AI & SOCIETY
https://doi.org/10.1007/s00146-021-01331-9

OPEN FORUM

Surveillance, security, and AI as technological acceptance

Yong Jin Park[1] · **S. Mo Jones-Jang**[2]

Received: 24 November 2021 / Accepted: 1 December 2021

Abstract
Public consumption of artificial intelligence (AI) technologies has been rarely investigated from the perspective of data surveillance and security. We show that the technology acceptance model, when properly modified with security and surveillance fears about AI, builds an insight on how individuals begin to use, accept, or evaluate AI and its automated decisions. We conducted two studies, and found positive roles of perceived ease of use (PEOU) and perceived usefulness (PU). AI security concern, however, negatively affected PEOU and PU, resulting in less acceptance of AI—(1) use, (2) preference, and (3) participation. AI surveillance concern also had negative effects on the credibility of AI and its recommendations. We integrated extant literature on socio-demographic differences, providing an insight on how AI acceptance is based on one's rationality regarding (1) technological risks (security/surveillance) and (2) benefits (PEOU/PU) as well as other contextual factors of socio-demographics.

Keywords AI · Surveillance · Data security · Algorithm

1 Introduction

With a shift to artificial intelligence (AI), popular sentiment has often been enthusiastic about the affordances of AI technologies and social dynamics in newly emerging forms of digital participation. Popular commentaries have expressed the great excitement, wonder about AI and its human-like functionality, as well as some of data-related concerns arising from automated decision-makings (Horvitz 2017; Złotowski et al. 2017). Still, little empirical evidence has been accumulated as to how people decide to adopt, use AI technologies, and find AI-based decisions credible—especially taking into consideration public worries about data surveillance or security (Milano et al. 2020). In other words, we do not know much about how individuals with their concern about personal data come to accept or reject AI-based platforms, tools, and applications that automate digital participation. Consequently, the precise mechanisms by which users take advantage of the plethora of social, economic, and political opportunities enabled by AI, and translate them into greater affordances at the end point of consumption is largely unexplored yet.

This study attempts a careful investigation of the relationship between salient features of cognitive process and the acceptance of AI, as indicated by (1) the likelihood of using AI and (2) the evaluation of AI-based recommendations. We modify the technological acceptance model, which promotes the two constructs of perceived ease of use (PEOU) and perceived usefulness (PU) (Davis et al. 1989; Venkatesh et al. 2003), in the context of AI—defined as algorithmic use of computer-programmed machines to perform tasks that traditionally require human intelligence (Nath and Sahu 2020; Shin 2021a; Shin, 2021a, b). We highlight contextual factors of personal data security and surveillance, and how these concerns are taken into account to shape one's decisions to accept AI. We further examine whether the function of these cognitive constructs depend on socio-demographic differences (Baum 2020; Dutton et al. 1987).

Collectively, using both experimental (Study 1) and survey designs (Study 2), this study contributes to existing literature in the following ways. First, we newly apply the technological acceptance model (TAM) to the use of AI in various contexts, expanding its theoretical plausibility. Second, we broaden the notion of technological acceptance, calling for context-specific models—specially, concerning

✉ Yong Jin Park
yongjinp@hotmail.com

[1] Howard University, 525 Bryant St NW, Washington, DC 20059, USA

[2] Boston College, 640 Commonwealth Avenue, Boston, MA 02215, USA

Published online: 19 January 2022

data privacy and surveillance. Third, the TAM, with its emphasis on cognitive rationality, is adjusted to explain socio-demographic variations as important to individual decisions on technological acceptance. Finally, practical implications are drawn with regard to how individual perceptions eventually take shape to put the affordances of AI-based technologies into practice.

2 TAM as a conceptual departure in cognitive heuristics

The TAM is a parsimonious theoretical framework that predicts and explains individual acceptance of a technology (Davis 1989). It is an individual-level account that highlights the cognitive power of rational calculation in making technology-related decisions. Early development of the TAM largely concerned the implementation of information systems in organizational settings (Venkatesh et al. 2003). Subsequent applications were made in an attempt to understand individual cognition when people decide to buy, adopt, or consume new technology products, such as personal computer, software applications, online communities, and Internet (Shin 2009, 2021a, b). The TAM's fundamental premise is built upon the idea that a rational sequence of decisions, which can be readily seen at the organizational level, is also expected at the individual level, as a person weighs whether to adopt, use, and accept a new technology, such as AI, and its decisions.

We are primarily interested in the TAM's two heuristic determinants: (1) PU, defined as the degree to which a user perceives the usefulness of technology in accomplishing her personal goals, thus resulting in technological acceptance and (2) PEOU, defined as the degree to which a user perceives the easiness of technology, i.e. the extent to which its uses are perceived as free of physical and mental efforts. Despite numerous variations, these two constructs remain the TAM's fundamental building blocks. In essence, the TAM is a variant on the theory of reasoned action (Fishbein and Ajzen 1975), as it posits motivational calculation as the determinant of a specific behavior. Broadly speaking, the underpinnings of the TAM imply a snap cognitive judgement, as rational people are capable of estimating the potential gains aligned with accepting a new technology. Here we propose that the TAM, when applied to AI, should be supplemented with two considerations: (1) data security and (2) surveillance concerns.

One way to think about this is that perceptional heuristics of the TAM are aided by other rational cues. Data security has become a significant issue, as industry experts (Vassakis et al. 2018) worry that vastly connected big-data applications and smart devices are vulnerable to potential attack by a malicious adversary. Hackers can hijack and command AI-based machine learning system by stealing the identities of controllers. The authenticity of AI recommendations can also be questionable, given the possibility that third-party actors possibly take over to tamper AI-run systems. Data surveillance, meanwhile, has considerably increased in recent years. Despite the incredible convenience of AI built into the iPhone X, for instance, its technologies also enable numerous mobile platforms or companies to track a user's precise movements. It has been reported that AI home devices, such as Alexa or/and Google Home, often collect voice command data and send them to central servers capable of processing and retaining personal information with no explicit consent (Park 2021c; Stegner 2018).

In a broader sense, these suggest the possibility that people's risk judgement, in deciding whether to accept AI, can work against perceived benefits of PU and PEOU. That is, data surveillance and security may pose threats to users, eliciting a different set of rational responses. This should not be surprising, given that new technologies at their inception have been often viewed as a threat to human autonomy and that such threats are always part of people's reaction to new technologies (Dutton et al. 1987; Janssen et al. 2019; Milano et al. 2020; Nath and Sahu 2020). On one hand, one can perceive benefits as AI and its automated decisions may be patently useful and easy to use. On the other hand, people see AI as the risk of losing control of their lives due to security breach or unwanted surveillance. Thus, the acceptance of AI as a new technology might be a function of heuristics interlaced with both positive and negative assessments, in lieu of a simple one-directional perception (Sundar 2020; Złotowski et al. 2017).

One caveat in fully understanding the applicability of TAM is that cognitive function is unlikely to be simply the product of individual mind. Several possibilities exist. First, individuals do not make every decision by themselves, but they pick up contextual clues from surrounding environments. Second, social groups influence individual perceptions, and their norms may not be shared by members outside social groups. Third, motivation to adopt a technology is not immune from external socio-demographic factors. Poverty, for instance, can limit one's ability to seek new opportunities and appreciate related affordances, being in a position not to afford additional steps and new products. It may be perfectly rational, depending on one's social status, for the individual to accept—or not to accept—a new technology. Scholars have been aware of these factors when applying the TAM. Venkatesh et al. (2003) and Shin (2009) proposed the unified theory of acceptance and use of technology in an attempt to integrate external elements not included in the original TAM, and they measured the effect of social factors such as age on the intention to adopt technologies (Baum 2020; Joo and Sang 2013). Importantly, they adopted a social constructivist's perspective with an

emphasis on the socializing process by which people bring their own experiences to interpret, assess, or internalize the use of new technologies. This idea is similar to what Rogers (2010) described as technological diffusion, or how the processes in which related norms begin to be shared amongst members of a social system affect technological adoption. The social construction of new technologies (Fulk 1993), wherein social relations, status, and positions shape the development of shared perceptions among members of a collective unit, also resonates our point. At the end, we see the need to go beyond purely cognitive analyses of decision making, as the rational acceptance of a technology can be socially situated, producing different perceptions about the conflicting premises of benefits (PU and PEOU) and risks (data security and surveillance concerns) related to AI.

3 Study 1: Experiment

Study 1 focused on health-related AI. Thus, the acceptance that we examine in Study 1 pertains to the likelihood of participating in health-related use of AI-based digital devices. Security and surveillance are serious concerns in the realm of personal medical data.

Crawford and Schultz (2014) argued that health data in AI-based analytics are extremely vulnerable to potential misuse because information about one's medical status can be used for other purposes, such as decisions on employment, job status, or promotion. Moreover, any consumption data, such as purchases of books, clothing, food, or even online search traces, can be linked to a person's health records. Other scholars (Lupton 2012) have observed that constant streams of personal data generated by digital consumption help private companies to paint a detailed picture of individuals' health status. Even as early as the year 2000, 85% of internet users who were in poor health condition worried about the privacy of medical data and about sharing their information online (Grimes-Gruczka et al. 2000). Scholars (e.g. Acquisti et al. 2015) have paid great attention to surveillance-related perceptions and how they might alter user behavior, such as information disclosure, in the contexts of e-commerce, online communities, and social media. Though these earlier studies were not directly related to AI, it is reasonable to predict that the onset of AI has exacerbated these concerns, influencing individual decisions about health-related use and adoption of AI.

We propose three-related hypotheses. The first hypothesis is that security and surveillance concerns will reduce the likelihood of health-related use of AI (H1a). The second hypothesis is that security and surveillance concerns will negatively influence PEOU and PU related to AI, which in turn will lead to a low likelihood of health-related use of AI (H1b). The third hypothesis is that when concerned about surveillance and security, individuals with a higher level of education will be less likely to perceive PEOU and PU and thus, less likely to accept AI use (H1c). Whereas H1a posits a direct effect of negative technology-related perceptions (security and surveillance) on the acceptance of AI use, H1b proposes an indirect relationship via PEOU and PU. H1c modifies the direct and indirect relationships by suggesting that they will vary depending on one's level of education, holding constant other socio-demographic factors. We have empirical bases to support these predictions. First, there is evidence that a high level of surveillance concern is significantly related to reluctance to use health-related digital platforms. Prior studies (Giovanis et al. 2012; Park and Shin 2020) have also indicated that perceptions as to whether personal data can be safe in an online system, such as electronic banking, affect people's willingness to adopt the system. The negative relationship between security concerns and each of PEOU and PU can be inferred, since the perception of adequate security has been found to be related to positive consumer attitudes toward electronic banking (Jahangir and Begum 2008).

In our investigation of how socio-demographics might affect people's perceptions of a new technology, we are particularly interested in the interactive effects of education. Studies have consistently shown a relationship between education and privacy-related perceptions, with more highly educated persons exhibiting greater awareness of data surveillance and security issues (Baruh et al. 2017). Generally, people with more education tend to be earlier adopters of new technologies (Rogers 2010). Although this pattern does not necessarily apply to value and concerns, focusing instead on the adoption of physical technologies (i.e. hardware), it is plausible to reason that those with a higher level of education can also become earlier adopters at the level of value, concerns, and new technology-related threats (i.e. software). Because our immediate focus is on health data, we expect that people with more education when they are alarmed will be even more alert about data security and surveillance, potentially nudging them to reform their perceptions about health-related use of AI and its benefits.

3.1 Methods

A national sample of adults ($n = 246$) participated in the study administered by Dynata using Qualtrics online platform in February 2019. We opted to use demographically diverse participants because we were interested in the functions of socio-demographic backgrounds as well as individual perceptions about AI. The sample consisted of 134 males (54.5%) and 112 females (45.5%). The mean age was 48.03 (aged 19 to 85, $SD = 16.06$), and the level of education, on a scale of 1 (less than high school) to 5 (graduate degree), was $M = 3.32$, SD = 1.08. Income among the participants was

$M = 3.73$, median = 4, SD = 1.08, measured on a scale of 1 (less than $20,000) to 8 ($200,000 or more).

Participants were randomly assigned to one of the three conditions: (1) security, (2) surveillance, and (3) control. Those in experimental groups 1 and 2 (data concern of security and surveillance) were told information that pertains to AI-related data security and surveillance, respectively. The information told in experiment groups 1 and 2 was to manipulate participants' sense of personal data risk so that they could perceive a higher level of concern or risk in their future use of AI—relative to the baseline control group in which no such information was provided. The treatment of information in each group was equivalent, except for the data risk statement on either security or surveillance, which was randomly presented to prime the concern of participants.

A manipulation check was conducted to ensure the effectiveness of the manipulation by asking participants about their levels of security and surveillance concerns (Min. = 1, Max. = 10; $M = 8.79$, SD = 1.37). A one-way ANOVA determined that there was a significant difference between the experimental (security-surveillance) and the control group, $F\ (2, 240) = 5.88$, $p < 0.01$. A follow-up Fisher's LSD test revealed that participants in the control group ($M = 8.39$, SD = 1.74) rated their concerns significantly lower than those in either the security ($M = 9.11$, SD = 1.07, $D = 0.71$, $p < 0.01$) or the surveillance ($M = 8.86$, SD = 1.12, $D = 0.47$, $p < 0.05$) conditions.

3.2 Measures

The dependent variables of our interest were: (1) the use of an AI device for health purposes, (2) participation in daily health monitoring activities by AI, and (3) preference for an AI-based medical diagnosis over a non-AI human doctor. For each of these three, a statement in a fully labeled 5-point scale (1 = extremely unlikely; 5 = extremely likely) asked participants to estimate their likelihood of accepting AI. Reliability of these items was high with Cronbach's α value of 0.85, and they were added to create a summary measure that captures the three dimensions of AI acceptance—use, participation, and preference (Min. = 3, Max. = 15; $M = 8.26$, SD = 3.49).

Four items of socio-demographics (education, age, income, and gender) were used as control variables. We also controlled for medical condition because those with chronic health issues are likely to need additional assistance, thus possibly resulting in a more acceptance of AI. Those who reported having one or more of the following conditions (diabetes, high blood, heart attack/condition, lung disease, arthritis, depression–anxiety or any type of cancer) was coded as 1, whereas those who reported having none of these problems were coded as 0 ($M = 0.21$, SD = 0.41).

3.3 Results

To test H1a which predicted a negative effect of security and surveillance concerns, we first ran a one-way ANOVA with the experimental (security-surveillance) condition as the independent variable (coded as 1) and the acceptance of AI as the dependent variable. We found no significant difference between the experimental and control groups. All three groups were also compared with regard to their level of AI acceptance. Still, the result of the ANOVA revealed no significant difference across the three groups ($M = 8.60$, SD = 3.49, security; $M = 7.72$, SD = 3.40, surveillance; $M = 8.48$, SD = 3.54, control), indicating no direct effect of data surveillance and security concerns on the acceptance of health-related use of AI.

To address H1b, we run OLS regression analyses with PEOU and PU as the dependent variables. Then, we tested PROCESS model 4 for the indirect effect (Hayes 2012), with PEOU and PU as the mediators and the experimental (security-surveillance) condition as the independent variable as in the model used to test H1a. First, OLS regressions showed significant negative relationships between the independent variable (security-surveillance) and PEOU ($\beta = -0.12$, $p = 0.05$) and PU ($\beta = -0.13$, $p < 0.05$), with those effect sizes relatively robust. As shown in Table 1, we also found

Table 1 Indirect effects of data security and surveillance concerns

IV	Indirect effect	Coefficients	SE	Bootstrap 95% CI	
				Lower	Upper
Security-surveillance (combined)	→ PEOU → AI acceptance	− 0.43	0.22	− 0.912	− 0.017
	PU	− 0.55	0.26	− 1.111	− 0.075
Security	→ PEOU → AI acceptance	− 0.03	0.23	− 0.501	0.419
	PU	− 0.17	0.26	− 0.727	0.322
Surveillance	→ PEOU → AI acceptance	− 0.41	0.24	− 0.929	0.043
	PU	− 0.40	0.25	− 0.915	0.082

Bootstrap resampling = 5000

CI confidence interval

significant indirect effects of the IV (security-surveillance PEOU and PU AI acceptance), with the estimates of − 0.43 (0.22) [− 0.916 to − 0.017] and − 0.55 (0.26) [− 1.095 to − 0.071] (CI entirely above zero). There was no indirect effect when we looked at the experimental condition of security and surveillance, separately.

To test H1c, PROCESS model 7 was used to detect the interactive effect of education, which was hypothesized to moderate the effects of the independent variable (surveillance-security) on PEOU and PU (conditional indirect effect on the dependent variable). In addition, we split the participants into high and low education groups (low < median = 3) and repeated the tests above. We found no supportive evidence. Instead, we found direct effects of education (− 0.62 (0.19) [− 1.008 to − 0.245], − 0.44 (0.18) [− 0.814 to − 0.085]) in the models that accounted for PEOU and PU separately. With respect to other socio-demographic factors, the effect of age was significant with the estimate of − 0.04 (0.01) [− 0.073 to − 0.025] and − 0.04 (0.01) [− 0.065 to − 0.019] as older people were less likely to accept health-related AI. No other socio-demographic factors were statistically significant, nor was the presence of chronic medical conditions.

4 Summary of findings and discussion

To summarize, there was no support for H1c, but we found the strong support for indirect effects (H1b) in the absence of direct effect as predicted by H1a. The results of Study 1 presented an opportunity to explore the TAM and its heuristic constructs applied to the health-related use of AI, preference over a human doctor, and participation in AI-based medical monitoring.

The finding that individuals—when they perceived the benefit of AI as PEOU and PU were likely to accept AI—supports the findings of prior studies that demonstrated significant links between PEOU, PU, and the acceptance of new technologies and their applications. Nevertheless, the indirect effects observed suggest strongly that the effects of positive TAM assessments, such as PEOU and PU, can be reversed with increased concern about security and surveillance, as individuals become worried about data threats related to AI technologies. Coupled with the absence of direct effects of security and surveillance concerns, this demonstrates that in the AI-related medical context, the cognitive function preceding AI acceptance (or its rejection) is tightly tied to the perceived value of utility—namely, how useful or easy to use an AI might be. In other words, the function of data-related concern may not be direct, but only indirect through one's rational judgement about AI utility values. This makes sense, given that the medical use of AI may be on a basis of more tangible needs than other digital consumption (namely, as opposed to mindlessly browsing through automatically suggested movie lists). Positive perceptions related to the utility of AI might be readily altered by personal data-related concern.

Importantly, we found no difference between security and surveillance conditions as to their respective effect. This finding suggests that neither area of concern is significantly more threatening than the other, at least with regard to health-related AI. Rather, the perceived benefit of AI in health contexts might be less prone to the type of a specific data concern, and this result is in line with the above reasoning which notes that one's decision about the medical use of AI will depend more on the perceived utility value (Winkelman et al. 2005). The finding of no conditional indirect effect via education level corroborates this interpretation, in that there may exist no or little variation by socio-demographic condition, such as one's extent of formal education, with regard to the heuristic function of PEOU or PU assessing AI utility.

Significant direct effects of covariates are noteworthy, nonetheless, as those with higher education displayed less inclination to accept AI (use, preference, and participation) for health purposes. The finding that older participants were less likely than younger people to accept the medical use of AI is also intriguing, given that the need for medical attention is likely to increase with age. On a similar note, it was surprising that having a chronic medical condition did not matter in any of the models analyzed in Study 1, although we might uncover its significance with additional measures of AI application specifically related to a person's particular medical condition. In this context, we reason that advanced AI applications, such as robotic surgeons or AI doctors, may be still viewed as distant realities by those suffering from chronic medical conditions (see Topol 2019).

5 Study 2: Survey

Study 2 aimed to replicate Study 1, extending the proposed model beyond health-related uses of AI. Accordingly, we modified the AI acceptance in various contexts of shopping, banking, finance, health, law enforcement, insurance, and government service. Whereas the experimental setup in Study 1 aimed to observe effects of AI related perceptions by putting them at the forefront of people's attention, Study 2 by using a survey investigated inner workings of heuristic decision-making in everyday contexts. We conceptualized the acceptance of AI in three dimensions: (1) credibility, (2) authenticity, and (3) accuracy. Importantly, Study 2 does not concern AI-instigated activities as observed in Study 1. Instead, we take a more subtle approach to understanding AI use, as we consider that the technological features of AI will broaden its use to the extent to which people find automated

information, decisions, and recommendations made by AI to be credible (i.e. trustworthy), authentic (i.e. verifiable), and accurate (i.e. correct).

People's credibility judgement can be explained in terms of perceptional evaluation, which is particularly helpful for our purposes, given our study's emphasis on the role of heuristic perceptions in the acceptance of AI as a new technology (Araujo et al. 2020; Shin 2021a, b). We propose that in consuming information suggested by AI, people go through quick evaluations, falling back on accessible mental short cuts of (1) PEOU and PU assessments and (2) data security and surveillance concerns specific to AI. In this way, the acceptance of AI as a credible source of information is impacted by multiple layers of heuristic predictors. As discussed in Study 1, PEOU and PU should lead to a higher level of acceptance. Perceptions of security and surveillance concerns, however, will negatively influence both PEOU and PU levels, reducing the acceptance of AI and the credibility of its information. Decisions on whether to accepting AI as an accurate and authentic source of information (Hilligos and Rieh 2008; Pelau et al. 2021; Sang et al. 2020; Vassakis et al. 2018) will also be vulnerable to security and surveillance concerns because these raise questions about hacking or/and third-party snooping, i.e. whether information provided is verifiable and correct at all.

At the end, Study 2 focuses on how individuals come to appreciate, evaluate, and eventually accept information in its credibility and related dimensions, when the source of information is automated by AI. We modify the line of reasoning built in Study 1, predicting that high levels of security and surveillance concerns will be less likely to result in the acceptance—indicated by credibility, authenticity, and accuracy—of information, decisions, or recommendations by AI (H2a). As in Study 1, we also predict negative relationships between security or surveillance and PEOU or PU, which will in turn indirectly affect the acceptance of AI in the three dimensions described above (H2b). In assessing the influences of social environments, we propose potential moderations by age, income, and education (Rogers 2010). We expect more affluent subjects, older people, and those with higher education to be less likely to accept or more critically evaluate AI, when they are concerned about surveillance and security (H2c). We thus broaden our analysis of socio-demographic factors relative to Study 1, when we considered only education as a possible conditional factor in H1c.

5.1 Methods

The data for Study 2 were collected and potential U.S. respondents were recruited by Dynata online in January–February 2019 (the age of 18 and above), with an initial sample of 950. From this, we excluded any respondents who failed an attention-check question, leaving a sample of 753 for analysis. Descriptive statistics reported below show that the demographic characteristics in the final sample are close to figures reported in the U.S. 2015 American Community Survey (ACS). Females were 54.8% (ACS = 51.4%); median income was 4, $M = 3.77$, SD = 1.97, $50,000 to $74,999 (ACS = $53,889); average education level (the range of 1–5) was some college, with $M = 3.28$, SD = 1.08 (ACS = some college); and the mean age was 46.47 (SD = 15.43) (ACS = 45–54 years).

5.2 Measures

To assess the criterion variable of AI acceptance in (1) credibility, (2) authenticity, and (3) accuracy, we used six items. In each case, we asked the respondents to rate all three dimensions on a five-point scale ranging from 1 (not at all) to 5 (extremely). The items included (a) a bank that uses AI to determine the best banking products to offer a customer, (b) the use of AI to provide personalized purchase recommendations, (c) a doctor using AI for aid in making a better diagnosis or recommendation, (d) a judge using AI to help make a better legal decision, (e) an insurance company using AI to monitor and analyze the respondent's daily activities, and (f) the government using AI to provide personalized public services. The wording for each item was as follows: assuming you had access to AI system, product or services, we are interested in (1) how accurate, (2) how authentic, and (3) how credible you would consider each AI machine and its decisions.

A principal component analysis with un-rotated factor was performed on the six items in each dimension. Items in accuracy loaded on a single factor, explaining 68.90% of the variance (Cronbach's alpha of 0.91). All items in each of authenticity and credibility also loaded on a single factor, with 74.21% and 73.29% of variance explained (Cronbach's alpha of 0.93 and 0.92). Six items in each dimension of AI acceptance were summed to create a score (AI accuracy, $M = 15.51$, SD = 6.04; AI authenticity, $M = 14.99$, SD = 6.40; AI credibility, $M = 14.93$, SD = 6.35, in all ranged from 6 to 30).

The original TAM was interested in the effect of user intention on adoption and actual use of a new technology. We adopted this unitary measure to assess whether one's overall intention to use AI mediates the effects of other predictors, as in the original TAM (Venkatesh et al. 2003). We asked how much respondents actually intend to use AI when they have access to an AI-enhanced system, product, or service. They reported the intensity of their agreement on a five-point scale ranging from 1 (strongly disagree) to 5 (strongly agree) ($M = 2.89$, SD = 1.26). Intention to use was correlated with each AI acceptance

dimension (accuracy 0.63, authenticity 0.61, credibility 0.60; all r, $p < 0.001$), displaying antecedent functions of this construct.

As in Study 1, the independent variable of interest is the data concern of security and surveillance. We used eight items (four for each threat) and asked respondents to estimate their concern about the likelihood that using AI would result in heightened risk of a data security or surveillance. A 5-point scale ranging from 1 (extremely unlikely) to 5 (extremely likely) was used. We added all items on each threat to create two overall scores: security ($M = 16.44$, SD = 3.29, Min. = 4, Max. = 20, Cronbach's alpha = 0.86) and surveillance ($M = 16.87$, SD = 3.38, Min. = 4, Max. = 20, Cronbach's alpha = 0.90).

These two TAM variables were measured using a total of six items. On a 5-point scale, respondents were asked to rate the degree to which they agreed with each statement assessing the potential of AI in its ease of use and usefulness (1 = strongly disagree to 5 = strongly agree). All items were added to create a score in each of PEOU and PU ($M = 9.39$, $SD = 2.70$, Min. = 3, Max. = 15, PEOU; $M = 9.70$, SD = 3.06, Min. = 3, Max. = 15, PU). Cronbach's alpha value was 0.74 (PEOU) and 0.87 (PU). All item wordings and descriptive statistics for PEOU, PU, and security and surveillance concerns can be found in Table 2.

Age, gender, education and income were controlled for in all analyses in Study 2. To account for the possibility that owning any AI device may reflect a general acceptance of information generated by AI, we controlled for ownership of AI home-devices such as Google Home or Amazon Alex, with 28.8% of the respondents owning at least one device.

5.3 Results

Study 2 expands our testing of the proposed causal links among different predictors. PROCESS model 6, which employs OLS path analyses with three mediators, was used for H2a and H2b, and Fig. 1 details the paths of direct and indirect effects. To test H2c, the moderators of education, income, and age were used in PROCESS model 7 in which the effects of the independent variables (security and surveillance concerns) via each mediator (PEOU, PU, and intention to use) were moderated—namely, conditional indirect effects. In support of H2a, we found significant direct effects of both security and surveillance concerns in all dimensions of AI acceptance (for security, accuracy, − 0.13 (0.04) [− 0.231 to − 0.039], authenticity, − 0.17 (0.05) [− 0.277 to − 0.069], credibility, − 0.17 (0.05) [− 0.280 to − 0.070]; for surveillance, accuracy, − 0.15 (0.04) [− 0.248 to − 0.058], authenticity, − 0.19 (0.05) [− 0.296 to − 0.090], credibility, − 0.16 (0.05) [− 0.297 to − 0.059], with all 95% CI). The support for H2b where indirect effects were expected, however, was mixed. For security concern, we found indirect effects via three mediators (PEOU PU intention to use) in each of three dimensions (accuracy, − 0.01 (0.00) [− 0.033 to − 0.003], authenticity, − 0.01 (0.00) [− 0.034 to − 0.004], credibility, − 0.01 (0.00) [− 0.032 to − 0.004], with all 95% CI). For surveillance concern, no support was found in any of the dimension, indicating that the precise paths of cognitive response differ by the type of data concern.

Table 3 shows the results of OLS regression employed in PROCESS model 6, which allows us to detect precise effects of predictors in each path. Note differences between security and surveillance concerns in influencing each mediator. Security concern negatively affected PEOU

Table 2 Descriptive statistics of PEOU, PU, security, and surveillance concerns

Predictors	Individual measures	*M*	SD
Security	Criminal use of AI technologies	3.93	1.04
$M = 16.44$, SD = 3.29	Malfunctions or/and bugs	4.14	0.93
Min. 4; Max. 20	Cyber-attacks or hacking	4.21	0.92
	Less security of personal data	4.15	1.00
Surveillance	Companies and/or the government having greater access to info about people	4.19	0.99
$M = 16.87$, SD = 3.38	An increase in the monitoring of what people do	4.25	0.94
Min. 4; Max. 20	An increase in the data collection of people's digital habits and activities	4.26	0.94
	Little control over the information collected about people in their daily life	4.16	0.96
PEOU perceived easiness	Interacting with AI will not require a lot of my mental effort	3.10	1.12
$M = 9.39$, SD = 2.70	I will find AI to be easy to use	3.25	1.09
Min. 3; Max. 15	I will find AI flexible to interact with	3.03	1.10
PU perceived usefulness	Using AI will enable me to accomplish tasks or what I want more quickly	3.35	1.07
$M = 9.70$, SD = 3.06	Using AI will enhance my effectiveness	3.27	1.11
Min. 3; Max. 15	I will find AI useful in my work	3.08	1.22

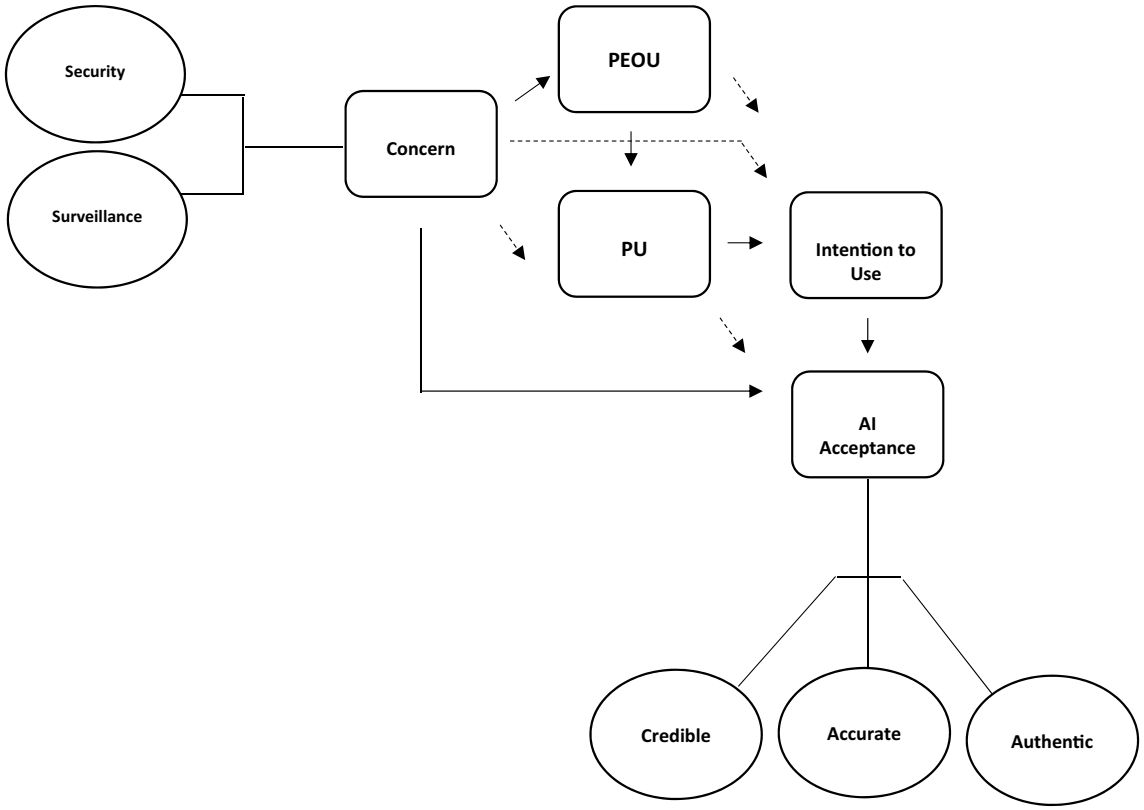

Fig. 1 Conceptual model of AI acceptance. Hypothesized relationships are indicated by solid arrows, with dotted arrows for additional statistical analyses accounted to estimate every path in regression analyses

Table 3 Regression analyses for direct and indirect relationships

	PEOU	PU	Intention to use	AI Accuracy	AI authenticity	AI credibility
IV: security	− 0.08 (0.02) **	− 0.01 (0.02)	− 0.01 (0.00)	− 0.13 (0.04) **	− 0.17 (0.05) **	− 0.17 (0.05) **
IV: surveillance	− 0.01 (0.02)	− 0.03 (0.02)	− 0.02 (0.00) **	− 0.15 (0.04) **	− 0.19 (0.05) ***	− 0.16 (0.05) **
M1: PEOU	–	0.61 (0.03) ***	0.07 (0.01) ***	0.18 (0.07) *	0.16 (0.08) *	0.11 (0.08)
M2: PU		–	0.22 (0.01) ***	0.58 (0.07) **	0.61 (0.08) ***	0.65 (0.08) ***
M3: intention			–	1.58 (0.18) ***	1.67 (0.20) ***	1.57 (0.20) ***
Age	− 0.02 (0.00) **	0.00 (0.00)	− 0.00 (0.00)	− 0.02 (0.01) **	− 0.01 (0.01)	− 0.02 (0.01)
Female	− 0.21 (0.19)	0.08 (0.18)	− 0.12 (0.06)	− 0.58 (0.33)	− 0.55 (0.36)	− 0.71 (0.36)
Income	− 0.19 (0.05) ***	− 0.04 (0.05)	− 0.02 (0.01)	0.10 (0.09)	0.01 (0.10)	0.11 (0.10)
Education	0.13 (0.09)	− 0.00 (0.09)	0.00 (0.03)	0.16 (0.16)	0.18 (0.18)	0.18 (0.18)
AI device owned	1.48 (0.22) ***	1.28 (0.21) ***	0.44 (0.08) ***	0.69 (0.41)	0.84 (0.44)	0.61 (0.45)
Constant	11.90 (0.73)	3.73 (0.80)	0.52 (0.29)	6.89 (1.48)	6.11 (1.61)	6.65 (1.62)
Adjusted R	0.12	0.39	0.53	0.48	0.46	0.44
F statistic	17.03 ***	68.54 ***	108.66 ***	79.01 ***	70.53 ***	66.48 ***

Unstandardized coefficients (B) reported. Standard errors in parentheses

*$p<0.05$, **$p<0.01$, ***$p<0.001$, M mediator. F-statistic, constant, and effects of covariates reported pertain to the model with IV of security concern. Separate analyses were run for surveillance concern

[$B=-0.08$ (0.02), $p<0.01$], which affected PU [$B=0.61$ (0.03), $p<0.001$] affecting intention to use [$B=0.22$ (0.01), $p<0.001$] that was significantly linked to AI credibility [$B=1.57$ (0.20), $p<0.001$], authenticity [$B=1.67$ (0.20), $p<0.001$], and accuracy [$B=1.58$ (0.18), $p<0.001$]. Surveillance concern, on the other hand, displayed no effect on

either of PEOU and PU, but directly and negatively affecting intention to use [$B = -0.02$ (0.00), $p < 0.01$].

Effects of covariates are important to address as we are interested in overall socialization, along with hypothesized conditional indirect effects (with income, education, and age, H2c). As shown in Table 3, age and income displayed significant influences on PEOU, with older people and those with higher income less likely to perceive the easiness of AI [$B = -0.02$ (0.00), $p < 0.01$; $B = -0.19$ (0.05), $p < 0.001$]. We also found the effect of age on AI accuracy as the older people were less likely to accept AI as accurate [$B = -0.02$ (0.01), $p < 0.01$]. Interestingly, accounting for all variables in regression models, the significant effect of AI device ownership (on PEOU, PU, and intention to use) entirely disappeared for all three dimensions, indicating that owning AI devices alone does not lead to the acceptance of AI-generated recommendation. Finally, we found conditional indirect effects of income and education on AI acceptance via PU, but the effect was significant only for surveillance concern, providing a limited support for H2c.

We plot the pattern in Fig. 2, which shows the negative conditional indirect effects of surveillance concern via PU on all dimensions of AI acceptance (education: accuracy, − 0.05 (0.01) [− 0.093 to − 0.015], authenticity, − 0.05 (0.02) [− 0.099 to − 0.017], credibility, − 0.05 (0.02) [− 0.103 to − 0.017]; income: accuracy, − 0.02 (0.01) [− 0.052 to − 0.007], authenticity, − 0.03 (0.01) [− 0.054 to − 0.008], credibility, − 0.03 (0.01) [− 0.058 to − 0.009], with all 95% CI).[3] The arrow in each figure indicates the precise point of each moderator at which the indirect effect becomes significant. For education, no indirect effect was found for respondents with "some college" or less. Similarly, with regard to income, we found the indirect effect only among those with annual income above $100,000. That is to say, indirect effects of surveillance concern via PU on AI acceptance varied depending upon one's income and educational level.

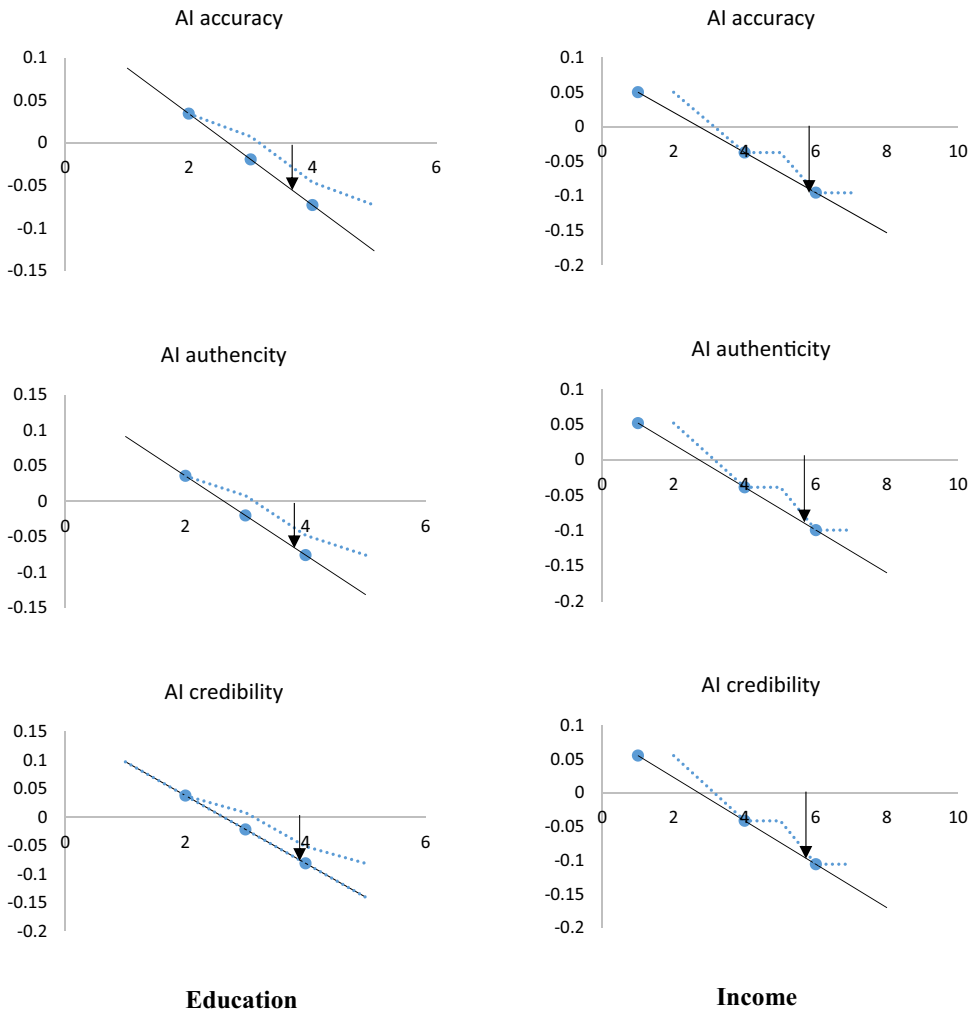

Fig. 2 Conditional interaction between surveillance and PU. *Y* = estimates of PROCESS index of conditional indirect effect of security and surveillance concerns, with a solid line for the trend and a dotted line for moving average (average of a series of coefficients, namely at the level between 2 and 3, and then, between 3 and 4 of moderator). Arrows indicate the precise levels of moderators at which estimates become significant

6 Summary of findings and discussion

The findings of Study 2, based on a survey, echoed the premise of Study 1 that the affordance of AI is contingent upon individual perceptions that are heuristically available in terms of PU and PEOU as well as security and surveillance concerns. But there were important differences as Study 2 extended the scope of AI acceptance into other areas of AI applications.

First, we highlight mixed support for H2b, as indirect effects of security concern were present in all three dimensions of AI, whereas we found no support for surveillance concern. This is interesting, because it shows that as in Study 1, the concern for data security was tightly linked to the perceived utility value of AI (i.e. to PEOU and PU). In other words, when security-related concerns cause people to turn away from AI, it seems to be because such issues as hacking, data breaches, or criminal use of confidential data prompt them to reassess AI's practical usefulness. Study 2's findings indicate that this heuristic judgement happens not only in an evaluation of potential AI uses, but also in terms of assessing the automated recommendations with regard to their credibility, authenticity, and accuracy. Second, although surveillance concern had no indirect effect as predicted, we did find direct effects of both security and surveillance concerns. This means that unlike the effect of data security, surveillance concern might affect the acceptance of automated information in a shorter cognitive route, not interlinked with heuristic evaluation of PEOU and PU. Also unlike Study 1 in which we found no difference between security and surveillance concerns, Study 2 shows that differences do arise when it comes to accepting the acceptance of AI-based information. In other words, controlling for socio-demographics, surveillance concern can be explained by the heuristic bypassing of PEOU and PU in inhibiting all aspects of AI credibility, accuracy, and authenticity.

Another interesting discovery of Study 2 is the power of PEOU and PU in explaining AI acceptance. In contrast, owning an AI personal device had no effect on any of the three dimensions, indicating that simply having access to AI devices does not necessarily lead to a fuller openness to AI-based suggestions. The finding of limited effects of socio-demographic factors, except for age (with older people being less likely to accept the accuracy of AI), also indicates that the heuristic powers of PEOU and PU are more robust than any other factors in the models. However, PEOU and PU exhibited variance along socio-demographic lines, as those with higher income and older people were less likely to view AI as useful or easy to use. To the extent that the significance of PEOU and PU remains subject to specific socio-demographic conditions, we can say that the formation of heuristic antecedents to AI acceptance is not solely a product of individual cognition, but also of socialization. In this regard, it is particularly critical to address the conditional indirect effect of surveillance concerns via PU on income and education, which suggests that when concerns about surveillance are prominent, those with an education level higher than "some college" and a household income of more than $100,000 are far less likely to consider AI as accurate, authentic, or credible, as they come to perceive AI has having little usefulness. The finding is fascinating in that it indicates that when surveillance concerns have a negative indirect effect via PU, the effect is socially contingent. Moreover, these results were significant on all dimensions of AI (i.e. accuracy, authenticity, and credibility).

7 Theoretical and practical implications

The two studies presented above show that the TAM, when modified with the variables of surveillance and security that are contextual of AI, can demonstrate delicately interlinked cognitive functions of AI acceptance. In Study 1, in which participants in the experimental condition were informed of data security and surveillance threats of AI, we observed that those manipulations created differences, indirectly through the heuristic predictors of PEOU and PU, in the acceptance of health-related AI use. In Study 2, we replicated the findings with regard to the acceptance of AI-based decisions in the areas of law, government, shopping, insurance, finance, as well as health, and we found direct and indirect effects of data security concern through PEOU and PU. In both studies, we investigated the conditional indirect effects with socio-demographics and Study 2 found such supports via PU, as we propose to understand AI as the end-user acceptance of technological use (Study 1) as well as of its automated information, decisions, or/and recommendations (Study 2).

A major contribution of this study is the demonstration that AI technologies, related affordances, and threats can be understood from the rational perspective of end-user consumption. Our point of departure was that the TAM, in its heuristic predictors, explains the function of cognitive rationality related to AI, helping us to map interlaced steps with security and surveillance concerns (Acquisti et al. 2015), as their effects on individual decision making are also conditional upon socio-demographic backgrounds (Rogers 2010). The empirical findings in our two studies offer greater opportunities for integrating different perspectives on the social shaping of heuristic rationality and its effects, while adhering to the core premise of the TAM that individuals can be rational actors in deciding on potential benefits of their choices. After all, people resort to quick mental shortcuts

or heuristic cues of a threat-and-risk for split seconds, and their decisions are hardly immune from socialization. On this note, contrary to Study 2's findings, if we found no relationship between aspects of social privilege (i.e. having more education and greater income) and careful, deliberate acceptance of AI decisions, then there would be little to debate. But because one's social background conditions how one incorporates data surveillance concerns, which in turn impacts one's perceptions of AI's usefulness, we can expect that the social, economic, and political opportunities enabled by AI will be unevenly distributed.

The theoretical flexibility of the TAM continuously allows for modeling additional variables that are either external or complementary to the model's original constructs of PEOU and PU. In this way, future AI system designers can have better conceptual tools to understand how individual cognition will respond to the rapid transition to personalized, data-based AI platforms. For instance, if AI programmers want to optimize user adoption of or participation in the full affordance of AI, their effort to transform personal data inputs into informational outputs should be accompanied by endeavors to foster more favorable perceptions about how the system will handle data safely (Ananny and Crawford 2018; Milano et al. 2020). Missteps in imprinting heuristics in users' minds may result in outright rejection of AI's credibility (as shown by the results of Study 2), no matter how useful a particular digital platform can be.

We can summarize the import of our results as follows. First, our findings clarify the joint processing of technological risk (security and surveillance) and benefit (PEOU and PU) assessment in a succession of cognitive heuristics. In this context, the acceptance of AI, whether at the level of either hardware adoption or consumption of information, stems from sequential steps that are heuristically linked, directly and indirectly. The presence or absence of those links is key to predicting the extent to which an individual will accept (or critically reject) AI. Here the distinction between security and surveillance, often conflated in public discourse, is important. One might correctly note that security has more to do with illegal access to data, as opposed to surveillance involving monitoring, collecting, and retaining personal information. As seen in the lack of direct effect of surveillance concern on PEOU and PU in Study 2, people seem to see that the ease of AI and its functional usefulness have little to do with surveillance, but a lot more to do with data security in their evaluation of AI-based financial or legal consulting, for instance. Or it can be simply the case that surveillance invokes not a train of cognitive responses in succession, but fearsome heuristics resulting in outright rejection of automated recommendations.

What is open for further debate is whether individual assessments concerning AI will stay purely rational as premised in the TAM. Rationality does not necessarily mean better, wiser, or even more informed decisions. In the end, perfectly rational but uninformed decisions related to AI are entirely possible. Imagine a scenario in which a person does not care about surveillance, finds a certain AI suggestion useful, and thus accepts the entire parameters of AI; but in fact, the person's private data may continuously distort what is algorithmically recommended (Araujo et al. 2020; Shin 2021a). As seen in the significance of the heuristic predictors of the TAM across all AI acceptances in Study 1 and Study 2, no matter how incomplete or imperfect one's evaluations of AI might be, one will be likely to act upon her perceptions. This has important implications in that people for the lack of complete information and algorithmic transparency will be more likely to rely on readily accessible mental cues to guide their AI-related decision making (Park 2021a, b). The scope of future works thus needs to expand to fully specify other cognitive heuristics that instigate, encourage or prevent AI acceptance. Expectancy violation, for instance, may explain one's rejection of AI recommendation and its credibility, when a person sees her expectations about the anonymity of data being violated in automated lists of product options. Reputation heuristic is also a likely candidate, given that a big brand name like Google or Apple will provide its users with quick cues of convenience and usefulness, or even negative connotations of surveillance for that matter.

Scholars in their future works might find it fruitful to uncover precisely how these alternative perceptional heuristics create the likelihood of AI acceptance in conjunction with PEOU or PU. Such precision will help us understand AI consumption decisions elicited of multiple cognitive heuristics. In this context, social influence at the meso-level, when this is understood as following others' AI-related decision within an organization, might be a more precise measure than socio-demographics at a macro-level as in this study's analysis. The modifications will be important because psychological antecedents alone may not be sufficient to explain variations in decision making regarding new technologies. The resulting perspectives will provide insight on enduring roles of socialization that incubates individuals' perceptions as members of one's social groups are likely to exert immediate influence on positive or negative assessments with regard to AI technology.

Funding No funding was received to assist with the preparation of this manuscript.

Declarations

Conflict of interest The authors have no relevant financial or non-financial interests to disclose. There is no conflicting interest to disclose.

Data availability statement There is no data set associated with this work to be publicly available.

References

Acquisti A, Brandimarte L, Loewenstein G (2015) Privacy and human behavior in the age of information. Science 347:509–514. https://doi.org/10.1126/science.aaa1465

Ananny M, Crawford K (2018) Seeing without knowing: limitations of the transparency ideal and its application to algorithmic accountability. New Med Soc 20:973–989. https://doi.org/10.1177/1461444816676645

Araujo T, Helberger N, Kruikemeier S, De Vreese CH (2020) In AI we trust? Perceptions about automated decision-making by artificial intelligence. AI Soc 35(3):611–623. https://doi.org/10.1007/s00146-019-00931-w

Baruh L, Secinti E, Cemalcilar Z (2017) Online privacy concerns and privacy management: a meta-analytical review. J Commun 67:26–53. https://doi.org/10.1111/jcom.12276

Baum SD (2020) Social choice ethics in artificial intelligence. AI Soc 35(1):165–176. https://doi.org/10.1007/s00146-017-0760-1

Crawford K, Schultz J (2014) Big data and due process: toward a framework to redress predictive privacy harms. BC Law Rev 55:93

Davis FD (1989) Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Q. https://doi.org/10.2307/249008

Dutton WH, Rogers EM, Jun SH (1987) Diffusion and social impacts of personal computers. Commun Res 14:219–250. https://doi.org/10.1177/009365087014002005

Fishbein M, Ajzen I (1975) Intention and behavior: an introduction to theory and research. Addition-Wesley, Boston

Fulk J (1993) Social construction of communication technology. Acad Man J. https://doi.org/10.5465/256641

Giovanis AN, Binioris S, Polychronopoulos G (2012) An extension of TAM model with IDT and security/privacy risk in the adoption of internet banking services in Greece. Eur Med J Bus 7:24–53. https://doi.org/10.1108/14502191211225365

Grimes-Gruczka T, Gratzer C, Dialogue C (2000) Ethics: survey of consumer attitudes about health web sites. California HealthCare Foundation

Hayes AF (2012) PROCESS: a versatile computational tool for observed variable mediation, moderation, and conditional process modeling. http://www.afhayes.com/public/process2012.pdf. Accessed 26 June 2021

Hilligos B, Rieh SY (2008) Developing a unifying framework of credibility assessment: construct, heuristics, and interaction in context. Inf Proc Man 44:1467–1484. https://doi.org/10.1016/j.ipm.2007.10.001

Horvitz E (2017) AI, people, and society. Science 357:7. https://doi.org/10.1126/science.aao2466

Jahangir N, Begum N (2008) The role of perceived usefulness, perceived ease of use, security and privacy, and customer attitude to engender customer adaptation in the context of electronic banking. Afr J Bus Man 2:032–040

Janssen CP, Donker SF, Brumby DP, Kun AL (2019) History and future of human automation interaction. Int J Hum Commun Stud 131:99–107. https://doi.org/10.1016/j.ijhcs.2019.05.006

Joo J, Sang Y (2013) Exploring Koreans' smartphone usage: an integrated model of the technology acceptance model and uses and gratifications theory. Comput Human Behav 29:2512–2518. https://doi.org/10.1016/j.chb.2013.06.002

Lupton D (2012) M-health and health promotion: the digital cyborg and surveillance society. Soc Theory Health 10:229–244. https://doi.org/10.1057/sth.2012.6

Milano S, Taddeo M, Floridi L (2020) Recommender systems and their ethical challenges. AI Soc 35(4):957–967. https://doi.org/10.1371/journal.pcbi.1005399

Moon JW, Kim YG (2001) Extending the TAM for a world-wide-web context. Inf Manag 38:217–230. https://doi.org/10.1016/S0378-7206(00)00061-6

Nath R, Sahu V (2020) The problem of machine ethics in artificial intelligence. AI Soc 35(1):103–111. https://doi.org/10.1007/s00146-017-0768-6

Park YJ (2021a) The future of digital surveillance: why digital monitoring will never lose its appeal in a world of algorithm-driven AI. University of Michigan Press, Michigan

Park YJ (2021b) Personal data concern, behavioral puzzle and uncertainty in the age of digital surveillance. Telem Inform. https://doi.org/10.1016/j.tele.2021.101748

Park YJ (2021c) Structural logic of AI surveillance and its normalisation in the public sphere. Javnost Public 28(4):341–357. https://doi.org/10.1080/13183222.2021.1955323

Park, YJ (2021d) Why privacy matters to digital inequality. In: Handbook of Digital Inequality (Hargittai E). Edward Elgar Publishing.

Park YJ, Shin DD (2020) Contextualizing privacy on health-related use of information technology. Comput Hum Behav 105:106204. https://doi.org/10.1016/j.chb.2019.106204

Pelau C, Dabija DC, Ene I (2021) What makes an AI device human-like? The role of interaction quality, empathy and perceived psychological anthropomorphic characteristics in the acceptance of artificial intelligence in the service industry. Comput Hum Behav 122:106855. https://doi.org/10.1016/j.chb.2021.106855

Rogers EM (2010) Diffusion of innovations. Simon and Schuster, New York

Sang Y, Lee JY, Park S, Fisher C, Fuller G (2020) Signalling and expressive interaction: online news users' different modes of interaction on digital platforms. Dig J 8(4):467–485. https://doi.org/10.1080/21670811.2020.1743194

Shin D (2009) Understanding user acceptance of DMB in South Korea using the modified technology acceptance model. Int J Hum Comput Interact 25:173–198. https://doi.org/10.1080/10447310802629785

Shin D (2021a) How do people judge the credibility of algorithmic sources? AI Soc. https://doi.org/10.1007/s00146-021-01158-4

Shin D (2021b) The effects of explainability and causability on perception, trust, and acceptance: implications for explainable AI. Int J Hum Commun Stud 146:102551. https://doi.org/10.1016/j.ijhcs.2020.102551

Stegner B (2018) January 10. 7 Ways Alexa and Amazon echo pose a privacy risk. https://www.makeuseof.com/tag/alexa-amazon-echo-privacy-risk/. Accessed 26 June 2021

Sundar S (2020) Rise of machine agency: a framework for studying the psychology of human–AI interaction. J Comput Med Commun. https://doi.org/10.1093/jcmc/zmz026

Topol EJ (2019) High-performance medicine: the convergence of human and artificial intelligence. Nat Med 25:44. https://doi.org/10.1038/s41591-018-0300-7

Vassakis K, Petrakis E, Kopanakis I, Skourletopoulos G, Mastorakis G, Mavromoustakis C, Dobre C, Pallis E (2018) Big data analytics: applications, prospects and challenges. In: Mobile big data. Springer, Cham, pp 3–20

Venkatesh V, Morris MG, Davis GB, Davis FD (2003) User acceptance of information technology: toward a unified view. MIS Q. https://doi.org/10.2307/30036540

Winkelman WJ, Leonard KJ, Rossos PG (2005) Patient-perceived usefulness of online electronic medical records: employing grounded theory in the development of information and communication technologies for use by patients living with chronic illness. J Am Med Inf Assoc 12:306–314. https://doi.org/10.1197/jamia.M1712

Złotowski J, Yogeeswaran K, Bartneck C (2017) Can we control it? Autonomous robots threaten human identity, uniqueness, safety, and resources. Int J Hum Comput Stud 100:48–54. https://doi.org/10.1016/j.ijhcs.2016.12.008