
	Malicious actors (PS)	0.297 (0.275)	0.279 (0.218)		
	Malicious actors (NE)			−0.109 (0.244)	0.140 (0.198)
	Individuals (PS)	0.693** (0.294)	0.249 (0.274)		
	Individuals (NE)			0.943** (0.402)	0.742* (0.403)
Control variables	Age (log)	−2.001 (1.329)	−0.261 (1.084)	−1.637 (1.352)	−0.122 (1.084)
	Gender (female & other)	−0.456* (0.244)	−0.428** (0.199)	−0.440* (0.241)	−0.409** (0.198)
	Income (above average)	−0.552** (0.281)	−0.407* (0.219)	−0.522* (0.278)	−0.408* (0.218)
	Constant	5.73 (5.691)	−0.016 (4.661)	4.189 (5.771)	−0.470 (4.653)
	R^2 Nagelkerke	0.16	0.10	0.14	0.09
	Log likelihood	−242.751	−328.771	−246.657	−330.874
	Akaike Information Criterion	511.502	683.541	519.314	687.748

Notes: $n = 502$; reported values—ß (*SD*); *** $p < 0.01$, ** $p < 0.05$, * $p < 0.1$.

separately (Boerman et al., 2021; Buchanan et al., 2007; Duffy & Chan, 2019). Thirdly, the inconsistent association of PS by corporations with IM (not consistent in the case of NE in either of the models or in relation to DP when examining PS), and the lack of relationship of both the PS and NE of the remaining agents with IM and DP (with the exception of individuals), reinforce previous findings on the discrepancy between concerns about digital surveillance and the absence of digital protection practices (Gerber et al., 2018). This also highlights the importance of studying vertical and horizontal surveillance separately, as they may be influenced by different factors that compromise protection against them (Andrejevic et al., 2021; Boerman et al., 2021; Dombrowski, 2023; Kalmus et al., 2022; Thompson et al., 2020). In this regard, the influence of PS from individuals (horizontal surveillance) and its NE in both IM and DP is interesting when considering some contextual elements. One is that surveillance by individuals is the least perceived as high, and that half of those who perceive it as high evaluate it negatively. Another is that, even if DP practices are more frequent, IM shows more association with PS or NE. It should be noted that one-to-one communication is the most frequent internet use purpose of respondents, and the vast majority of them have children. Lastly, trust in the surveillance agent and the need to stay connected with them are relevant drivers of surveillance acceptance (Marston et al., 2019; Thompson et al., 2020), independently of whether this may generate ambivalent or negative feelings (Boström et al., 2013). Ultimately, our study does not confirm previous associations of digital protection practices (Kalmus et al., 2022) with knowledge gaps or the perceived risk to privacy, given that these did not perform well in our models. Instead, it draws attention to the relevant role of self-stereotypes and problematic conceptions of technologies as potential predictors of apparent digital apathy or resignation in later life (Draper & Turow, 2019; Hargittai & Marwick, 2016).

Based on our results, qualitative studies would be useful to explore further why horizontal—and not vertical—surveillance activates digital protective practices. From the perspective of horizontal surveillance (whether in later life or not), digital protective practices may constitute ways of negotiating trust, intimacy, safety, and control with others to sustain digital autonomy (Andrejevic et al., 2021). Thus, our study suggests that older people appear to be in a period in which surveillance by other individuals, and therefore horizontal forms of surveillance, might be under special negotiation. The role of perceived severity and ineffectiveness of protective practices against vertical surveillance is also worth exploring further (Boerman et al., 2021), as well as whether surveillance protection is related to a rational calculus (Dienlin, 2023; Gupta & Chennamaneni, 2018) or ambivalent feelings and attitudes (Boström et al., 2013). It is also relevant to further investigate the social and contextual elements shaping older adults' protection practices, including the generational experience of the Spanish dictatorship, along with the slow and stealthy transition to a mass digital surveillance system (Dombrowski, 2023; Kalmus et al., 2022; Raab et al., 2015) marked by a context of polycrisis. These are structural factors that also affect "possible" and "effective" protection practices against surveillance.

5. Conclusion

This study offers novel insights into the determinants of digital resilience to surveillance among older internet users in Spain, successfully dissecting protective practices into two distinct strategies to prevent and cope with surveillance: IM and DP. It does so in a context of polycrisis that keeps arguments in favour of a mass surveillance system constantly active. This system has been stealthily, ubiquitously, and gradually implemented over recent decades, eroding the reference points of normalcy and causing sustained stress that may be difficult to recognise and resist.

Results indicate that only the high and negative perception of horizontal surveillance (by individuals), alongside ageist-related digital attitudes, are associated with greater engagement in both IM and DP practices among older internet users in Spain. Neither the high perception nor the negative evaluation of vertical surveillance (by corporations, governments, social institutions, or malicious actors) play a relevant role. We therefore conclude that it is of paramount importance to cautiously assess the role of high surveillance perception as a predictor of resilience to surveillance to avoid: firstly, placing the burden on individuals to cope with its detrimental effects; and secondly, seeking individualistic answers to the lack of association between the high levels of perception and negative evaluation of surveillance and the lack of engagement in protection practices. To thoroughly understand older adults' protective practices against surveillance, it is relevant to analyse, at least, their perception of: (a) the context and vertical or horizontal nature of surveillance and its effects; (b) the surveillance agent—acknowledging the conflicting influence of dynamics of trust and care, or the potential benefit of being under its surveillance; (c) the effectiveness of diverse types of digital protection practices when facing specific surveillance agents; (d) ageist stereotypes regarding digital technologies; and (e) the useful and confident or, on the contrary, problematic conceptions of technologies. These perceptions must be contextually assessed in relation to the generation-specific experience of surveillance, including the sociocultural background and the global technological developments witnessed. All of these factors shape the reference point of normalcy, the timescale, and the perception of surveillance, and consequently, resilience and resistance to it.

This study has limitations. Firstly, the sample of older internet users is not fully representative of the general Spanish population aged 60 and over. Specifically, due to the digital divide affecting later life, the participants are typically younger, better educated, and there is an over-representation of male respondents. Besides excluding less digitally proficient users, an opt-in online panel might skew the sample towards particular forms of digital privacy concerns, a dimension that warrants further research. Furthermore, as this analysis relies on cross-sectional data, the assumed causal relationships in the logistic regression models are theoretically grounded but cannot be definitively established.

Acknowledgments

The authors acknowledge the contributions of the Aging in Data team and the participants in the lectures given.

Funding

This research is part of the following competitive projects: (a) Aging in Data (895–2021-1020, Social Sciences and Humanities Research Council of the Government of Canada); (b) Grup SGR Consolidat Communication Networks and Social Change (2021 SGR 01397, Agència de Gestió d'Ajuts Universitaris i de Recerca, Generalitat de Catalunya). Sara Suárez-Gonzalo's contribution has been funded by the research grants: Juan de la Cierva-Formación FJC2020–044757-I (Ministerio de Ciencia e Innovación/Agencia Estatal de Investigación [Gobierno de España]/10.13039/501100011033 and the European Union/NextGenerationEU/PRTR), and José Castillejo (CAS22/00216, Ministerio de Universidades, Gobierno de España).

Conflict of Interests

The authors declare no conflict of interests.

Data Availability

Data and materials to be archived at Concordia University's Borealis Data Repository (https://borealisdata.ca/dataverse/concordia).

Supplementary Material

Supplementary material for this article is available online in the format provided by the authors (unedited).

References

Albrechtslund, A. (2008). Online social networking as participatory surveillance. *First Monday*, *13*(3). https://firstmonday.org/ojs/index.php/fm/article/download/2142/1949

Andrejevic, M. (2002). The work of watching one another: Lateral surveillance, risk, and governance. *Surveillance & Society*, *2*(4), 479–497. https://doi.org/10.24908/ss.v2i4.3359

Andrejevic, M., Davies, H., DeSouza, R., Hjorth, L., & Richardson, I. (2021). Situating 'careful surveillance.' *International Journal of Cultural Studies*, *24*(4), 567–583. https://doi.org/10.1177/1367877921997450

Barth, S., & de Jong, M. D. T. (2017). The privacy paradox: Investigating discrepancies between expressed privacy concerns and actual online behavior. *Telematics and Informatics*, *34*(7), 1038–1058. https://doi.org/10.1016/j.tele.2017.04.013

Bartol, J., Prevodnik, K., Vehovar, V., & Petrovčič, A. (2024). The roles of perceived privacy control, internet privacy concerns and Internet skills in the direct and indirect Internet uses of older adults. *New Media & Society*, *26*(8), 4490–4510. https://doi.org/10.1177/14614448221122734

Berridge, C., & Fox Wetle, T. (2020). Why older adults and their children disagree about in-home surveillance technology, sensors, and tracking. *The Gerontologist*, *60*(5), 926–934. https://doi.org/10.1093/geront/gnz068

Boerman, S. C., Kruikemeier, S., & Zuiderveen Borgesius, F. J. (2021). Exploring motivations for online privacy protection behavior. *Communication Research*, *48*(7), 953–977. https://doi.org/10.1177/0093650218800915

Boletín Oficial del Estado. (1941). *Ley por la que se reorganizan los servicios de Policía* (BOE-A-1941-3293). https://www.boe.es/buscar/doc.php?id=BOE-A-1941-3293

Boström, M., Kjellström, S., & Björklund, A. (2013). Older persons have ambivalent feelings about the use of monitoring technologies. *Technology and Disability*, *25*(2), 117–125. https://doi.org/10.3233/TAD-130376

Bourbeau, P. (2013). Resiliencism: Premises and promises in securitisation research. *Resilience*, *1*(1), 3–17. https://doi.org/10.1080/21693293.2013.765738

Buchanan, T., Paine, C., Joinson, A. N., & Reips, U. (2007). Development of measures of online privacy concern and protection for use on the internet. *Journal of the American Society for Information Science and Technology*, *58*(2), 157–165. https://doi.org/10.1002/asi.20459

Büchi, M., Festic, N., Just, N., & Latzer, M. (2021). Digital inequalities in online privacy protection. In E. Hargittai (Ed.), *Handbook of digital inequality* (pp. 293–307). Edward Elgar. https://doi.org/10.4337/9781788116572.00029

Büchi, M., Festic, N., & Latzer, M. (2022). The chilling effects of digital dataveillance. *Big Data & Society*, *9*(1). https://doi.org/10.1177/20539517211065368

Cea D'Ancona, M. Á. (2025). Survey quality in digital society: Advances and setbacks. *Revista Española de Investigaciones Sociológicas*, *191*, 25–42. https://doi.org/10.5477/cis/reis.191.25-42

Dienlin, T. (2023). Privacy calculus: Theories, studies, and new perspectives. In S. Trepte & P. Masur (Eds.), *The Routledge handbook of privacy and social media* (pp. 70–79). Routledge.

Dombrowski, J. (2023). What does it take? Factors determining individual privacy regulation. In M. Hennemann, K. V. Lewinski, D. Wawra, & T. Widjaja (Eds.), *Data disclosure* (pp. 89–104). De Gruyter. https://doi.org/10.1515/9783111010601-006

Draper, N. A., & Turow, J. (2019). The corporate cultivation of digital resignation. *New Media & Society*, *21*(8), 1824–1839. https://doi.org/10.1177/1461444819833331

Duffy, B. E., & Chan, N. K. (2019). "You never really know who's looking": Imagined surveillance across social media platforms. *New Media & Society*, *21*(1), 119–138. https://doi.org/10.1177/1461444818791318

Fernández-Ardèvol, M., Suárez-Gonzalo, S., & Karadkar, U. (2026). Older adults' perception of digital surveillance by civil society organisations: Disappointment and protective practices. *Journal of Global Ageing*. Advance online publication. https://doi.org/10.1332/29767202Y2025D000000041

Fortune global 500: 2025. (2025). *Fortune*. https://fortune.com/ranking/global500

Friedman, A. B., Pathmanabhan, C., Glicksman, A., Demiris, G., Cappola, A. R., & McCoy, M. S. (2022). Addressing online health privacy risks for older adults: A perspective on ethical considerations and recommendations. *Gerontology and Geriatric Medicine*, *8*. https://doi.org/10.1177/23337214221095705

Gallistl, V., Fernández-Ardèvol, M., Suárez-Gonzalo, S., & Peine, A. (2025). Privacy apathy in later life? Online surveillance perception and privacy protection among older internet users. *Journal of Global Ageing*. Advance online publication. https://doi.org/10.1332/29767202Y2025D000000040

Gerber, N., Gerber, P., & Volkamer, M. (2018). Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & Security*, *77*, 226–261. https://doi.org/10.1016/j.cose.2018.04.002

Gupta, B., & Chennamaneni, A. (2018). Understanding online privacy protection behavior of the older adults. *Journal of Information Technology Management*, *29*(3), 1–13.

Hänninen, R., Taipale, S., & Haapio-Kirk, L. (2025). *Digital repertoires: Embedded and everyday technologies in later life*. UCL Press. https://doi.org/10.14324/111.9781800088443

Hargittai, E., & Marwick, A. (2016). "What can i really do?" Explaining the privacy paradox with online apathy. *International Journal of Communication*, *10*, 3737–3757. https://ijoc.org/index.php/ijoc/article/view/4655

Instituto Nacional de Estadística. (n.d). *Encuesta sobre equipamiento y uso de tecnologías de información y comunicación en los hogares 2024*. https://ine.es/dynt3/inebase/es/index.htm?padre=11811

Kalmus, V., Bolin, G., & Figueiras, R. (2022). Who is afraid of dataveillance? Attitudes toward online surveillance in a cross-cultural and generational perspective. *New Media & Society*, *26*(9), 5291–5313. https://doi.org/10.1177/14614448221134493

Klein, N. (2007). *The shock doctrine*. Metropolitan Books.

Köttl, H., Gallistl, V., Rohner, R., & Ayalon, L. (2021). "But at the age of 85? Forget it!": Internalized ageism, a barrier to technology use. *Journal of Aging Studies*, *59*, Article 100971. https://doi.org/10.1016/j.jaging.2021.100971

Lampe, C., Ellison, N., & Steinfield, C. (2006). A face(book) in the crowd: social Searching vs. social browsing. In P. Hinds & PD. Martin (Eds.), *CSCW '06: Proceedings of the 2006 20th anniversary conference on Computer supported cooperative work* (pp. 167–170). ACM. https://doi.org/10.1145/1180875.1180901

Leaver, T. (2017). Intimate surveillance: Normalizing parental monitoring and mediation of infants online. *Social Media + Society*, *3*(2). https://doi.org/10.1177/2056305117707192

Léveillé, F., Lafontaine, C., Peine, A., Karadkar, U., & Sawchuk, K. (2026). Bad actors as agents of surveillance: Older adults' perceptions of online surveillance by scammers and criminals. *Journal of Global Ageing*. Advance online publication. https://doi.org/10.1332/29767202Y2025D000000046

Litt, E., & Hargittai, E. (2016). The imagined audience on social network sites. *Social Media + Society*, *2*(1). https://doi.org/10.1177/2056305116633482

Lyon, D. (2001). *Surveillance society: Monitoring everyday life*. Open University Press.

Macrakis, K. (2008). *Seduced by secrets: Inside the Stasi's spy-tech world*. Cambridge University Press.

Mannheim, I., Varlamova, M., van Zaalen, Y., & Wouters, E. J. M. (2023). the role of ageism in the acceptance and use of digital technology. *Journal of Applied Gerontology*, *42*(6), 1283–1294. https://doi.org/10.1177/07334648231163426

Marciano, A. (2019). Reframing biometric surveillance: From a means of inspection to a form of control. *Ethics and Information Technology*, *21*(2), 127–136. https://doi.org/10.1007/s10676-018-9493-1

Marciano, A. (2025). Toward a gerontoveillance approach: Studying surveillance in later life. *Journal of Global Ageing*. Ahead of print. https://doi.org/10.1332/29767202Y2025D000000044

Mariano, J., Marques, S., Ramos, M. R., Gerardo, F., Cunha, C. L. D., Girenko, A., Alexandersson, J., Stree, B., Lamanna, M., Lorenzatto, M., Mikkelsen, L. P., Bundgård-Jørgensen, U., Rêgo, S., & de Vries, H. (2022). Too old for technology? Stereotype threat and technology use by older adults. *Behaviour & Information Technology*, *41*(7), 1503–1514. https://doi.org/10.1080/0144929X.2021.1882577

Marston, H. R., Genoe, R., Freeman, S., Kulczycki, C., & Musselwhite, C. (2019). Older adults' perceptions of ICT: Main findings from the technology in later life (TILL) study. *Healthcare*, *7*(3), Article 86. https://doi.org/10.3390/healthcare7030086

Marwick, A. (2012). The public domain: Surveillance in everyday life. *Surveillance & Society*, *9*(4), 378–393. https://doi.org/10.24908/ss.v9i4.4342

Mayer-Schönberger, V., & Cukier, K. (2014). *Big data: A revolution that will transform how we live, work, and think*. Mariner Books.

McAfee, N., & Howard, K. B. (2023). Feminist political philosophy. In E. N. Zalta & U. Nodelman (Eds.), *The Stanford encyclopedia of philosophy*. Stanford University.

Mols, A., Pereira Campos, J., & Pridmore, J. (2023). Family surveillance: Understanding parental monitoring, reciprocal practices, and digital resilience. *Surveillance & Society*, *21*(4), 469–484. https://doi.org/10.24908/ss.v21i4.15645

Monahan, T. (2012). Surveillance and terrorism. In K. Ball, K. Haggerty & D. Lyon (Eds.), *Routledge handbook of surveillance studies* (pp. 285–291). Routledge.

Morin, E., & Kern, A. B. (1999). *Homeland earth: A manifesto for the new millennium*. Hampton Press.

Morrison, B., Coventry, L., & Briggs, P. (2021). How do older adults feel about engaging with cyber-security? *Human Behavior and Emerging Technologies*, *3*(5), 1033–1049. https://doi.org/10.1002/hbe2.291

Mortenson, W. B., Sixsmith, A., & Woolrych, R. (2015). The power(s) of observation: Theoretical perspectives on surveillance technologies and older people. *Ageing and Society*, *35*(3), 512–530. https://doi.org/10.1017/S0144686X13000846

Neocleous, M. (2013). Resisting resilience. *Radical Philosophy*, *178*(6), 2–7. https://www.radicalphilosophy.com/commentary/resisting-resilience

Neves, B. B., Waycott, J., & Malta, S. (2018). Old and afraid of new communication technologies? Reconceptualising and contesting the 'age-based digital divide.' *Journal of Sociology*, *54*(2), 236–248. https://doi.org/10.1177/1440783318766119

Nimrod, G. (2024). *Older adults' perceptions of ICT-based surveillance: The ageing in data (AiD) cross-national study*. Aging in Data. https://agingindata.ca/wp-content/uploads/2024/02/AiD-Surveillance-Study-Descriptive-report.pdf

Nimrod, G., Rosenberg, D., & Lifshitz, R. (2025). Perceived surveillance and technostress among older employees. *Journal of Global Ageing*. Advance online publication. https://doi.org/10.1332/29767202Y2025D000000029

Poell, T., Nieborg, D., & van Dijck, J. (2019). Platformisation. *Internet Policy Review*, *8*(4), 1–13. https://doi.org/10.14763/2019.4.1425

Quan-Haase, A., & Ho, D. (2020). Online privacy concerns and privacy protection strategies among older adults in East York, Canada. *Journal of the Association for Information Science and Technology*, *71*(9), 1089–1102. https://doi.org/10.1002/asi.24364

Quinn, K., & Epstein, D. (2023). Dimensionalizing privacy to advance the study of digital disempowerment. *Big Data & Society*, *10*(2). https://doi.org/10.1177/20539517231221739

Raab, C. D., Jones, R., & Székely, I. (2015). Surveillance and resilience in theory and practice. *Media and Communication*, *3*(2), 21–41. https://doi.org/10.17645/mac.v3i2.220

Rosenberg, D., Marciano, A., Suárez-Gonzalo, S., Ivan, L., & Fernández-Ardèvol, M. (2026). 'Don't look up!' Older adults' views on digital state surveillance: A cross-sectional multi-country study. *Journal of Global Ageing*. Advance online publication. https://doi.org/10.1332/29767202Y2025D000000045

Segijn, C. M., Opree, S. J., & van Ooijen, I. (2022). The validation of the perceived surveillance scale. *Cyberpsychology*, *16*(3), Article 9. https://doi.org/10.5817/CP2022-3-9

Serhan, Y. (2023, January 20). Why 'polycrisis' was the buzzword of day 1 in Davos. *Time*. https://time.com/6247799/polycrisis-in-davos-wef-2023

Snowden, E. J. (2019). *Permanent record*. Metropolitan Books.

Thompson, N., McGill, T., Bunn, A., & Alexander, R. (2020). Cultural factors and the role of privacy concerns in acceptance of government surveillance. *Journal of the Association for Information Science and Technology*, *71(9)*, 1129–1142. https://doi.org/10.1002/asi.24372

Tooze, A. (2022, October 20). Welcome to the world of the polycrisis. *Financial Times*. https://www.ft.com/content/498398e7-11b1-494b-9cd3-6d669dc3de33

van Dijck, J., Poell, T., & de Waal, M. (2018). *The platform society*. Oxford University Press. https://doi.org/10.1093/oso/9780190889760.001.0001

World Economic Forum. (2023). *The global risks report 2023 18th edition*. https://www.weforum.org/publications/global-risks-report-2023

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.

About the Authors

Sara Suárez-Gonzalo is associate professor of information and communication sciences (CNSC research group, UOC-TRÀNSIC Center) at Universitat Oberta de Catalunya. She critically examines the sociopolitical implications of digital platforms and data-driven technologies through the lens of political theory and the political economy of communication.

Joel Peiruza-Parga is a PhD student in political science and a member of the Communication Networks and Social Change research group (CNSC, UOC-TRÀNSIC Center) at Universitat Oberta de Catalunya. His research explores political participation and representation in the context of digital citizen engagement.

Mireia Fernández-Ardèvol is professor of digital communication and excellence academy professor (AGAUR) at the Universitat Oberta de Catalunya (Faculty of Information and Communication Sciences; CNSC Research Group, UOC-TRÀNSIC Center). Her research focuses on the intersection of ageing and communication studies, a field she has helped shape and consolidate.