Securing the smart city: patterns of public acceptance for integrated technological solutions

BAYERL, Petra <http://orcid.org/0000-0001-6113-9688>, BATES, Luke and AKHGAR, Babak <http://orcid.org/0000-0003-3684-6481>

Citation:

BAYERL, Petra, BATES, Luke and AKHGAR, Babak (2023). Securing the smart city: patterns of public acceptance for integrated technological solutions. In: 2023 IEEE International Smart Cities Conference (ISC2). IEEE. [Book Section]

Securing the smart city: Patterns of public acceptance for integrated technological solutions

Petra Saskia Bayerl
CENTRIC
Sheffield Hallam University
Sheffield, UK
p.s.bayerl@shu.ac.uk

Luke Bates
CENTRIC
Sheffield Hallam University
Sheffield, UK
l.bates@shu.ac.uk

Babak Akhgar
CENTRIC
Sheffield Hallam University
Sheffield, UK
b.akhgar@shu.ac.uk

Abstract— **Security solutions for smart cities are a contested topic, particularly with the increasing deployment of advanced technologies such as AI. However, current discussions often focus on specific solutions such as live facial recognition in public spaces, yielding mixed results for citizen acceptance. In this paper we offer a systematic investigation of citizen acceptance by comparing disparate types of security solutions and disparate deployment situations for these solutions. This investigation offers explanations for the often seemingly disjointed patterns of citizen acceptance. It further evidences the expected safeguards and the actors, citizens deem (most) responsible for securing public spaces. Our study is relevant to organizations tasked with planning and developing security solutions in smart cities, particularly to inform proactive engagements with citizens about smart city security solutions.**

Keywords—smart cities, safety, security, citizens, public acceptance, CCTV, drones, Artificial Intelligence

I. Introduction

Smart city efforts are often accompanied by ambitions to improve public safety and the security of citizens in public spaces. The solutions (actual or proposed) vary greatly, from local sensors for sounds, smells or movement to the broad-area capture of biometrics or the integration of multi-data streams to automate decision-making by security actors.

The introduction of safety solutions for the protection of public spaces are of particular concern to citizens as they go about their daily lives. While some efforts may stay invisible, many tangible representations of security solutions (e.g., visible sensors, CCTV, drones) can affect citizens' sense of place as they move through their everyday urban environments [1]. Citizens can experience this in various ways: as reassurance for their personal safety, as subtle pressure to avoid such spaces or as severe infringement into their personal freedom.

Despite depicting some of the biggest social and ethical challenges, security in smart cities is most often discussed in terms of cybersecurity or reviewed in the light of data privacy [2]. In contrast, the consideration of citizen views on public space protection often remains absent from the smart city discourse [3]. This is problematic, not only because of the wide-ranging consequences security solutions can have on citizens but also because citizen acceptance is vital for the sustainability of smart city implementations. Some high-profile smart city projects such as the Google-linked Sidewalk initiative in Portland, Oregon, USA or Toronto, Canada failed perhaps not exclusively due to citizen concerns but certainly in part because of them [4],[5].

Currently, not enough is known about the acceptance of specific technologies or the specific concerns that citizens might have about them. Also, while past studies have indicated disparities in acceptance for rural versus urban deployments of various security solutions (e.g., [6]), it remains largely unknown how citizens react to deployments across disparate types of urban locations.

It is important to understand citizens' opinions, in order to promote the development of democratically responsible smart cities. A better understanding of citizen concerns will also support more responsible security practices that are designed with citizens' preferences in mind, helping to ensure the public acceptance of future smart city safety solutions.

In this paper we report findings from an investigation into citizen acceptance for disparate safety solutions that are being trialed in various locations within Europe. The investigation enables a more systematic understanding of what drives variations in their acceptance.

II. Methodology

To investigate patterns of citizen acceptance for public space protection we conducted a scenario-based online survey with citizens in the UK. Scenario-based approaches are a powerful approach to study reactions to situations that cannot be created or replicated in real-life, as they combine realism with the controlled manipulation of situational features that can explain variations in reactions [7]. In this section we describe our approach, including the origin of the scenarios, as well as the study sample and further data collection decisions.

A. Sample

A total of 150 participants took part in the study. Participants represent a diverse set of citizens with 52% living in urban, 36.6% in suburban and 11.3% in rural areas. About a quarter of respondents (23.3%) self-identified as ethnic minority and 68.7% as ethnic majority (8% preferred not to say). The majority held a university degree as highest education (69.3%), 17.3% primary or secondary school degrees, and 12.7% other degrees (0.7% preferred not to say). The sample tends towards younger and middle-aged citizens (41.3% 18-34 years, 52.0% 35-54 years, 6.7% 55+ years) and men (70% men, 29.3% women, 0.7% non-binary). 44.7% had children compared to 54.7% (0.7% preferred not to say). We further asked participants whether they work in a security profession, as security expertise is likely to impact individuals' reactions. Overall, 20.9% indicated working in a security or safety related profession (i.e., security, first responder, online security/ cyber). Participants were recruited

This research was conducted as part of the APPRAISE project. The APPRAISE project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No. 101021981. For the purpose of open access, the authors have applied a Creative Commons Attribution (CC BY) license to any Author Accepted Manuscript version arising from this submission.

through the online crowdsourcing platform mTurk and received £2.38 ($2.91) after completion of the survey, calculated based on hourly wage rates in the UK.

B. Variables and Analysis

Patterns of acceptance were investigated with respect to two aspects: (1) the *type of technology* used for public space protection and (2) the *type of public space* the technologies are implemented in. Both the technologies and the public spaces used in the survey scenarios described actual cases. The technologies are developed for public space protection in the EU-funded project APPRAISE which pilots these technologies in five concrete locations, each in a different EU country (for details see https://appraise-h2020.eu). For the purpose of this study, the concrete technologies (e.g., tool names) and locations (e.g., a specific shopping mall or sports event) were reformulated into more generic descriptions to ensure that the descriptions were useful and understandable to participants independent of where they live.

Type of technologies: The following six public space protection solutions were presented: (1) online analyses of social media in order to monitor posts that may indicate potential threats; (2) CCTV with video analysis capabilities placed in key locations that can identify dangerous objects as well as abnormal behaviors by vehicles and individuals; (3) microphones that can autonomously recognize sounds such as gunshots or screams placed in key locations in order to detect potential threats; (4) drones to monitor surrounding areas; (5) a crowdsensing mobile app that can be downloaded by attending citizens, so that they can report anomalies themselves to security actors for investigation; (6) a graphical user interface system security actors use to integrate all data streams from the technologies mentioned above, to help them with their communication and coordination.

Type of public space: Five locations were assessed, in line with the five pilots tested in the project. The different locations allowed to compare disparities in citizens' reactions to two aspects: (1) *duration of technology usage*: continuous vs event-specific, (2) *scope of technology usage*: large-scale vs specific area. Participants were asked to imagine that the technologies above were used in each of the five locations using the following prompts:

- Location 1 (duration: continuous; scope: large-scale): Technologies are deployed within the whole of a large European city. The city is continuously monitored by the technologies for any potential crimes including terrorist attacks.
- Location 2 (duration: continuous, scope: specific area): Technologies are deployed in a popular shopping and entertainment complex. The shopping and entertainment complex is continuously monitored by the technologies for any potential crimes including terrorist attacks.
- Location 3 (duration: event, scope: large-scale): Technologies are deployed during a professional cycling tour that takes a long route starting in one country and ending in another. The cross-border route will be monitored during the race by the technologies for any potential crimes including terrorist attacks.
- Location 4 (duration: event, scope: specific area): Technologies are deployed during a tennis tournament which is held in a large indoor arena. The venue will be monitored during the event by the technologies for any crimes including terrorist attacks.
- Location 5 (duration: event, scope: specific area): Technologies are deployed during an international fair event held in an indoor exhibition hall. The venue will be monitored during the event by the technologies for any potential crimes including terrorist attacks.

Locations 4 and 5 both focus on *events* at a *specific* area. The inclusion of both situations was decided to allow a comparison of all five pilot sites within the context of the project.

Acceptance of technologies was measured with six items (e.g., "Security actors should use this technology for public space protection" and "This use of technology benefits society"; α values across the six technologies: .91-.95). Acceptance of deployment in specific locations was assessed with three items (e.g., "I have no hesitation to be in this situation where APPRAISE technologies are employed."; α values across the five public spaces: .90-.95).

In addition to acceptance within locations, we also captured participants' feelings of safety within each of the locations given the use of the technologies. This was assessed by one item: "This use of the APPRAISE technologies makes me feel safe". All items were measured on a 5-point Likert scale (1: strongly disagree to 5: strongly agree).

We further asked participants for safeguards they expected to see in place if such technologies are deployed in public spaces. Participants were asked to rank four safeguards in order of importance (1: highest importance to 4: lowest importance):

- The surveillance technologies must be properly regulated.
- The surveillance technologies must conclusively contribute to the safety of society.
- The security actors involved must have the support of citizens.
- The surveillance technologies must be visible to citizens, rather than hidden.

An open question allowed participants to list additional safeguards ("Are there any other conditions you have for security actors to use advanced surveillance technologies?").

A question to assess expectations about the type of organizations responsible for security in public spaces was included to understand who should be tasked with the protection of public spaces (item: "Who would you say is responsible for your security in public spaces?"). The question was asked twice, each offering a set of three answer options to choose from: (1) security actors, participants themselves or both, (2) private security actors, police or both.

All participants were presented with all technologies and locations (within-subject design) to allow the direct comparison of reactions. However, technologies and locations were presented in a randomized order across participants to avoid potential influences due to sequence effects. Given the within-subject design, repeated ANOVAs (Analysis of Variance tests) were conducted with acceptance as dependent variable. Two ANOVAs were conducted, one to compare acceptance between technologies, the second to compare acceptance between locations. Fig. 1 provides an overview of the methodology.

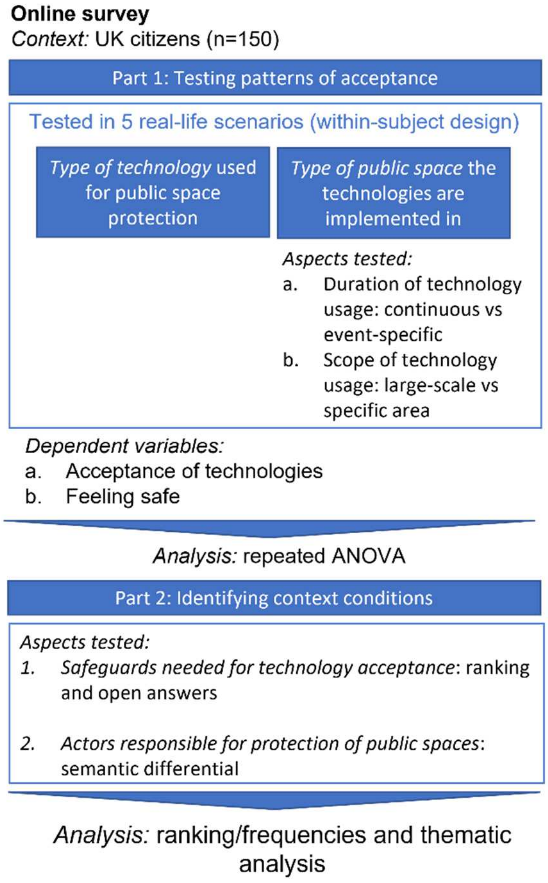
Online survey
Context: UK citizens (n=150)
Part 1: Testing patterns of acceptance
Tested in 5 real-life scenarios (within-subject design)
Type of technology used for public space protection
Type of public space the technologies are implemented in
Aspects tested:
a. Duration of technology usage: continuous vs event-specific
b. Scope of technology usage: large-scale vs specific area
Dependent variables:
a. Acceptance of technologies
b. Feeling safe
Analysis: repeated ANOVA
Part 2: Identifying context conditions
Aspects tested:
1. Safeguards needed for technology acceptance: ranking and open answers
2. Actors responsible for protection of public spaces: semantic differential
Analysis: ranking/frequencies and thematic analysis

Fig. 1. Overview of study methodology

C. Ethics

The study received ethics approval from our university's ethics committee. All surveys were collected anonymously (i.e., no capturing of IP addresses, location data, etc.). Participants were further asked to give their informed consent for the study as well as the usage of their answers in publications. Participants who did not consent were not able to enter the survey to ensure that only valid data would be included in the study.

III. Findings

A. Acceptance Differences with respect to Technologies

Clear disparities emerged in the level of acceptance for specific technologies to keep public spaces safe. The differences are significant, F(4.66, 694.56)=18.73, p<.001, η^2=.11, indicating that certain technologies were systematically seen as more or less acceptable. The highest acceptance was found for CCTV with video analysis capabilities followed by the crowdsensing mobile app that can be used by citizens themselves to report anomalies (cp. Fig. 2). In contrast, the integration of various data streams in a graphical interface and particularly the usage of drones to monitor areas elicited the lowest acceptance.

We next tested the impact of individual characteristics by entering demographic variables as between-subject factors into the repeated ANOVAs. Interestingly, most demographics did not show any systematic impacts, indicated by non-significant results for gender (p=.10), age group (p=.45), education (p=.75), self-ascribed ethnic minority/majority status (p=.28) and living in a (sub)urban or rural area (p=.10). However, working in a security related profession increased acceptance, F(1,148)=4.47, p<.05, η^2=.03, as did the fact of having children, F(1,147)=16.23, p<.001, η^2=.10.

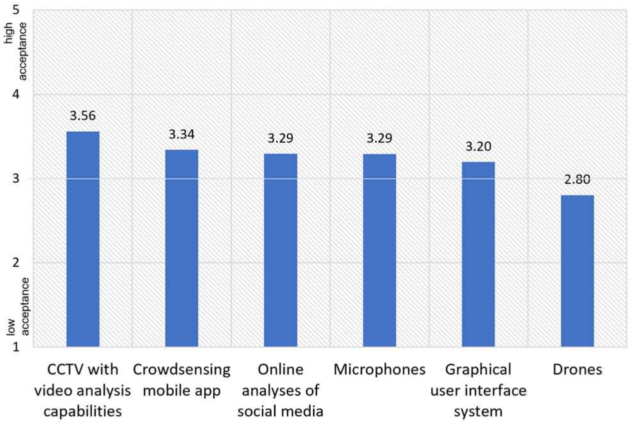

Fig. 2. Disparities in acceptance of specific technologies

B. Acceptance Differences with respect to Location

Systematic differences also emerged for the type of public space the six technologies would be employed in for public space protection (cp. Fig. 3). A direct comparison of the five locations shows that acceptance was highest for deployment during a tennis event (m=3.91) or during a fair (m=3.85), while deployment in a mall (m=3.63) or citywide (m=3.27) were less favored. These disparities were highly significant with F(3.06, 455.96)=27.71, p<.001, η^2=.16. Visually investigating the ordering suggests that the features of the location and deployments have an impact on acceptance levels.

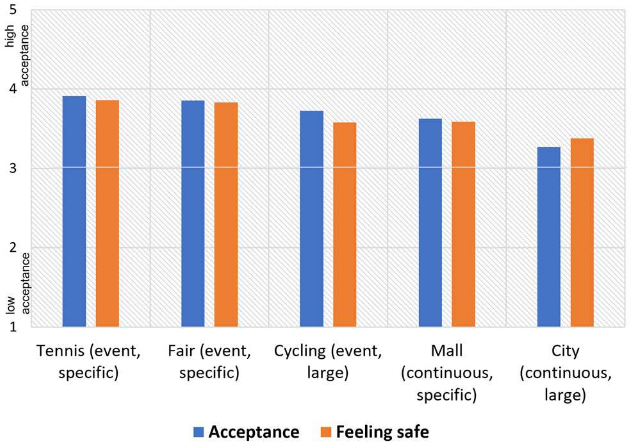

Fig. 3. Disparities in reactions to technologies across locations (ordered for decreasing acceptance)

To test this assumption, in a separate analysis we systematically compared locations with respect to the two dimensions *duration* (continuous vs event-specific) and *scope* (large-scale vs specific place; see methodology section). Of the two public places representing the combination of *event* and *specific place*, we used the tennis tournament for the analysis. The repeated ANOVA confirms a clear impact for both dimensions (cp. Fig. 4): firstly, continuous deployments were less acceptable than event-specific deployments, F(1,149)=46.98, p<.001, η^2=.24, secondly, large-scale deployments were less acceptable than deployments in limited places, F(1,149)=29.01, p<.001, η^2=.16.

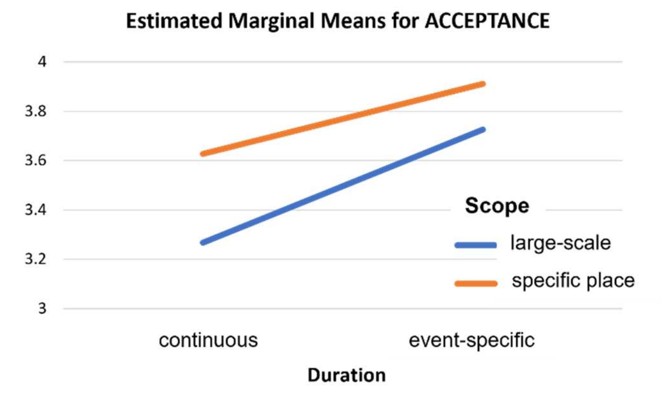

Fig. 4. Disparities in acceptance based on duration and scope of public space surveillance

Investigating demographic differences showed no impacts on acceptance for gender (p=.50), age (p=.35), education (p=.60), ethnic minority/majority status (p=.25), (sub)urban vs rural living area (p=.55) and security-related profession (p=.11). Only having children had a significant influence, F(1,147)=15.22, p<.001, η^2=.10, with overall higher acceptance across all tested locations for those who had children compared to those who had none.

An important measure of impact is the question, how safe participants feel in each of the situations if the project technologies would be used. Comparing locations, feelings of safety ranged from neutral to moderate across the five deployment situations (from m=3.38 to m=3.86). As Fig. 3 demonstrates, slight disparities can be observed for deployments during a cycling event and within a city. However, the differences are small, indicating that feeling safe was largely aligned with the level of acceptance in a situation. This close link between acceptance and feeling safe suggests that acceptance may be driven (also) by perceived benefits of advanced technologies for personal safety in public spaces.

C. Expected Safeguards

Participants were offered four possible safeguards. Fig. 5 shows the ranking decisions for the four safeguards, presenting how often each safeguard appeared on rank 1 (most important), 2, 3 or 4 (least important), respectively. As the findings demonstrate, proper regulation was considered by far the most important safeguard. In second place, with near equal spread across ranks, was the need to contribute to the safety of society, followed by involvement of citizens by security actors and last the visibility of technologies. The respective relevance of safeguards is even more clearly illustrated by the respective mean ranks for each of the safeguards: regulation: 1.6; contribution to society: 2.5; being supported by citizens: 2.9; visibility: 3.0.

Next to the four pre-defined aspects, the open answers yielded important pointers for further safeguards to improve the acceptability of safety solutions in public spaces. Of the 150 participants, 91 provided inputs, which were clustered thematically to extract common themes. Some comments covered more than one theme. These comments were split into separate parts, each representing one theme only. Three comments were unclear and thus excluded, leaving a total of 108 usable entries.

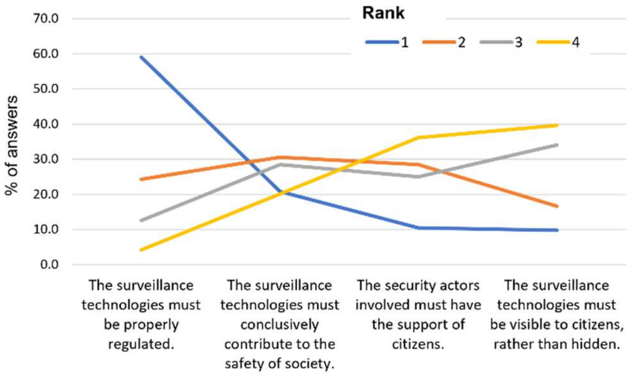

Fig. 5. Ranking decisions for each of the four safeguards

Eight themes can be differentiated referring to (1) *deployment* of the technologies, (2) their *regulations*, (3) *protections* for citizens, (4) *transparency*, (5) *impacts*, (6) the need for *trust*, (7) the *technologies* themselves and (8) no usage. Within each of the first five themes further sub-themes emerged that clarified specific aspects; for instance, safeguards with respect to technology deployment relate variably to acceptable ways of data storage, (un)acceptable locations, ethics of data usage, etc. Safeguards relating to deployment were also the most frequent acceptance conditions, followed by proper regulation/oversight, appropriate protections and sufficient transparency. Compared to these areas, the remaining themes played a considerably smaller role.

The full list of themes and sub-themes identified in the data together with example quotes (taken verbatim from the data) is given in Table 1.

D. Responsible Actors

Another important perspective is added by considering the actors responsible for security in public spaces. Interestingly, only 17.3% considered security to be primarily the responsibility of security actors, compared to nearly half of the participants (45.3%) who considered the responsibility primarily to lie with themselves and 37.3% with both parties (cp. Fig. 6).

Focusing on security actors, police were seen by three quarters of participants as the main responsible party and only 1 in 5 considered police and private security actors together as responsible (21.3%). Only a minor part saw the core responsibility with private security actors alone (4.7%).

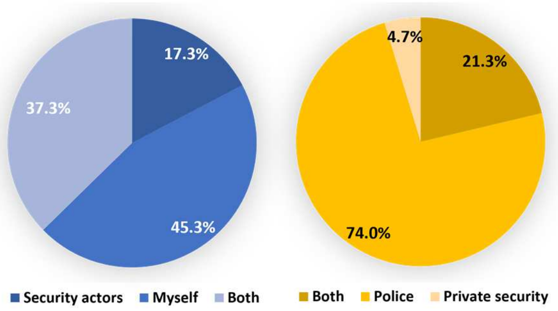

Fig. 6. Actors responsible for security of public spaces

TABLE I. ADDITIONAL SAFEGUARDS AND ACCEPTANCE CONDITIONS

Themes and sub-themes	#	Example quotes
Deployment	***29***	
– Data storage	14	Data should be kept for a fixed period of time and then erased if not contributing to safety.
– Location	7	It shouldn't be in residential areas unless the people living there request it. The advanced surveillance tech should mainly/only be used for businesses and public shopping areas.
– Use only as supplement	3	More visible police presence is required as well. Need to avoid the crime not just moving to somewhere else that has less security.
– Ethics of data usage	2	If used they must not be abused and used to target people with prejudice.
– Costs	1	Should be cost effective
– Commitment	1	That the police should support it as well.
Regulation/oversight	***20***	
– Monitoring of usage/vetting	11	The people using these technologies should be screened and reviewed regularly for potential bad actors.
– Regulation	5	Proper regulation of the use of these technologies is paramount; Regulation and auditing must be done by multiple unaffiliated parties, private and public.
– Redress	2	Severe penalties should be imposed on security actors that abuse this new tool.
– Oversight	1	Civilian oversight
– Independence of contracts	1	Contracts independently awarded
Protections	***17***	
– Privacy protections	13	Privacy of innocent civilians must be guaranteed.
– Purpose limitations	4	Surveillance technologies should only be used for their intended purpose.
Transparency	***15***	
– Transparency needed	14	It must be made clear in all circumstances that these measures are present and being used; Transparency regarding where any collected data goes.
– Secrecy needed	1	Security technologies must be a secret and effective
Impacts	***6***	
– Societal benefits	4	The use of such technology should only be used where it provides a demonstrable benefit to society over time.
– Actions	1	There should be immediate action when a crime is detected
– Safe for citizens	1	The technologies must be safe for citizens.
Trust	***2***	The actors should use their skills to show people or consumer how the product was trustworthy.
Technologies	***2***	Continually develop the system and not let it stagnate as society and environments are ever changing.
Do not use	***3***	I don't think it's a good idea.
[no comment]	***14***	All good

IV. DISCUSSION AND CONTRIBUTIONS

The protection of public spaces is a continuing concern of municipalities and citizens and requires close attention within smart city efforts. The implementation of security measures, however, is often contested [8]. Our study provides important insights into the factors that increase or decrease citizen acceptance towards advanced security technologies, as they are deployed in different public spaces. Particularly, we demonstrate that acceptance is impacted by the specific type of technology solution used as well as the scope and duration with which these technologies are used.

Generally, clearly circumscribed locations and timescales find higher acceptance than large-scale and long-lasting or even continuous deployments. Considering acceptance levels for the specific technologies tested in our study adds interesting pointers towards other potential impact factors. Firstly, the comparatively high acceptance for CCTV with video analysis capabilities may have to be seen in the context of the sample, namely participants in the UK. In the UK, CCTV cameras are a common feature in public spaces (over 5.2 million according to some estimates; [9]), which means that UK citizens are highly familiar with this technology. This may suggest that advanced solutions that are comparable to already existing solutions (in our case CCTV that is enhanced with AI features) might thus be easier to argue for than unfamiliar solutions.

The crowdsourcing app, as the second most accepted solution, offers citizens control over data streams. Given common safeguarding expectations voiced in the open answers around data storage, regulation and transparency on the one side, and the fears of rogue actors using advanced technologies in an unpredictable or biased way on the other, retaining control may be one factor that positively sways citizens towards security solutions. This also chimes with the considerable number of participants who see the responsibility for public security by themselves rather than security actors. The lower acceptance of drones, in contrast, may be linked to their ability to cover large areas and thus the potential to be deployed as mobile units on a broad geographical scope and with little control by citizens [10]. Tan and colleagues, for instance, demonstrate the general impact of fears and privacy concerns for lowering acceptance [11], while Sakiymaya and colleagues found direct indications that the deployment location plays a crucial role with higher acceptance for rural contexts compared to urban contexts [6]. Clearly, these aspects and their impacts require further study. We put them forward here as hypotheses that deserve further investigation.

In the same regard, it is important to note that even the highest level of acceptance for specific technologies was only on a moderate level (m=3.56 on a 5-point scale). While security in public spaces is a common concern for citizens, it seems that being confronted with concrete locations and the specific technologies with which to achieve this security leads to more nuanced and thus less generically positive reactions. This is also visible in the highly varied and differentiated expectations for safeguards which arose from our study. This observation should caution against ever expecting full acceptance of security solutions. Instead, municipalities – and security actors themselves – will have to engage with the varied expectations of citizens in equally differentiated ways. Relatedly, questions put towards citizens need to go beyond generic questions about smart cities' benefits or security, if the aim is to achieve a realistic appreciation of acceptance by citizens.

In this context, our findings on demographics are revealing and thought-provoking, in that none of the 'traditional' group-based demographics (e.g., gender, age group, self-ascribed ethnic minority/majority status) yielded any significant results, in contrast to individual-level variables (i.e., parenthood and profession). What this suggests is that assumptions around 'who ought to be welcoming or resenting' security solutions, and related discussions about data or usage biases from advanced technologies, may be more varied than often assumed, in that very personal circumstances (such as parenthood) can have important (additional) impacts on perceptions of specific security solutions.

A. Further Research

The survey was conducted with a diverse set of UK citizens using real-life security solutions currently being developed and piloted in European cities. This means that the findings from this study provide a solid foundation to judge citizen acceptance based on actual implementation parameters. In the same regard, our study is cross-sectional, i.e., provides one view or snapshot in time which focuses on one-time acceptance for the deployment of such technologies. While this is valuable, especially to understand initial reactions of citizens to the (potential) introduction of new technologies, as many studies consistently demonstrate, technology implementation and adoption is a continuous process during which attitudes towards technologies can shift and change considerably [12],[13]. Hence, there is value in understanding how attitudes adapt, for instance, with longer-term exposure to specific technologies in a public space, or as citizens become more familiar with advanced security solutions in their lifes over time (e.g., AI or drones).

Given our findings about demographics and personal experiences, we further propose closer investigations into the intersection between various diversity and experiental aspects on the group and individual level.

Attitudes towards technologies, and specifically technologies which sections of society may constitute as 'surveillance tools', are informed by cultural and historical contexts [14],[15]. Therefore, in the near future we are aiming for replication and validation of our findings in other cultural and country contexts.

V. Conclusions

Overall, our study demonstrates that investigations into citizen reactions profit from an approach that facilitates the identification of patterns of acceptance and concerns. In consequence, we would argue that meaningful investigations into citizen acceptance need approaches that are transparent about the concrete features, usage purposes and application scenarios of security solutions in public spaces. In addition, our findings offer very practical contributions for decision-makers in smart cities, not only by providing insights into the differentiated reaction to specific security solutions, the scope and duration of their deployment, but also the categories of expected safeguards and responsible actors.

[1] V. Butot, G. Jacobs, P. S. Bayerl, J. Amador, and P. Nabipour, "Making smart things strange again: using walking as a method for studying subjective experiences of smart city surveillance," Surv. Soc., vol. 21, pp. 61-82, 2023.

[2] E. Ismagilova, L., Hughes, N.P. Rana, and Y.K. Dwivedi, "Security, privacy and risks within smart cities: Literature review and development of a smart city interaction framework," Inf. Syst. Front, vol. 24, pp. 393–414, 2022.

[3] F. de Haan and V. Butot, "Finding safety in the smart city: a discourse analysis with strategic Implications," in International Security Management: New Solutions to Complexity, G. Jacobs, I. Suojanen, K. E. Horton, and P. S. Bayerl, Eds. Switzerland: Springer, 2021, pp. 225-242.

[4] J. Wakefield, "The Google city that has angered Toronto," BBC, 18 May 2019, https://www.bbc.co.uk/news/technology-47815344

[5] J. Wakefield, "Google-linked smart city plan ditched in Portland," BBC, 23 February 2021, https://www.bbc.co.uk/news/technology-56168306

[6] M. Sakiyama, T.D. Miethe, J.D. Lieberman, M.S.J. Heen, and O. Tuttle, "Big hover or big brother? Public attitudes about drone usage in domestic policing activities," Sec J, vol. 30, pp. 1027-1044, 2017.

[7] H. Aguinis, and K. Bradley, "Best practice recommendations for designing and implementing experimental vignette methodology studies", Organ. Res, Methods, vol. 17, pp. 351-371, 2014.

[8] A. van Twist, E. Ruijer, and A. Meijer, "Smart cities and citizen discontent: A systematic review of the literature," Gov. Inf. Quart., vol. 40, 101799, 2023.

[9] HR News, "Number of CCTV Cameras in the UK reaches 5.2 million," 19 November 2020, https://hrnews.co.uk/number-of-cctv-cameras-in-the-uk-reaches-5-2-million/

[10] H. Sabino, R.V.S. Almeida, L. Baptista de Moraes, W. Paschoal da Silva, R. Guerra, C. Malcher, D. Passos, and F.G.O. Passos, "A systematic literature review on the main factors for public acceptance of drones," Tech. in Soc., vol. 71, 102097, 2022.

[11] L. Tan, B.C. Lim, G. Park, K.H. Low, and V.C. Yeo, "Public acceptance of drone applications in a highly urbanized environment," Tech. in Soc., vol. 64, 101462, 2021.

[12] D. Leonard-Barton, "Implementation as mutual adaptation of technology and organization," Res. Policy, vol. 17, pp. 251-267, 1988.

[13] P.S. Bayerl, K. Lauche, and C. Axtell, "Explaining the dynamics of group-based technology adoption over time," MIS Quart., vol. 40, pp. 775-784, 2016.

[14] V. Kalmus, G. Bolin, and R. Figueiras, R., "Who is afraid of dataveillance? Attitudes toward online surveillance in a cross-cultural and generational perspective," New Media & Society, online in advanc/e, 2022.

[15] N. Thompson, T. McGill, A. Bunn, and R. Alexander, "Cultural factors and the role of privacy concerns in acceptance of government surveillance," J Assoc Inf Sci & Tech, vol. 71, 2020.