International Journal of Urban Planning and Smart Cities
Volume 3 • Issue 1

Privacy Behavior in Smart Cities

Liesbet van Zoonen, Erasmus University Rotterdam, The Netherlands*
Emiel Rijshouwer, Erasmus University Rotterdam, The Netherlands
Els Leclercq, Delft University of Technology, The Netherlands
Fadi Hirzalla, Erasmus University Rotterdam, The Netherlands

ABSTRACT

In this article, the authors present exploratory research about privacy behaviour in a smart city. They ask if and why people share personal data in a smart city environment. They designed a gamified survey that offers realistic scenarios in which people are asked to identify smart technologies and to share or withhold their personal data. The findings show that most respondents are willing to share their data for surveillance purposes and security benefits. They found that privacy behaviour was directly and most strongly explained by privacy concerns: people with more concerns shared less personal data than others. Smart city literacy had a much smaller effect on privacy behaviour, as did age, education, and income. They found no effect of gender or place of residence on any of the dependent variables. They discuss the meanings of these outcomes for local governments as a matter of digital placemaking (i.e., designing the smart city in a way that makes technology visible and provides transparency with respect to privacy and data governance).

KEYWORDS

Digital Placemaking, Gamified Survey, Personal Data, Privacy Concerns, Smart Cities

INTRODUCTION

In this article, we ask *if and why people share personal data in a smart city environment*. We consider such data sharing as a particular dimension of privacy behaviour, and we define a smart city as one monitored and managed by digital and data technologies.

Our research was conducted in the Netherlands in 2019, where many cities have embraced smart technologies but where no city as a whole qualifies as 'smart' (Pisani, 2015). Moreover, outside the circle of IT and data professionals or city civil servants, few Dutch people know what a smart city is, neither can they see it around them, as the constituting technologies are by and large invisible in the physical environment: cables are under the ground, Wi-Fi signals float through the air, and data are inconspicuously collected and stored (Caprotti, 2017, 2019; Van Zoonen & Hirzalla, 2018). There is, hence, no easily accessible, physical research site to observe privacy behaviour of citizens in the smart city and it is unlikely to find a large enough group of research participants who know what a smart city will be, to identify and reflect on such behaviour.

DOI: 10.4018/IJUPSC.302127 *Corresponding Author

This article published as an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/) which permits unrestricted use, distribution, and production in any medium, provided the author of the original work and original publication source are properly credited.

However, privacy behaviour is quickly becoming a salient issue in the further development of smart cities. Apart from compliance with privacy and administrative laws, it is crucial for municipalities, knowledge institutes, IT and data companies to understand and adapt to privacy behaviour and concerns of citizens, if they want to make a smart city that is beneficial to all of them and respects the public value of privacy. This is a widely held desire among smart city stakeholders as the many recent laws, charters and manifestos about ethical principles for the smart city demonstrate. Key among those documents and publications is an acknowledgment of privacy protection and citizen engagement as fundamental ingredients of a smart city (e.g., Cardullo, Di Feliciantonio & Kitchin, 2019; Greenfield, 2013; Kitchin, 2016; Morozov & Bria, 2018; Thomas et al., 2016). However, as Engelbert, Van Zoonen & Hirzalla (2019) argue, the main corporate and governmental actors frame digital and data technologies mainly as operational solutions to urban challenges. This withholds an acknowledgment of the wider societal issues at stake and the need for public debate about the democratic legitimacy of smart city development.

In this context of invisible technologies and the absence of public debate, the challenge for research is to represent the smart city in a way that speaks to research participants and elicits realistic privacy behaviour. To that end we designed a gamified and richly illustrated survey in which participants move through a virtual urban environment where they have to fulfil data-knowledge assignments, make behavioural decisions and answer value questions about privacy. Along the way they receive awards for finalizing tasks. We developed the gamified survey for two purposes: to examine, by proxy of the virtual representation, privacy behaviour in the smart city, and to raise awareness and conversation among members of the Dutch public (about which we reported in Rijshouwer, Leclercq & Van Zoonen 2022). The choices and actions of game players were registered automatically and transformed into a standard data matrix for analysis. It is this empirical data on which this article is based.

Before we discuss more details of game design, variable construction and analysis, we briefly review the literature about privacy behaviour and smart cities which informed the conceptual underpinnings of this research and the design of the survey game.

PRIVACY BEHAVIOR IN SMART CITIES

We define privacy behaviour in smart cities as the conscious sharing of personal data with urban actors, such as public authorities, private companies, civic associations or other citizens. Two elements are particularly important in this definition for our study: conscious sharing and personal data. In The Netherlands collecting personal data without explicit consent is forbidden, unless for legitimized security purposes. In other words, sharing personal data has to be a conscious act however casually and routinely this may be done. Much smart city surveillance, sensing and monitoring happens without people knowing that their cars, bicycles, movements or behaviours are being monitored: they are unaware that their data is harvested. In the Dutch context, this is only possible if this data is not turned into information about individuals, unless, again, for legitimized security purposes. There is a quickly growing body of literature about privacy in a smart city context. These studies focus on design and engineering challenges (e.g., Cui et al., 2018); privacy enhancing technologies (e.g., Martinez-Ballaste et al., 2013); on particular smart city applications (e.g., Al-Turjman et al., 2019); on privacy protecting systems (e.g., Elmaghraby & Losavio, 2014); a range of other technical solutions for securing privacy in urban digital and data technologies (see Sookhak et al., 2018 for an overview); and for achieving anonymity in urban contexts, through different systems such as k-anonymity (Sweeney, 2002) or IRMA (Alpàr & Jacobs, 2013).

There is, however, little about privacy concerns of privacy behaviour of citizens in the smart city. Van Zoonen (2016) is an exception. Building on existing literature about privacy concerns and privacy behaviour she points at four interdependent factors that may explain privacy behaviour in the smart city: the types of data that are at stake, what people know about data in the smart city (technical familiarity); their privacy concerns; and individual demographic differences. We will discuss these

factors separately, specify the research questions that follow from them, and visualize their relations in a tentative heuristic model to help explore our data.[1]

Types of Data

In smart cities, different types of data are collected and analysed. Van Zoonen (2016) distinguishes between impersonal data about, among others, air quality, ground water level, or presence of green spaces and suggests that it is highly unlikely that people will have concerns about this type of data collection or adjust their behaviour accordingly. It is personal data that is at the heart of individual concerns and collective worries.

The purpose for sharing one's personal data can vary tremendously and although there is no systematic analysis of what difference particular purposes make, there are many indications that people find the sharing of personal data for medical purpose acceptable (e.g., Ancker et al., 2013; Dinev et al., 2016). In the immediate aftermath of terrorist attacks, people are more willing to share data for security purposes, although this willingness seems to wane after about half a year (Sanquist et al., 2008; Smith & Lyon, 2013). Van Zoonen (2016) distinguishes more generally between surveillance and service purposes, closely following Lyon's (2001) distinction between control and care aims in collecting data about citizens.

The literature furthermore shows that privacy behaviour is affected by the benefits one expects from sharing personal data. These are economic benefits or financial rewards (Hann et al. 2007; Hui et al. 2007), service and convenience (Chellappa & Sin 2005; Hann et al. 2007), social or relational benefits (Jozani et al., 2020) and safety advantages (Demmers, 2018). Together these factors constitute a privacy trade-off or calculus that would influence people's privacy behaviour (Dinev & Hart, 2003). This leads to the following two research questions:

RQ1: For which purposes are people willing to share their data in a smart city context?
RQ2: For which benefits are people willing to share their data in a smart city context?

Technical Familiarity

Research in online environments indicates that Internet users' capacities to control their personal information could, in part, be explained by their awareness or knowledge regarding the technology at stake (cf. Hargittai, 2007). In accordance with research by Hargittai (2004), Park (2013, p. 230) demonstrates that people's 'technical familiarity' appears to "function as the most significant predictor of personal information control". This notion indicates that there could be a knowledge gap and hence differences in privacy decision-making behaviour between various segments in the public. Although the aforementioned studies were primarily concerned with general technical knowledge and online behaviour, rather than smart cities in particular, we consider the knowledge people have about smart city technologies as a possible factor that could explain privacy concerns and privacy behaviour in digitalized and datafied urban environments. However, as various authors have demonstrated, (technical) familiarity with the smart city is relatively low (Caprotti, 2017, 2019; Van Zoonen & Hirzalla, 2018). This leads to the following research question:

RQ3: Is there a direct relation between technical familiarity with the smart city and people's privacy concern or their willingness to share personal data?

Privacy Concerns

On the basis of consumer surveys since the 1960s, Westin (2003) developed a typology of consumers and their concerns about privacy. He distinguishes between *fundamentalists* who are generally worried about privacy and lack trust in institutions to handle their data carefully; *pragmatists* who weigh benefits and risks in particular situations; and *unconcerned* who are generally trusting and

willing to share their data for personal benefit. Throughout the surveys, the largest portion of people is found to be pragmatists (King, 2014; Kumaraguru & Cranor, 2005). Sheehan (2002) constructs a similar typology from survey data about Internet users but identifies four categories: alarmed, wary, circumspect and unconcerned. In their study regarding biometric data, Norval & Prasopoulu (2012) also identify four categories of people: privacy advocates, conservative techies, safety champions and casual adopters. However, there is no straightforward relation between privacy concerns and privacy behaviour, as the much observed privacy paradox testifies. While assuming that privacy concerns will lead people to adjust their privacy behaviour, many researchers have found that while people say to worry about privacy, they do share their data on a large number of occasions. (see Kokolakis, 2017 for an overview). This leads to the following research question:

RQ4: Is there a direct relation between privacy concerns and willingness to share personal data in the smart city?

Individual Differences

Socio-demographic features, especially gender, age and education are associated with technical familiarity, privacy concerns and privacy behaviour. With regard to gender there are indications that women score lower than male counterparts in technical knowledge and behaviours as well as that they score the same (e.g., boyd & Hargittai, 2010). Similarly, there are studies that find no gender difference in privacy concerns and behaviour, while other studies (e.g., Fogel & Nehmad, 2009) indicate that "female users exercise even more privacy control than male users did on social networking sites." (e.g., Park, 2013, p. 231). With respect to age, Acquisti et al. (2016, p. 5) argued that privacy concerns and behaviour are too idiosyncratic to make between-group comparisons useful. For education, studies have consistently demonstrated that a higher level of education is associated with more technological and digital knowledge (cf. Van Dijk, 2006), but the relation with privacy concerns and privacy behaviour is not similarly evident (Maineri et al., 2018).

In the context of a smart city, place of residence is relevant, especially the difference between living in large metropolitan environments where smart technologies have already been implemented and other, more rural environments where these are less common (see Visvizi & Lytras, 2018). The varied results about the importance of socio-demographic differences leads to the following research question:

RQ5: How do individual differences affect technical familiarity with the smart city, privacy concerns and privacy behaviour?

Relations

Of these four factors (individual differences, privacy concerns, technical familiarity and types of data) individual differences will be considered as independent variables preceding and affecting all others. The current literature gives no definite answer as to the direction and size of these effects, with the exception of the positive relation between education and technical familiarity.

Our discussion of the literature furthermore shows that two factors need to be considered as intermediate variables, i.e. technical familiarity (preceding privacy concerns and privacy behaviour), and privacy concerns (possibly but not necessarily leading to privacy behaviour).

The dependent factor in these relations is privacy behaviour in smart cities, which we defined as the conscious sharing of personal data.

We combine these relations in a heuristic model that visualizes the relations between individual differences, technical familiarity privacy concerns and privacy behaviour.

RESEARCH AND DESIGN OF GAMIFIED SURVEY

In the absence of a tangible research site or a well-informed research population, we designed a gamified survey that would make the notion of the smart city and its technologies visible and understandable to participants. Gamification in academic research is increasingly explored as a means to improve respondent engagement (e.g., Downes-Le Guin et al., 2012) and prevent the disadvantages of online surveys like non-response, respondent fatigue and straight lining (Turner et al., 2014). The latter authors did indeed find positive effects of two survey games with respondents expressing high satisfaction rates and 96% of them indicating that they would like to conduct a gamified survey again. However, Downes-Le Guin and colleagues (2012) found that completion rates for the gamified version of a survey were much lower than for text-only and merely illustrated surveys (58% as opposed to 94%). Keusch & Zhang (2017, p. 157) comment that the gamification narrative in their study was not related to the survey topic, which could explain the lack of positive effect on data quality and the low completion rate. In our current study, the survey game was perceived to be an essential means to make the smart city imaginable and tangible for our respondents, hence, topic, visualisations, gamification and questions were closely connected.

Our gamified survey, called Your Neighbourhood, Your Data (Jouw Buurt, Jouw Data), was launched on the occasion of the Dutch Science Festival in October 2018, at the website "jouwbuurtjouwdata.nl". It was produced by an independent game company from Rotterdam[2] that worked in close collaboration with the research group. The designers developed visuals, narratives and game interactions based on theoretical and methodological input from the researchers. We commissioned a dedicated panel from a Dutch commercial marketing agency to make sure we had a representative, high quality sample playing the game.[3] Panel members played the game between the 23rd and 26th of May 2019. In total, 2,800 respondents started the game, 2,118 of whom completed the survey game, a completion rate of around 75%. This is in line with the completion rate found in research on gamified surveys (Downes-Le Guin et al., 2012). After cleaning the data, N was established at 2,039.

Socio-Demographic Variables

We measured and analysed age on a 6-points-scale (1=16-24 years; 2=25-34 years; 3=35-44 years; 4=45-54 years; 5=55-64 years; 6=65 years and older; M=4.27, SD=1.402). About half of the respondents is female (53.7%; Female=0; Male=1). Education was measured on a 6-points-scale regarding which level respondents completed, with response options ranging from (1) "I am still in school" to (6) "university" (M=4.29, 1.053). We measured income on a 7-points-scale, ranging from (1) "minimum income" to (7) "more than twice of median income" (M=3.86, SD=1.674). Lastly, we also analysed place of residence, especially if people lived in one of the four big cities in the Netherlands (Amsterdam, Rotterdam, The Hague, Utrecht) or elsewhere. A minority of the respondents (13.6%) lived in one of these cities (Not living in one of these places=0; Living in one of these places=1).

Technical Familiarity

Respondents' technical familiarity with the smart city was tested in the game by providing them with two visualisations, one of a park and one of a square (Figure 3). In each of them, 10 smart technologies that collect data ('data points') were taken up, among which CCTV camera's, Wi-Fi trackers, traffic and environmental sensors, and check-in gates at public transport or city hall. Through a point-and-click action, the respondent was asked to identify as many of these data points as possible within 90 seconds. The visualisations also contained non-smart objects to distinguish random clicking from correct identifications. The respondent's total recognition score was composed of the total of correctly identified data points. The score for technical familiarity thus ranges from 0 (no correct identification) to 20 (full identification) (M=9.6, SD=3.469).

Privacy Concerns

We measured privacy concerns in the game following the logic of Westin's work and inserted three standard statements between the urban scenes in the game. The advantage of Westin's validated statements is that they also pertain to the institutions that collect data. As the responsibility for the smart city and its technologies tend to be designated to municipalities and privacy is increasingly regulated by law, we specifically asked the respondents about their concerns with respect to government. Respondents were asked to indicate to what extent, on a scale of 0 to 10, they agree with the following statements:

1. Citizens have lost all control over how personal information is collected and used by the government.
2. Most governmental institutions handle the personal information they collect about citizens in a proper and confidential way.
3. Existing laws and organizational practices provide a reasonable level of protection for citizens' privacy today.[4]

The three items (with the first one reverse-coded) formed a reliable composite variable (Cronbach's $\alpha = .675$) with values ranging from 0 to 30 (M=14.7, SD=5.797).

Privacy Behaviour

We measured people's privacy behaviour by presenting them with eight dilemmas throughout the game. With each dilemma, respondents had to decide whether or not to share their personal data. The dilemmas corresponded with purposes of financial, social or security benefits as discussed in the literature review. While entering the game, for example, respondents passed the tourist office where they were invited to leave their e-mail address in exchange for a discount pass. Further in the game, people were asked to show their ID-card to get access to a public event on the city pier. We designed these dilemmas in a service and a surveillance purpose for collecting data. This resulted in the eight game situations shown in Table 1.

The eight items produced a reliable composite variable, ranging from 0 (times personal data shared) to 8 (times personal data shared) (Cronbach's $\alpha = .604$, M=4.03, SD=1.907).

Analysis

We assessed the direct and indirect relations in our heuristic model through path analysis based on a series of multivariate regressions that tested different parts of the model before analysing the composite set of variables (see Appendix for details). We acknowledge that our independent variables have been measured as dummy (gender, residence) or as ordinal (age, education, income). As for the purpose of this explanatory study, we find this statistically acceptable as we are interested in the relative strengths and directions of relations rather than in the exact sizes of it (about which we also will not

Table 1. Data sharing in the survey game

	Convenience benefit	Financial benefit	Social benefit	Security benefit
Data collected for service purpose	Usage of personal travel card as opposed to buying ticket	Sharing one's e-mail address for a discount pass	Use social media account to rate visit to the city	Keep phone on to enable geolocation and crowd monitoring
Data collected for surveillance purpose	Ignore security cameras for the shortest route	Get reimbursement on one's debit card for waste disposal	Trade facial recognition data for personalized video	Show ID card to get access to public event space

claim results). Moreover, our intermediate and dependent variables are measured at interval level and our sample size is large, both of which are commonly considered more crucial (for an extensive discussion see Jaccard & Wan, 1996).

Before discussing the results of the path analysis, we discuss more descriptive details of technical familiarity, privacy concerns, and privacy behaviour.

RESULTS

Descriptive Statistics

Technical Familiarity

Most respondents identify about 10 of the 20 data points that were visible in the search pictures. This suggests that people generally have an idea about smart technologies in the city, but are by no means fully aware of all that are present in public space. The most often recognized technologies were the free Wi-Fi, the rain sensor and the access to public transport. The least recognized were the town hall and the smartphone (see Table 2). With respect to the latter, it must be said that the representation of the phone was small and its placement inconspicuous.

Parts of this rank order suggests that personal data collection is more easily recognized than impersonal data. The large majority of respondents, for instance, identified free Wi-Fi, public transport and the cell phone tower as data points while they did not see the collection of impersonal

Table 2. Recognized data points

Data point	% recognized
Free Wi-Fi	87.1
Rain sensor	78.5
Public transport	71.9
Cell phone tower	70.0
Personalized advertisement	65.9
Parking meter	65.3
Electric car charging point	58.3
Smart bin	55.8
Smart lamp post	50.5
CCTV camera	48.7
Vehicle registration control	45.4
Drone	41.6
Bicycle sharing service	39.5
Wi-Fi tracker	32.2
Police officer with body cam	30.8
Weather station	30.4
Traffic loop	27.6
Municipal ground water sensor	20.0
Town hall	17.5
Smartphone	12.0

data collection through the weather station, ground water sensor and traffic loop. Nevertheless, the visibility of the rain sensor modifies such an overall conclusion, as does the low rank of the town hall. We interpret this outcome as a tendency that people are more aware of their personal data being collected than of the impersonal data that the city uses as well.

Privacy Concerns

In line with Westin's findings, we find that a relatively small part of our respondents have serious concerns regarding the way their data are protected by government and law (20% are concerned about all three items). The majority (63%) finds one or two items problematic, while 16% does not worry about any statement. Scores on the individual statements are presented in Table 3.

Table 3 suggests that the privacy concerns of the Dutch with respect to the way the government handles their data are not very high; they have somewhat more concerns when it comes to the role of the law. However few respondents feel they have control over the government's usage of their personal information. [5]

Privacy Behaviour

On average, respondents were willing to share personal data in four or five of the eight situations in which they were invited to do so. Table 4 shows that respondents share their data most easily for surveillance purposes and security or convenience benefits.

Table 4 also shows the importance for respondents of other convenience benefits (taking the short route and using a personal transport card) and – to a lesser extent – of financial benefits (sharing

Table 3. Privacy concerns

Could you indicate on a scale of 0 (disagree) to 10 (agree) to what extent you agree with the following statement	Modus (the score that is most often chosen)
"Citizens have control over how personal information is collected and used by the government" *(NB. initial statement was reversely coded)*	3
"Most governmental institutions handle the personal information they collect about citizens in a proper and confidential way"	7
"Existing laws and organizational practices provide a reasonable level of protection for citizens' privacy today"	5

Table 4. Contexts of data sharing

Contexts	% Willing to share
Location data of your phone is used to provide safe routes through the centre	85.1%
You go to the city pier and take the short route with all the CCTV cameras	67.2%
For security reasons you let your ID be scanned to get access to the city pier	60.9%
You use your personal transport card to move through the city	59.7%
You share your e-mail address to get discounts in the city	50.2%
You have your bank card scanned by the smart bin to get a deposit	49.1%
You allow facial recognition in return for a personalized video of your city visit	22.5%
You share and review your city trip on social media	15.7%

e-mail and bank data). Sharing data for social benefits is uncommon among the respondents of the survey game.

Path Analysis

To examine our heuristic model depicted in Figure 1, we ran a number of regression analyses (see Appendix for details). The resulting significant relations and their sizes are visualized in Figure 4. Relations that did not come out of the analysis as significant, are not represented in the figure.

Direct Predictors of Privacy Behaviour

Comparing the effect sizes in Figure 4 shows that the most important direct predictor of privacy behaviour in the smart city is the degree to which people are concerned about their privacy. Technical familiarity is the second important direct predictor, with the effect size showing that the more data points people recognize, the less likely they are to share personal data. Age is the third direct predictor saying that older people are less likely to share their data, but its effect size is relatively small. The same holds for the direct impact of education. People with higher education share less data, but it is a relatively small effect.

Indirect Predictors of Privacy Behaviour

The indirect relations show that the impact of age on privacy behaviour is, more complex as well, as it is mediated by technical familiarity. Young people have a higher technical familiarity than older people and those well-informed younger groups share less data than their less-informed older fellow

Figure 1. Heuristic model explaining privacy behaviour in smart cities

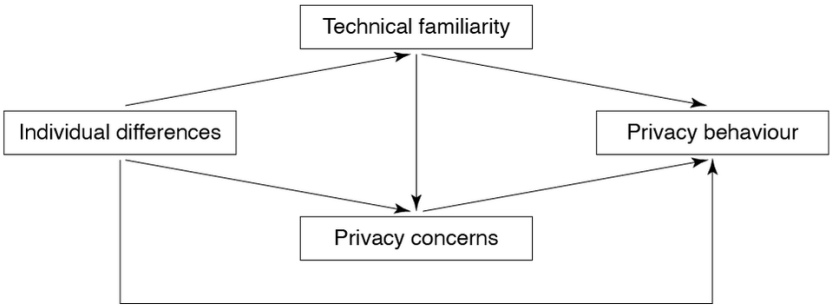
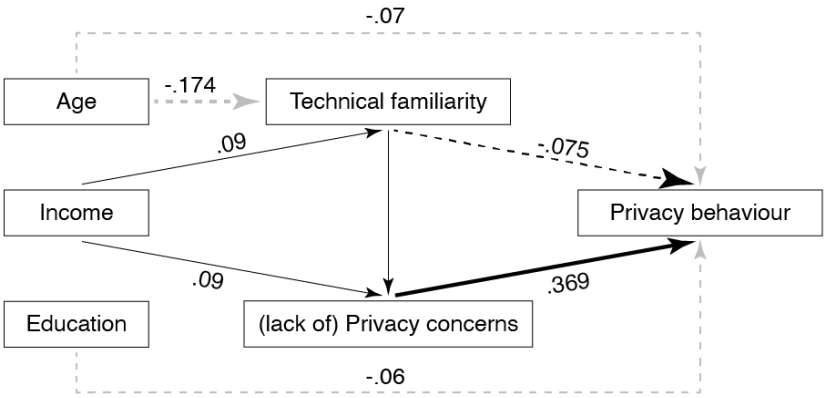


Figure 2. Opening screen of survey game Your Neighbourhood Your Data

Figure 3. Park and square where respondents are invited to identify 'data points'

Figure 4. Explaining privacy behaviour



respondents. The indirect effects of income follows two routes: one effect is that a high income is connected to more privacy concerns, which in its turn prevents data sharing. Another is that a high income is related to high technical familiarity, which also leads to less data sharing.

CONCLUSION

Summary

In this research we asked the question if and why people share their personal data in a smart city context.

The question *if* people in the smart city share their personal data (specified in more detail in research question 1 and 2 about the purpose and benefits of sharing data) has to be answered with a caveat and a condition. The caveat comes from our outcomes that show that people may not be aware of technologies that use their data. While people are able to identify some of the technologies used to collect data in cities, few of them have a comprehensive recognition. We did find a tendency that people are more aware of instruments that collect their personal data rather than seeing the means to gather impersonal data that the city deploys as well. The condition comes from our finding that sharing personal data depends on the purpose and the expected benefits. When asked explicitly if they want to share their data, our results demonstrate that our respondents are willing to share data

for surveillance purposes and if they are promised security as a benefit in return. A smaller group, but still about half of the respondents, shares data in contexts where they are offered convenience or financial benefits. In the context of this survey game, we found few people willing to share their personal data for social benefits.

The second part of our question, *why* people are sharing their data (or not), was answered by our path analysis which demonstrated that the degree of data sharing in our virtual smart city environment was most strongly predicted by the degree of privacy concerns people have (thus answering research question 4 positively). People who have few privacy concerns have a tendency to share more data than others. This variable appeared more important than technological familiarity (research question 3), age and education (research question 5). We also found that technological familiarity importantly modifies the effects of (young) age, as more technological familiarity among young people, significantly brings down their willingness to share data.

Discussion

What do these findings mean, both for academic research and for actual smart city making by local governments, entrepreneurs and citizens themselves?

First, the importance of privacy concerns as a predictor of privacy behaviour in the smart city is in direct contrast to earlier research about the privacy paradox which observed that despite their privacy concerns, people nevertheless engage eagerly in sharing their personal data. It should be noted, however, that much of that research is about social media engagement and not about a smart city environment. Nevertheless, our findings in this respect suggest a situational aspect of the privacy paradox that has not been proposed before. Secondly, the mediating effect of technical familiarity on privacy behaviour of young people importantly provides a possible explanation for the conundrum that existing studies have not found consistent effects of age on privacy behaviour; our research suggests this effect is contingent on context rather than independent.

The outcomes of our gamified survey give several suggestions for further research, especially regarding privacy concerns and their antecedents. Moreover, the absence of a privacy paradox in the smart city context of the survey game suggests strongly that both privacy concerns and privacy behaviour are situated variables that can only be well understood in the specific contexts in which they are examined. The smart city, evidently, is such a specific environment. However, currently for most people such a city is hardly a real lived environment yet. Future research, therefore, will have to rely on speculative methods like a gamified survey until there are more physical and recognizable urban spaces that qualify as 'smart'. While an increasing number of scholars is experimenting with such methods (e.g., Vervoort et al., 2015), there is, to date, little meta-analytical reflection on their validity and reliability. For our own survey game, we intend to expand the current analysis with focus groups who play the game and then reflect, jointly, on their privacy behaviour as it emerges from the game but also on their assessment of the game, its realism and relevance.

For smart city makers (governments, entrepreneurs and citizens) the results of the current research produce clear directions for policy and development. First, given that most of our respondents only recognize about half of the smart technologies in the city, a call for more data or technical familiarity of citizens seems self-evident and we are certainly not the first to do so (e.g., Engel, 2017). However, such calls implicitly frame citizens as lacking the capacities to understand the smart city, and leaves aside corporate and governmental responsibilities to make the smart city open to participation, subject to public debate and democratic decision making.

There is a design challenge here to make smart technologies in the city visible and subject to reflection. This is a challenge that goes far beyond putting up warning signs about camera surveillance or Wi-Fi tracking. Our results showed that many people in the city are willing to share their data for surveillance purposes in return for safety and convenience. Their privacy behaviour is thus, as said, contingent on specific situations and benefits. However, in addition, it appeared that people's willingness to share data is also dependent on their privacy concerns. In the smart city context,

people would need to know to which national or local privacy regimes and legislations smart city technologies are subject to, in order to make an informed assessment whether or not to share their data. This necessitates a design strategy for smart city that does not only aim at making technologies visible, but also at making them *transparent* and *contestable* in terms of the data that they collect, the purpose that it serves, the ownership of the data and other matters of data governance.

Our research outcomes thus lead to a recommendation for designing (technologies for) the smart city in ways that make them literally visible and make their data governance transparent. In this respect, current experiments with "digital placemaking" (Foth, 2017) are worth to explore further, as they focus on digital technologies as tools that need to be exposed, examined and criticized, but also as often playful and well-designed instruments to improve public space. Regarding exposure, Van Zoonen (2020) analysed a wide range of such interventions, often coming from artists and designers who are worried about urban surveillance systems, and concludes that their spectacular nature helps to 'de-normalize' surveillance technology. With respect to playfully improving public space, Frith & Richter (2020) show how digital tools can help excavate and represent lost narratives in neighbourhoods and streets. As digital placemaking is an emerging movement, it is too early to firmly assess their effectivity in making the smart city more open and inclusive. However, the studies that have been published in the past two or three years, do suggest that "the artful integration of people, place and technology" (Foth, 2017) makes it possible to include the wide array of citizens and their perspectives that are currently not part of smart city developments.

FUNDING

This work was funded by the municipality of Rotterdam, the Leiden-Delft-Erasmus Centre for BOLD Cities and the executive board of Erasmus University Rotterdam.

REFERENCES

Acquisti, A., Taylor, C., & Wagman, L. (2016). The economics of privacy. *Journal of Economic Literature*, *52*(4), 442–492. doi:10.1257/jel.54.2.442

Al-Turjman, F., Zahmatkesh, H., & Shahroze, R. (2019). An overview of security and privacy in smart cities' IoT communications. *Transactions on Emerging Telecommunications Technologies*, 3677. doi:10.1002/ett.3677

Alpár, G., & Jacobs, B. (2013, April). Towards practical attribute-based identity management: The IRMA trajectory. In *IFIP Working Conference on Policies and Research in Identity Management* (pp. 1-3). Springer. doi:10.1007/978-3-642-37282-7_1

Ancker, J. S., Silver, M., Miller, M. C., & Kaushal, R. (2013). Consumer experience with and attitudes toward health information technology: A nationwide survey. *Journal of the American Medical Informatics Association: JAMIA*, *20*(1), 152–156. doi:10.1136/amiajnl-2012-001062 PMID:22847306

boyd, d. & Hargittai, E. (2010). Facebook Privacy Settings: Who Cares? *First Monday, 15*(8).

Caprotti, F. (2017, April 20). *Research in the invisible city: Challenges for 'knowing' the smart city* [Blog post]. https://ugecviewpoints.wordpress.com/2017/04/20/research-in-the-invisible-city-challenges-for-knowing-the-smart-city/

Caprotti, F. (2019). Spaces of visibility in the smart city: Flagship urban spaces and the smart urban imaginary. *Urban Studies (Edinburgh, Scotland)*, *56*(12), 2465–2479.

Cardullo, P., Di Feliciantonio, C., & Kitchin, R. (Eds.). (2019). *The right to the smart city*. Emerald Publishing Limited.

Chellappa, R. K., & Sin, R. G. (2005). Personalization versus privacy: An empirical examination of the online consumer's dilemma. *Information Technology and Management*, *6*(2-3), 181–202.

Cui, L., Xie, G., Qu, Y., Gao, L., & Yang, Y. (2018). Security and privacy in smart cities: Challenges and opportunities. *IEEE Access: Practical Innovations, Open Solutions*, *6*, 46134–46145.

Demmers, J. (2018). *Consumers and their data. When and why they share it* (PhD thesis). Amsterdam Business School, University of Amsterdam.

Dinev, T., Albano, V., Xu, H., D'Atri, A., & Hart, P. (2016). Individuals' attitudes towards electronic health records: A privacy calculus perspective. In A. Gupta, V. Patel, & R. Greenes (Eds.), *Advances in healthcare informatics and analytics* (pp. 19–50). Springer.

Dinev, T., & Hart, P. (2003). Privacy concerns and internet use – a model of trade-off factors. *Academy of Management Proceedings*, *1*, 1–6.

Downes-Le Guin, T., Baker, R., Mechling, J., & Ruyle, E. (2012). Myths and realities of re- spondent engagement in online surveys. *International Journal of Market Research*, *54*(5), 613–633.

Elmaghraby, A. S., & Losavio, M. M. (2014). Cyber security challenges in Smart Cities: Safety, security and privacy. *Journal of Advanced Research*, *5*(4), 491–497.

Engel, J. (2017). Statistical literacy for active citizenship: A call for data science education. *Statistics Education Research Journal*, *16*(1), 44–49.

Engelbert, J., Van Zoonen, L., & Hirzalla, F. (2019). Excluding citizens from the European smart city: The discourse practices of pursuing and granting smartness. *Technological Forecasting and Social Change*, *142*, 347–353.

Fogel, J., & Nehmad, E. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior*, *25*(1), 153–160.

Foth, M. (2017). Lessons from urban guerrilla placemaking for smart city commons. In *Proceedings of the 8th International Conference on Communities and Technologies*. Association for Computing Machinery.

Frith, J., & Richter, J. (2021). Building participatory counternarratives: Pedagogical interventions through digital placemaking. *Convergence*. 10.1177/1354856521991956

Greenfield, A. (2013). *Against the Smart City*. Do projects.

Hann, I-H., Hui, K-L., Tom Lee, S-Y. & I.P.L. Ping (2007). Overcoming Online Information Privacy Concerns: An Information-Processing Theory Approach. *Journal of Management Information Systems*, *24*(2), 13–42.

Hargittai, E. (2004). Internet access and use in context. *New Media & Society*, *6*(1), 137–143.

Hargittai, E. (2007). A framework for studying differences in people's digital media uses. In N. Kutscher & H. Otto (Eds.), *Cyberworld unlimited* (pp. 121–137). VS Verlag für Sozialwissenschaften GWV/Fachverlage GmbH.

Hui, K. L., Teo, H. H., & Lee, S. Y. T. (2007). The value of privacy assurance: An exploratory field experiment. *Management Information Systems Quarterly*, *31*(1), 19–33.

Ippoliti, E. (Ed.). (2015). *Heuristic Reasoning: Studies in Applied Philosophy, Epistemology and Rational Ethics*. Springer.

Jaccard, J., & Wan, C. K. (1996). LISREL approaches to interaction effects in multiple regression. Quantitative applications in the social sciences, 144.

Jozani, M., Ayaburi, E., Ko, M., & Choo, K. K. R. (2020). Privacy concerns and benefits of engagement with social media-enabled apps: A privacy calculus perspective. *Computers in Human Behaviour, 107*.

Keusch, F., & Zhang, C. (2017). A Review of Issues in Gamified Surveys. *Social Science Computer Review*, *35*(2), 147–166.

King, J. (2014). *Taken Out of Context: An Empirical Analysis of Westin's Privacy Scale* [Paper presentation]. Workshop on Privacy Personas and Segmentation (PPS) at SOUPS, Menlo Park, CA, USA.

Kitchin, R. (2016). The Ethics of Smart Cities and Urban Science. *Philosophical Transactions of the Royal Society A*, *374*(2083). https://doi.org/10.1098/rsta.2016.0115

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

Kumaraguru, P., & Cranor, L. F. (2005). *Privacy indexes: a survey of Westin's studies*. Carnegie Mellon University, School of Computer Science, Institute for Software Research International, CMU-ISRI-5-138.

Lyon, D. (2001). *Surveillance society: Monitoring everyday life*. McGraw-Hill Education.

Maineri, A. M., Achterberg, P., & Luijkx, R. (2018, July). The educational divide in e-privacy skills in Europe. In *Proceedings of the Second International Conference on Advanced Research Methods and Analytics*. Editorial Universitat Politecnica de Valencia.

Martínez-Ballesté, A., Pérez-Martínez, P. A., & Solanas, A. (2013). The pursuit of citizens' privacy: A privacy-aware smart city is possible. *IEEE Communications Magazine*, *51*(6), 136–141.

Morozov, E., & Bria, F. (2018). *Rethinking the Smart City. Democratizing Urban Technology*. Rosa Luxemburg Stiftung.

Norval, A. J., & Prasopoulou, E. (2012). *Living in the biometric state: Examining citizen engagement with new identification technologies* [Conference paper]. 7th International Conference in Interpretive Policy Analysis (IPA 2012). Understanding the drama of democracy: Policy work, power and transformation, Tilburg, The Netherlands.

Park, L. (2013). Digital Literacy and Privacy. Behaviour Online. *Communication Research*, *40*(2), 215–236.

Pisani, F. (2015). *A Journey through smart cities: between datapolis and participolis*. UNESCO Publishing.

Rijshouwer, E., Leclercq, E., & Van Zoonen, L. (2022). Public views of the smart city; towards the construction of a social problem. *Big Data & Society*. Advance online publication. doi:10.1177/20539517211072190

Sanquist, T. F., Mahy, H., & Morris, F. (2008). An exploratory risk perception study of attitudes toward homeland security systems. *Risk Analysis*, *28*(4), 1125–1133.

Sheehan, K. B. (2002). Toward a typology of Internet users and online privacy concerns. *The Information Society*, *18*(1), 21–32.

Smith, E., & Lyon, D. (2013). Comparison of survey findings from Canada and the USA on surveillance and privacy from 2006 and 2012. *Surveillance & Society*, *11*(1-2), 190–203.

Soohak, M., Tang, H., He, Y., & Yu, F. R. (2018). Security and privacy of smart cities: A survey, research issues and challenges. *IEEE Communications Surveys and Tutorials*, *21*(2), 1718–1743.

Sweeney, L. (2002). k-anonymity: A model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-based Systems*, *10*(05), 557–570.

Thomas, V., Wang, D., Mullagh, L., & Dunn, N. (2016). Where's Wally? In Search of Citizen Perspectives on the Smart City. *Sustainability*, *8*(3), 1–13.

Turner, G., van Zoonen, L., & Adamou, B. (2014). *Research through gaming: Public perceptions of (the future of) identity management*. SAGE Research Methods Cases.

Van Dijk, J. A. (2006). Digital divide research, achievements and shortcomings. *Poetics*, *34*(4-5), 221–235.

Van Zoonen, L. (2016). Privacy concerns in smart cities. *Government Information Quarterly*, *33*(3), 472–480.

Van Zoonen, L. (2020). Performance and Participation in the Panopticon: Instruments for Civic Engagement with Urban Surveillance Technologies. In International security management: new solutions to complexity. doi:10.1007/978-3-030-42523-4

Van Zoonen, L., & Hirzalla, F. (2018). Empowering city employees in the smart city arena: Finding big open and linked data while walking. In A. Zuiderwijk, & C. Hinnant (Eds.) *Proceedings of 19th Annual International Conference on Digital Government Research*. ACM.

Vervoort, J. M., Bendor, R., Kelliher, A., Strik, O., & Helfgott, A. E. (2015). Scenarios and the art of world making. *Futures*, *74*, 62–70.

Visvizi, A., & Lytras, M. (2018). Rescaling and refocusing smart cities research: From mega cities to smart villages. *Journal of Science and Technology Policy Management*, *9*(2), 134–145.

Westin, A. F. (2003). Social and political dimensions of privacy. *The Journal of Social Issues*, *59*(2), 431–453.

ENDNOTES

1. A heuristic model is an informal way to summarize variables and relations that differs from theoretical models meant to test hypotheses (see Ippoliti, 2015).
2. WeAreReasonablePeople, Rotterdam
3. Motivaction Research and Consultancy, Amsterdam
4. In the gamified survey, i.e. in Dutch, these questions were formulated as follows: 1) Ik denk dat mensen controle hebben verloren over de persoonlijke gegevens die de overheid over hen verzamelt. 2) Ik denk dat de overheid op een nette en betrouwbare manier met de persoonlijke gegevens van mensen omgaat. 3) Ik denk dat de wetten en regels in ons land ervoor zorgen dat de privacy van burgers beschermd wordt.
5. It is important to take account of the time of measurement in the spring of 2019. Early 2020, the Dutch tax office was confronted with massive outrage about its arbitrary use of data to control citizens and keep them from receiving allowances. It could be that levels of privacy concerns have risen since the survey game was conducted as a result. https://www.dutchnews.nl/news/2019/12/minister-survives-tax-office-fraud-scandal-debate-pledges-speedy-compensation/

APPENDIX

Regression Analyses

Model 1. Y = Technical familiarity

	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
(Constant)	10.191	0.512		19.907	0.000
Age	-0.430	0.066	-0.174	-6.513	0.000
Gender	0.340	0.182	0.050	1.867	0.062
Income	0.203	0.056	0.099	3.636	0.000
Education	0.054	0.089	0.017	0.608	0.543
Urbanization	0.111	0.254	0.011	0.436	0.663

Model 2. Y = Privacy concerns

	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
(Constant)	14.913	0.891		16.730	0.000
Age	0.062	0.115	0.015	0.541	0.588
Gender	0.195	0.316	0.017	0.617	0.537
Income	0.299	0.097	0.086	3.082	0.002
Education	-0.304	0.156	-0.054	-1.952	0.051
Urbanization	-0.016	0.442	-0.001	-0.037	0.971

Model 3. Y = Privacy behaviour

	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
(Constant)	4.950	0.286		17.316	0.000
Age	-0.075	0.037	-0.055	-2.028	0.043
Gender	0.049	0.102	0.013	0.480	0.632
Income	0.047	0.031	0.042	1.506	0.132
Education	-0.144	0.050	-0.081	-2.892	0.004
Urbanization	0.200	0.142	0.036	1.409	0.159

Model 4. Y = Privacy concerns

	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
(Constant)	15.651	1.003		15.599	0.000
Age	0.031	0.117	0.007	0.263	0.792
Gender	0.219	0.317	0.019	0.693	0.488
Income	0.313	0.097	0.090	3.218	0.001
Education	-0.300	0.156	-0.054	-1.926	0.054
Urbanization	-0.009	0.442	-0.001	-0.020	0.984
Tech. fam.	-0.072	0.045	-0.042	-1.600	0.110

Model 5. Y = Privacy behaviour

	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
(Constant)	3.594	0.322		11.149	0.000
Age	-0.095	0.035	-0.070	-2.732	0.006
Gender	0.040	0.094	0.011	0.425	0.671
Income	0.018	0.029	0.016	0.632	0.528
Education	-0.107	0.046	-0.060	-2.313	0.021
Urbanization	0.204	0.132	0.037	1.548	0.122
Tech. fam.	-0.041	0.013	-0.075	-3.056	0.002
Privacy concerns	0.118	0.008	0.369	15.324	0.000