To what extent do public perceptions of connected places affect the security and sustainability of connected places?

A Systematic Literature Review

Joe Bourne[1], Chengyuan An[1], Agnieszka Dutkowska-Zuk[1], Xuan Gao[1], Oktay Cetinkaya[2], Peter Novitzky[3], Gideon Ogunniye[3], Rachel Cooper[1], David De Roure[2], Julie McCann[4], Jeremy Watson[3], Tim Watson[5], and Eleri Jones[3]

[1]Lancaster University
[2]University of Oxford
[3]University College London
[4]Imperial College London
[5]The Alan Turing Institute

Executive Summary

This review has been conducted by PETRAS National Centre of Excellence for IoT Systems Cybersecurity.[1] PETRAS stands for: privacy, ethics, trust, reliability, acceptability and security. These factors are key in the analysis of the security and sustainability of the Internet of Things, and by association, connected places. Therefore, the authors have considered cyber security through each of these lenses when conducting the review.

The review explores the existing literature on public perceptions and behaviors in the context of cyber security in connected places. It reveals that while many articles highlight the importance of public perceptions and behavior during a cyber-attack, there is no consensus on how to influence them to minimise attack impact and expedite recovery. Additionally, there is disagreement across the literature on who the public and connected place managers are, their motivations, and how they relate to each other in the context of connected place cyber security. The review also shows that public perceptions can affect the success and sustainability of connected places, however, exactly how and to what extent is not known. Findings of note include:

- End user devices and the way they are maintained are key technical vulnerabilities for the security and sustainability of connected places. However, it is unclear how much influence connected place managers can have on weak points in either user behaviour or the supply chain of these devices.
- In general, the majority of the public is oblivious to connected places. This presents a passive threat of accidental damage and increased vulnerability to attacks oriented to social engineering that may damage the infrastructure of the connected place and data reliability.
- In extreme circumstances, the public can become an active threat to the security and sustainability of connected places should they reject a connected place due to lack of trust or perceived invasion of privacy. This may manifest itself as low-skilled cyber-attacks, data obfuscation, or vandalism to hardware.
- Public perceptions and behaviours increase in importance during and immediately after an attack when place managers need to manage public behaviours.

[1]https://petras-iot.org

- Models, policies and place managers' communication can be vital in shaping public perceptions of connected places. However, there is not enough evidence to provide guidance on which are most effective due to the lack of depth and transferability in current research and the complexity of the connected place landscape.
- Existing literature emphasises the importance of involving the public in discussions about connected places to ensure the success and security of these places.

The authors argue that more research is needed on the mechanisms to assess the influence of public perceptions and associated behaviors on threats to security in connected places. The authors also argue that there is a need to investigate the models and tools currently being deployed by connected place design and management to understand and influence public perceptions and behaviors. Furthermore, the authors identify a need to investigate the complex relationship between the public and connected place managers and explore the patterns between specific connected place cyber security incidents and the methods used to influence public perceptions.

1 Introduction

Connected places present new and potentially urgent challenges for their designers and managers: as the public interacts with Data-Driven Technology (DDT) and the Internet of Things (IoT) within built environments, it is unknown to what extent their perceptions and behaviour present security and sustainability threats. These technologies often present the promise of improving the quality of life for public users of these places. However, the actual public perceptions of these technologies, their acceptability, safety and trustworthiness are complex. Common challenges include the wide range of attitudes towards surveillance and personal privacy [1, 2, 3, 4, 5], varied awareness and appetites for the technologies and associated risks; and the intertwined relationship between the way the public perceives a connected place and the way they perceive connected place managers in broader or other contexts, for example, local and central governments.

We conducted this systematic literature review to provide an overview of current research addressing the research question: "*To what extent do public perceptions of connected places affect the security and sustainability of connected places?*". It was commissioned by the Department for Science, Innovation and Technology (DSIT) to provide a state of the current knowledge, review themes in literature, and inform future research concerning this emerging challenge.

The emerging and diverse range of applications of connected places informed the selection of a systematic review process combined with a narrative discourse analysis of findings. We seek to understand how research relating to connected places' perceptions, security and sustainability is developing while identifying all potentially relevant research problems which have implications for this complex, socio-technical challenge. The review is an important step in understanding the opportunities and threats that public perceptions present to the security and sustainability of connected places. We aim to inform connected place managers and designers with a better understanding of the way the public may behave within connected places, to provide a foundation and recommendations for specific future research questions. We also intend to identify any evidence of effective tools which connected place managers and designers can deploy to understand and positively influence public perceptions and security behaviours.

1.1 Taxonomy

In this section, we provide a brief overview of the key terms needed to establish the scope and motivations of this research.

Connected Places

Due to the policy-oriented motivation of this research, we have used the Department for Science Innovation and Technology's (DSIT) definition of 'connected place', provided in their Secure Connected Places Guidance [6], informed by both the National Cyber Security Centre (NCSC) and the Centre for the Protection of National Infrastructure (CPNI). This ensures our research is as applicable to those managing, regulating and designing connected places as possible. DSIT works to the NCSC definition of connected places:

> "A community that integrates information and communication technologies and IoT devices to collect and analyse data to deliver new services to the built environment, and enhance the quality of living for citizens."[2]

Secure

This research is informed by NCSC's description of cyber security:

> "Cyber security's core function is to protect the devices we all use (e.g., smartphones, laptops, tablets, and computers), and the services we access - both online and at work - from theft or damage. It is also about preventing unauthorised access to the vast amounts of personal information we store on these devices, and online."[3]

[2] https://www.ncsc.gov.uk/collection/connected-places-security-principles
[3] https://www.ncsc.gov.uk/section/about-ncsc/what-is-cyber-security

Sustainable

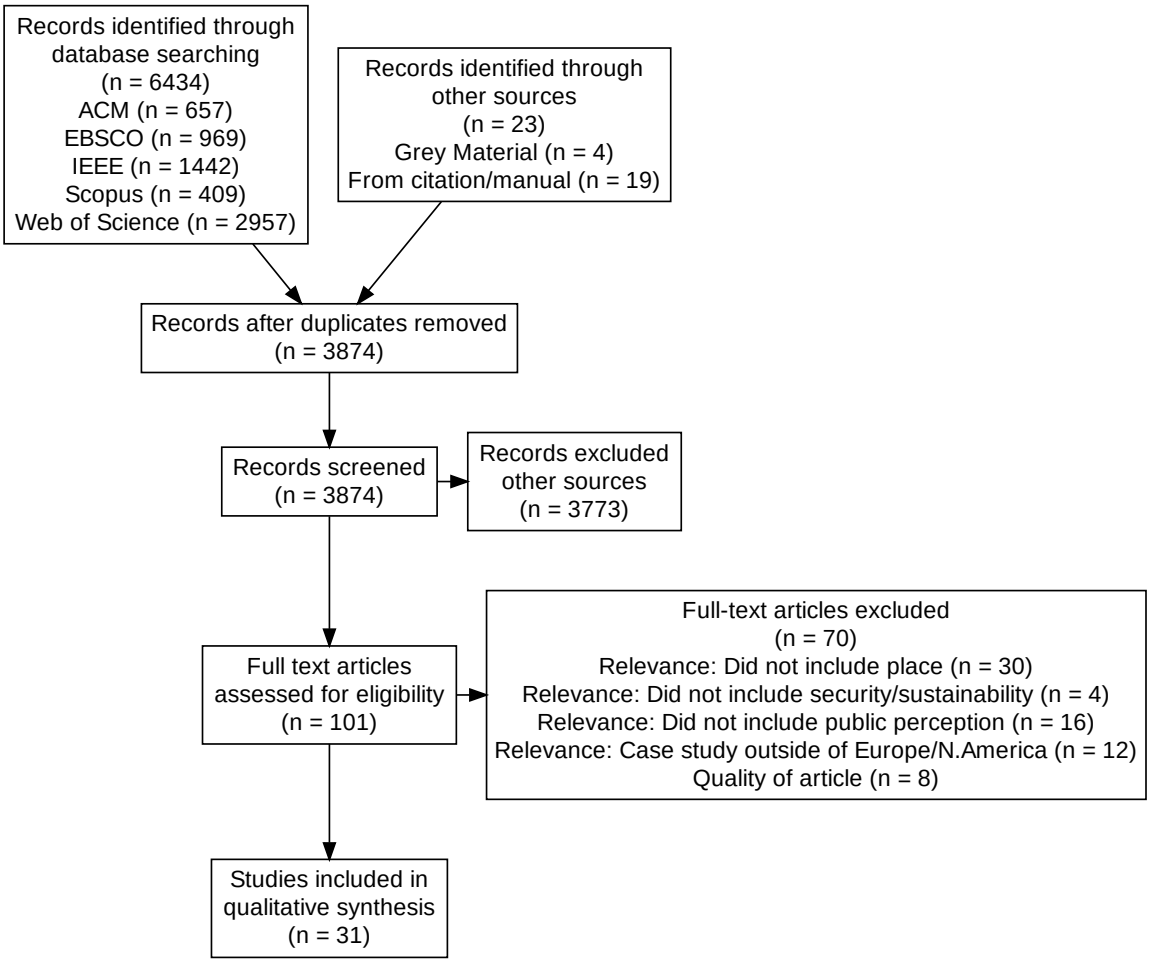
The authors, in consultation with DSIT's Secure Connected Places Team, define a sustainable connected place as a connected place which continues to deliver new services to the built environment and enhance the quality of living for citizens indefinitely. To achieve sustainability, a connected place must be able to withstand attacks, be resilient to these attacks in the way it responds and rebuilds, and be accepted and adopted by citizens within it.

2 Methods

The authors followed a systematic approach[4], using the PRISMA framework [7], when conducting the search and eligibility screening for this review. We then conducted a qualitative thematic analysis to synthesise findings and report patterns or contradictions in the literature. Our search strategy included a search for grey literature relevant to connected places in the UK. This involved using the query syntax as a web search and consulting policy, guidance and research on government websites.

Taking into account the emerging nature of this research challenge, we developed a robust protocol to search, identify, and select relevant publications. The protocol was pilot-tested and calibrated prior to data collection by the authors. To achieve comprehensiveness and systematic rigour, relevant publications were retrieved using the search strategy shown in Fig. 1. This strategy is discussed in detail in Section 2.1.

Figure 1: PRISMA Flow Diagram.



[4]Snyder, Hannah. "Literature review as a research methodology: An overview and guidelines." Journal of business research 104 (2019): 333-339.

2.1 Search Strategy

After conducting some initial test searches of likely databases, we were able to refine our query syntax and eligibility criteria to ensure a comprehensive and focused data set was generated. The tests revealed immediately that it is very rare for research relevant to connected places to use the term 'connected places' and that the wide variety of types of connected places would require us to construct search terms that looked for multiple specific research problems, as opposed to one broad area. Similarly, the multifaceted and socio-technical nature of public perceptions is rarely tackled directly in the literature. Therefore, we had to identify the key terms that could possibly uncover research relating to public perceptions. These key terms were developed in consultation with DSIT to ensure we found research that was within the scope of the policy challenge (cf. Table 1).

Table 1: Search Syntax.

Constant Concept	**Variable Concept**
`((public OR user N5 trust* OR perspective* OR attitude* OR perception* OR awareness OR accept*) AND (‘‘cyber?security" OR cybersecurity))`	`Cit*; place; smart; connected; hospital; airport; station; centre OR center; port; prison; "social housing"`

This syntax passed sensitivity testing in which we assessed the range and quality of articles retrieved by early searches.

2.2 Information Sources

The databases searched were EBSCO, IEEE, ACM, Web of Science and Scopus. These databases were selected to provide a broad and comprehensive list of possible articles. Each database was manually searched with all articles found using the above query syntax added to a shared reference manager. All researchers conducted manual web searches using the query syntax for relevant grey literature. Government websites and those referenced by government guidance were also searched for relevant literature. All relevant grey literature was added to the library at this stage and screened for relevance and eligibility. At a later stage, after eligibility screening, additional articles were found via citations and added to the library if they met the eligibility and relevance criteria.

2.3 Eligibility criteria

Search results were screened by at least two different researchers against eligibility criteria agreed upon in consultation with DSIT's Secure Connected Places Team:

- Language: Full-text article written in English
- Title relevance: Mentions user perceptions or a variable of; an aspect or type of connected place; and, an aspect or synonym of cyber security and/or sustainability.
- Abstract relevance: Mentions user perceptions or a variable of; an aspect or type of connected place; and, an aspect or synonym of cyber security and/or sustainability.
- Geography of case studies: Given the UK policy orientation of this reviews purpose the authors agreed with DSIT's Secure Connected Place Team that only case studies in the UK, Europe and North America would be eligible for inclusion

A large number of articles were excluded at the stage of screening by title or abstract (3773) due to the nature of our broad search terms, designed with the aim of finding articles relevant only to specific types of connected places; or which, while not public perceptions oriented referenced another article which was.
Articles still included after the above screening were included in a full-text eligibility evaluation, which evaluated the relevance and quality of an article. At least two researchers conducted an independent full-text assessment of each article, marking articles for inclusion or exclusion, and disputes were discussed throughout the research team at weekly meetings.

2.4 Mapping Workshops

When analysing the articles, the authors extracted the text of any evidence that addressed our research question to a shared Miro board. All the arguments and evidence collated on the Miro board in this way were then independently evaluated for relevance by all authors. The authors then conducted an affinity mapping exercise in which text extracts were grouped by overall argument. Connecting lines were drawn between arguments that supported or contradicted each other. This was conducted over two workshops, one in-person and one online, with authors who also worked on the Miro board independently between these workshops. Then, clusters of extracts that supported or contradicted arguments were gathered together into broader groups, often relating to broader research problems within our overall research question. Our findings have been presented against these groups. The authors then worked collaboratively online to write the narrative discourse which is presented in our findings section 4.

3 Results

3.1 Background Characteristics

In this literature review, we screened 3874 articles before selecting 27 journal and conference articles and 4 pieces of grey literature which contained qualitative information on the extent to which public perceptions of connected places affect the security and sustainability of connected places.

The existing literature, both academic and grey, is predominantly technology-focused with regard to connected place security and sustainability, despite the focus on public perception of our search. Four literature reviews within selected articles agree that the number of articles investigating the security impact of public perceptions is still relatively small [1, 8, 9, 10]. Those which have investigated this tend to orientate more around privacy than security [10]. Case studies included in our articles lack attention to safety, sustainability, equity and resilience of connected places [9].

3.1.1 Characteristics of Results against Query Syntax Variables

Throughout the full text assessment of the articles, the reviewers tagged the articles against the query syntax. 24 articles (77%) were tagged with #cyber security. All those not tagged with #cybersecurity were identified by citations from articles that reference cybersecurity.

Each article was tagged against the query syntax terms. Of the variables relating to public perspectives #Awareness (24%), #Trust (19%) and #Perspective (17%) were the three highest in frequency (Fig. 2). #Smart (41%) and #Cit* (33%) dominate tags that refer to place-based variables in the query syntax (Fig. 3). This represents the extent to which urban environments dominated the examples of connected places disussed within the literature.

3.1.2 Characteristics of Results by Connected Place Feature

The great majority of articles (21) included in our review focused on urban environments (Fig. 3). However, all articles referred to a wide range of technologies underpinning connected places.

3.1.3 Characteristics of Results by Geographic Focus

Reviewed articles which did focus on a specific geography, i.e., those with a case study or survey-oriented methodology, researched connected places in either the UK (8), Europe (7), or North America (1). The remaining articles had no specific geographic focus.

Figure 2: Public Perspective Variable Tags.

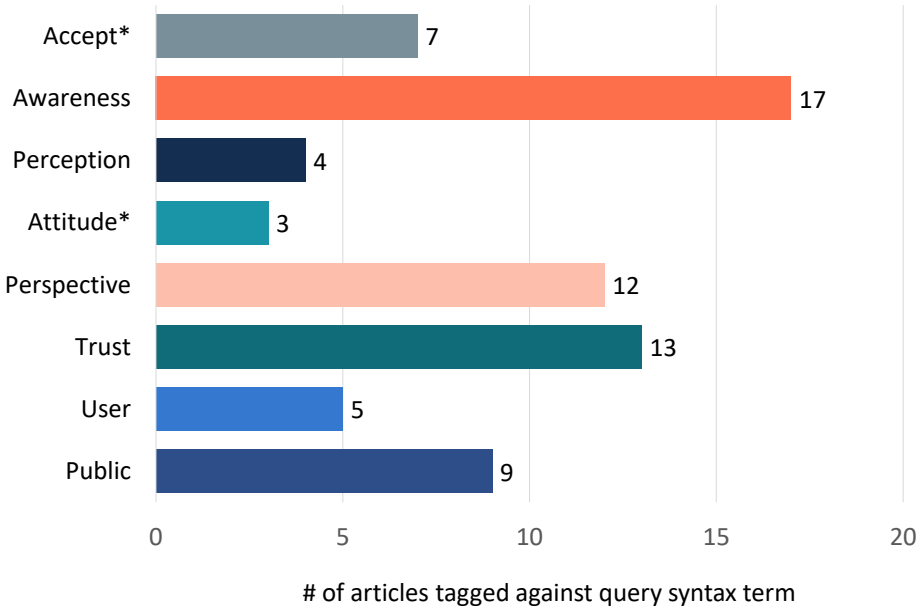


Figure 3: Connected Place Variable Tags.

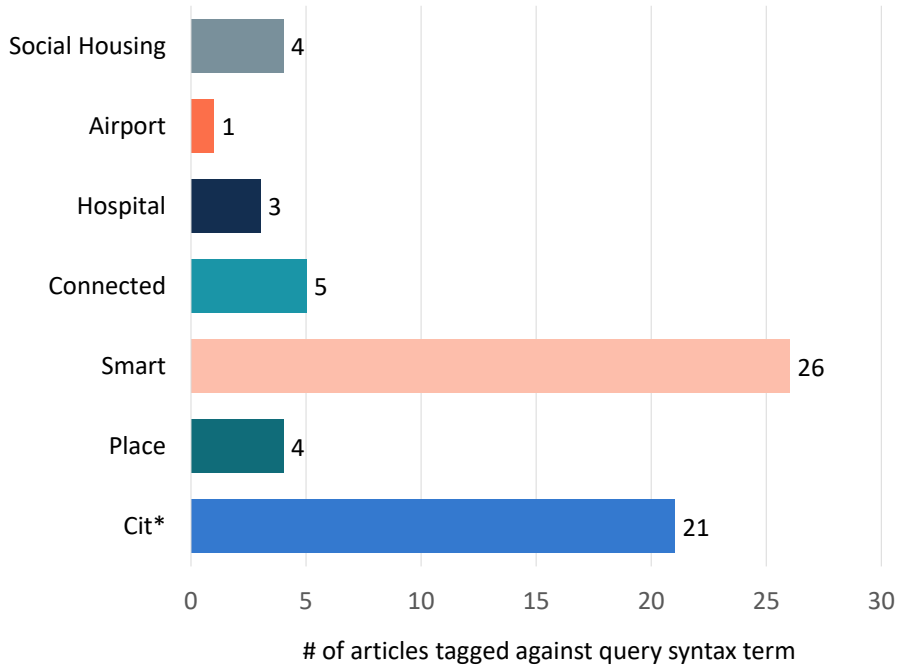


Table 2: Technologies referenced.

Parent Category	Subcategory 1	Subcategory 2	Frequency
Application	Smart Transport		32
Application	Sensors		27
IoT devices			19
Connectivity & Data Transport	Radio Network	Wi-Fi	17
IoT Devices	Sensors	Environmental Monitoring	17
Application	E-Governance		14
IoT devices	End Point Devices	Smartphone	14
Application	Smart Lighting		13
ICT			13
IT Security			12
Application	Smart Homes		10
Application	Smart Surveillance Systems		9
IoT devices	Wearable	Wearables	9
Application	Smart Parking		8
Application	Smart Healthcare		8
Application	Smart Building		8
Big Data	Artificial Intelligence		8
Connectivity & Data Transport	Mobile Network	5G	8
IT Security	Authentication	Smart Cards	7
Data Management	Data Storage	Cloud	6
Big Data			5
IoT devices	End Point Devices	PC	5
Application	Surveillance System	CCTV	4
Application	Energy Infrastructure		4
Application	Smart Delivery Systems		4
Connectivity & Data Transport	Radio Network	Bluetooth	4
Connectivity & Data Transport	Satelite Navigation	GPS	4
Connectivity & Data Transport	Low Power Network	LoRaWAN	4
IoT devices	Smart Meters		3
IoT Platforms	Urban-Scale Iot Platforms		3
IT Security	Contactless	RFID	3
IT Security	Contactless	NFC	3
Service			3
Application	Actuators		2
Connectivity & Data Transport	ISP		2
Software	App	Waze	2
Application	Smart Building	Air Conditioning (HVAC)	1
Application	Baggage Handling Systems		1
Application	BMS		1
Application	Environmental Monitoring	Connected Forest Project	1
Application	BMS	IEQ	1
Application	Digital Twins		1
Application	Surveillance System	Smart Alarm Systems	1
Blockchain			1
Connectivity & Data Transport	Radio Network	Free Open Networks	1
Connectivity & Data Transport	Radio Network	NB-IoT	1
Connectivity & Data Transport	Low Power Network	Weightless	1
Connectivity & Data Transport	Network Layer	Zigbee	1
Connectivity & Data Transport	Low Power Network	NB-IoT	1
Connectivity & Data Transport	Network Hardware	VSAT	1
Connectivity & Data Transport	Protocol	CoAP	1
Connectivity & Data Transport	Radio Network	CWN	1
Connectivity & Data Transport	Protocol		1
Connectivity & Data Transport	Mobility Service	V2X	1
Connectivity & Data Transport	Mobility Service	VANETS	1
Connectivity & Data Transport	Protocol	DNS	1
Cyberspace	User Experience	VR	1
Cyberspace	User Experience	AR	1
Data Management	Data Management	CKAN	1
Data Management	Data Storage	USB	1
Edge Computing	Edge And Fog Computing		1
ICT	Microcontrollers		1
IoT devices	End Point Devices	Smart Batteries	1
IoT devices	End Point Devices	EUT	1
IoT devices	End Point Devices	Smart Plugs	1
IoT devices	Programmable Logic Controllers (PLCs)		1
IoT Platforms	WoTKit		1
IT Security	Authentication	PIN	1
IT Security	Authentication	MFA	1
IT Security	Encryption	PIN	1
IT Security	Authentication	readers	1
Service	Financial Service	E-Banking	1
Service	LBS provider		1
Software	App	Otonomo	1
Software	App	Corona-Warn-App	1
Software	Mobility Service	Smart Back-office Systems	1
Software	Control System Architecture	SCADA	1

4 Findings

This section captures the authors' synthesis of the literature concerning the ways in which public perceptions of connected places affect the security and sustainability of connected places, both theoretical and empirical findings, to build a conceptual framework. The authors bring together related concepts to provide a broader understanding of the research problem.

4.1 Public Perceptions Influencing Public Security Behaviours

It is important to note that the literature suggests that the majority of the public will be oblivious to connected places [11], let alone desirable security behaviours within them [5, 12]. The literature suggests that public perceptions and security behaviours in connected places are being influenced by many different things: the value offered by connected place technology [13]; the clarity of risks and security procedures communicated [14, 15]; the ability to express concerns and participation in design and development [15, 16, 2, 11]; perceptions of privacy and risk [17, 2, 1]; trustworthiness [18, 12, 19, 10]; and, the type and purpose of data collection [2, 5].

Connected place users might be more willing to accept security and privacy risks when they perceive a space to be delivering high value, functionality and convenience [13]. Fayoumi et al [14] present a correlation between the explanation of security and privacy issues in an IoT system and resulting enhanced user awareness and ability to avoid risks. However, the wide-ranging pre-existing levels of awareness amongst public users of connected places make a one-size-fits-all approach to the explanation of security and privacy issues challenging. Some argue that many members of the public have a good understanding of network and data security processes but with low awareness of threats [20] or the information being shared by their devices in a connected place [12, 5].

A further complication is the degree to which the public perceives the connected place to be actively protecting them from these harms, which could lead to neglecting cyber security because they feel protected and that controls are being taken care of elsewhere [21]. This presents a challenging puzzle for connected place designers and managers who may rely on members of the public feeling protected for the acceptance, use and sustainability of their places. Similarly, while the public becoming more aware of threats and more risk averse is no doubt an attractive goal for connected place managers, this knowledge of risk aversion may result in an unwanted consequence of residents avoiding connected places or specific technologies within them [17].

User behaviour relating to privacy and cyber security can become more secure the more personal they consider the data being gathered to be, as their perception of risk increases. If members of the public are hesitant to share personal information in government-management interfaces, as they often are [1], then it is likely they would have similar concerns if asked to actively consent to data being collected in a connected place they perceive to be government managed. Other privacy factors which affect a user's perception of security are: the purpose for which data is collected, i.e. service or surveillance [2]; which data is collected, i.e. personal or impersonal [2], and the context data sharing is taking place within, for example, users are more willing to share data in the event of a friend being endangered [5]. Notable in its absence is any reference to public concerns regarding where their data is stored.

It is not known to what extent behaviours in a 'smart home' environment are transferable to a connected place in the public. Indeed, it is also not known to what extent security behaviours in a connected place are influenced by behaviours and experiences in cyberspace. Taher et al [22] suggest that when using 'smart campus buildings', students' privacy concerns are influenced by their experiences and knowledge in other computing contexts and that similar consent controls would be desirable. Other authors commented on the influence of the personal experience of cyber-attack in cyber-space, as opposed to in a cyber-physical environment such as a connected place [22]; demographic differences such as age and gender [5, 23], and pre-existing awareness of cyber security vulnerabilities and controls [20]. Although none of these findings, at an article-by-article level or across the literature as a whole, is comprehensive enough to draw general or applicable conclusions from.

Many of the above articles refer to privacy and security concerns that make it less or more likely for a member of the public to engage with a connected place. Willemsen [24] comments that increased

security measures come with increased friction for the user experience, potentially affecting the acceptability of a connected place and increasing the likelihood of a user disengaging. Van Twist et al [1] argue that rejection of a connected place can be considered a threat to security itself as data may become unreliable and in extreme instances rejection related to mistrust can lead to the public themselves becoming a threat to security. This is explored further in section 4.2.3.

4.2 Perspectives on Public Security Behaviours Affecting Security and Sustainability of Connected Places

4.2.1 Reasons public perceptions of connected places affect connected place security and sustainability

Hernandez-Ramos et al [12] point to examples such as the Mirai botnet attack to demonstrate the potential for compromised IoT devices to be used to launch attacks against ICT systems and critical infrastructure. In their example, they suggest that a single citizen's lack of awareness, and resulting poor cyber security hygiene, could be a threat to the security of the general public and systems within a smart city [12].

Habib et al found, through a survey of 1,444 Denton residents, that "*approximately 55% of trust in technology by residents is related to their perception of security and privacy, which in turn influences their trust and adoption of smart-city services*" [17, p. 618]. Smart city users value safety and security, supporting increased regulation to this end, and residents are more likely to show interest in using smart city services when they are innovative and privacy is assured [17].

While privacy and security are intertwined, the literature suggests that privacy appears to matter slightly more than cyber security to public users of connected places [11]. Zoonen [2] argues for the importance of recognising citizens' privacy concerns in order to sustain support and participation. Habib et al [17] similarly identify perceived cyber security to be key to citizen acceptance, and place cyber security by association, with citizens valuing safety and public security, quality of information and services quality and increased government regulation. However, Van Twist [1] argues that over-surveillance, often motivated by public safety, can lead to citizens rejecting a connected place, negatively affecting its sustainability. Manfreda et al [15] list perceived privacy, innovation concept and service quality as key factors of acceptance, with cyber security notably absent. This is an area needing further research as the above potentially contradicts the understanding that those who experience a data breach are more privacy and security conscious as a result.

Security measures creating friction with members of the public's experience need to be addressed within the context of a connected place. Willemsen [24] presents airports as public spaces in which the trade-off between security and friction is more actively considered by place managers given the need to manage passenger comfort, processing efficiency and security. Airports are, however, places in which security and safety are arguably more critical than other places such as a town centre or social care environments, and in which the public has come to expect security checks. Manfreda et al [15] argue that it is "*immensely important to analyse the trade-off between city's effectiveness and its security*" [15, p. 277].

4.2.2 Specific technical vulnerabilities to connected place security and sustainability which affect and are affected by public perception

,

Vanolo [4] argues that personal devices are essential for the sustainability of connected places given the way an intelligent environment receives feedback from residents' smartphones. However, based on the literature surveyed, this review suggests that end-user devices present the greatest security threat to connected places [19, 5, 2, 13] with many users' perceptions of the importance of security being very low [12, 5], and often not maintaining security updates and patches. Herbert et al [5, p. 283] cite a 2019 study by Ali et al [5] in which more than half of 3,000 global smartphone users surveyed were

[5] Ali, Md Nawab Yousuf et al. "Security and privacy awareness: A survey for smartphone user." Editorial Preface From the Desk of Managing Editor 10, no. 9 (2019).

not aware of smartphone security and privacy. A result which correlates with the findings of Ipsos Mori's "Consumer Attitudes Towards IoT Security" Report [6], for example, that only 24% of Wi-Fi router owners have changed the password since purchase, or that 20% report checking the minimum support period when purchasing a smart device. It is debatable, however, whether this means that place managers should consider them their primary focus for security controls, given that public perceptions may affect the way they behave on and with their devices; or, whether place managers should design and run connected places in a way that is resilient to user behaviour on their devices, through extreme limitations of user access for example. Vitunskaite et al [19] argue that the only way to control user-generated vulnerabilities of connected places is to control what is on the market; we argue though that this would not control a users behaviour with a device, in particular their likelihood to maintain antivirus or security updates and patches [18].

As well as providing feedback and creating 'citizen-sensors' in the way Vanolo [4] describes, personal devices are often the access point for the public to access public Wi-Fi, another technological feature of connected places, at the network layer, included in multiple articles. In a university-based study Papic [25], found that 43% of 110 students at Osijek University, Croatia never feel safe when using public Wi-Fi. The manner in which devices remember and automatically reconnect to Wi-Fi may present vulnerabilities to outsider attacks [18], with user behaviour being key in addressing this weak link in connected place infrastructure, especially when users frequently misjudge the risky situations in the wild [23]. Willemsen [24], writing about the arguably more security-critical environment of an airport, argues for limiting the possibility for the public to access connected place networks, both through reducing access points and by separating public networks from internal networks.

There is a question as to whether public Wi-Fi is a threat to the connected place, the user within a connected place, or both, given the data some users will be willing to share on insecure networks [12]. Similarly, are devices a point of a security vulnerability in a connected place system, or a point of data leakage, privacy threat and over-surveillance for the member of the public within a connected place?

The final technology to feature to a notable extent was smart cards. Smart cards present a good example of the assessments users make when deciding on whether or not to adopt new technology in a connected place, that of perceived usefulness, i.e. value, and perceived security [26]. Indeed they are seen by citizens, according to Bellanche-Gracia [26], as guaranteeing secure transmission of sensitive data, unlocking connected places services and infrastructure. Similarly, the present smart cards serve as a good example of how connected places may "*depend more on citizens' perceptions of privacy and security risks than on the actual technological, design, or policy guarantees of privacy*" [26, p. 474].

Notably absent from the literature are less user-orientated IoT architectures, such as sensors, Low Power Wide Area (LPWA) networks or the processing and application layers in general as can be seen in (fig). The latter three of these layers are not public-user-oriented and therefore not surprising in their absence, but sensors are often extremely public-user-oriented, if in a passive way with regards to user experience, i.e. the user may be unaware of the engagement. The literature in which they are featured [19, 1, 3] describes what happens when members of the public take far from passive actions to reject sensors in connected places, as we describe in the next section.

4.2.3 The public as a threat to connected places security and sustainability

Public users are positioned within the literature as influential threats [1, 12] to connected place security and sustainability in various ways:

- Naive or optimistic users who may unintentionally threaten a place's security through inaction [13] or being victim to the influence of bad actors, in particular via social engineering [27];
- Allies of the place managers who are aware of threats [13], and keen to contribute to security efforts. Some articles draw a connection between trust in connected places and trust in government in general, with influence travelling in both directions [10, 17, 18];

[6] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/978685/Consumer_Attitudes_Towards_IoT_Security_-_Research_Report.pdf

- Malicious actors themselves due to the ease of causing significant damage though low-skilled cyber attacks [19, 3] or rejecting surveillance through non-technical tampering, data obfuscation or vandalism [1, 3];

Isin and Ruppert [3] call for a new type of digital citizenship in which the complexities of the above can be discussed in a way which considers the multiple possible roles any member of the public may play at any one time in a connected place.

4.2.4 Public perspectives before, during, and after a cyber-attack on a connected place

A number of different articles focus on the public at different parts of a cyber security timeline: before, during and after an attack. The vast majority focus on the role of the public as part of a socio-technical system working together, though not necessarily knowingly, to protect all parts of the system from attack [5, 10, 28, 12]. A few articles [20, 9, 21, 17] explore public perceptions, and by association behaviour, during an attack, and suggest that the public's role in the system increases significantly during this time: minimising the impact of an attack in terms of technical damage [20] but also keeping themselves safe from physical harm due to an awareness of the way an attack will affect a places infrastructure and the mitigating actions they may have to take. This becomes especially relevant when considering attacks which may not manifest in ways that affect a physical element of the place, i.e. working machines or environmental conditions, but instead might aim to spread misinformation. Public perceptions and the ability to distinguish reliable data are very important during an attack of such, especially if this attack takes place during an existing crisis such as natural disasters or warfare [9]. Finally, the way in which the experience of an attack affects the public perceptions of a connected place's security is disputed. Zwilling [21] argues it has no effect, while Habib [17] argues that it can increase rejection of connected places and present a future threat to a place's security and sustainability in itself.

4.3 The Relationship between Connected Places, their Managers and Public Perceptions, and How this Affects Security and Sustainability

4.3.1 The various definitions of users, place managers and the public in connected places cyber security research and guidance

Related to the need for research on the multiple positions and motivations a user may manifest [18]., there is also a need to better define users in general. A great deal of literature excluded from this review used the term 'user' to refer to operators and managers of connected places. Referring to them as 'users' of the connected place as a tool to meet their needs, often positioning them as a customer of the designers, developers and manufacturers of connected places technologies. This was also common across the grey materials with government guidance using the term 'user' to refer exclusively to place managers and operators [29, 30, 28].

4.3.2 The influence of connected place managers and their relationship with the public

Literature is divided on the influence a place manager can have on public perceptions and behaviours. Cilauro [28] points towards the significance of the technical factors or process factors in securing the connected place to suggest that people factors matter not. However, Vitunskaite et al [19] point to the actions of fourth and fifth parties, i.e. those producing devices which enter the connected place, as being so critical to security that managers are powerless to influence these risks. Cilauro [28] warns against focusing on user-oriented concerns as it may lead to over-investment in end-point security. Cilauro [28] is also critical of councils in particular, reporting that a connected place commissioner believed "*most councils do not know enough about technology or cyber security to procure technology*" [28, p. 52]) and suggests this may well apply across the public sector. Others suggest that even if public perceptions do matter, place managers are helpless to influence them and should not waste their time trying. Others on the other hand suggest that place managers must take a 'user-centric' approach to fully understand and overcome connected place security threats [18]. The gap in research

on the influence of public perceptions was raised by four articles [10, 1, 15, 9]. Van Zoonen [2] argues that connected place managers must acknowledge public concerns about privacy in order to maintain their support and participation.

A few articles take a very user-focused view of the privacy and security of connected places. They argue that privacy and security is a human right [31, 15, 10] and that it is the duty of government to regulate connected places in a way that protects citizen data [8]. They argue that it is the place that is the risk to the citizen's security, not the citizen who is the risk to the place's security.

4.3.3 Tools, frameworks, models and methods that affect the influence of public perceptions on connected places' security and sustainability

Non-technical tools proposed by the literature include a five-dimensional model for citizens' privacy in smart cities [31], privacy impact assessments [2], cyber security culture frameworks [20] and citizen-centric approaches of connected place design and development such as living labs, crowdsourcing and citizen participation [2, 16].

Technical solutions include privacy-enhancing technologies [2] which align with the argument that citizen engagement is futile and the level of risk afforded to any public should be minimised to the point of irrelevance. Hernandez-Ramos et al [12] take this further by identifying the deployment of certified devices and systems, i.e., solutions which must be created far up the connected place supply chain from connected place managers influence, as ways to build citizens' trust in smart city services. They don't however articulate how you communicate that certification to citizens. Louw and Van Zolms [18] make an argument for end-user information security portals or dashboards, a very user-centric technical solution. They suggest that these can be used to communicate training and awareness content directly to users, "*seamlessly blending in with the Wi-Fi user journey*" [18, p. 125].

5 Discussion

Many of the articles reviewed point to the heightened importance of public perceptions and behaviour during a cyber-attack on a connected place [5, 10, 28, 12, 20, 9, 21, 17]. However, there is no consensus on how perceptions and behaviour can be influenced to minimise the impact of, and expedite recovery from, a cyber-attack. This question requires further research, which can deliver up-to-date and technology-specific recommendations alongside best practices.

There is disagreement across the literature concerning who the public are, who connected place managers are, and how aligned both groups are with the aims of a secure and sustainable connected place. There is also a contradiction across the literature with regards to the aims of attempts to influence public perceptions and behaviours within connected places: are they to keep the place itself, i.e. its infrastructure, institutions and operations, safe; or should they protect the citizen's privacy and safety? While the answer can be both, many of the reviewed articles were orientated toward one or the other motivation and did not explore the relationship between the two.

Existing literature tended to reveal the following common assumptions within connected place managers:

- Connected places security is simultaneously in the interest of both the public and place managers and these interests are not ever in conflict.
- That public users and place managers are entirely separate groups, with no individuals taking dual roles within a connected place.
- That malicious actors are 'another' separate group to public users and place managers, and that users or place managers themselves always act in the interests of the other group and those within their own group.
- Place managers often focus on the technical requirements of privacy without adequate consideration of the social requirements. The technical aspects of privacy focus on the technical requirements (such as access control, data minimization) required to ensure privacy, while the

social aspects focus on the privacy preferences of the public users, the relationships between public users and how such relationships impact their privacy.

Finally, it is unclear whether the most significant security and sustainability risks exist in the way end-user devices are used and maintained, further up the supply chain in the standards and regulation applied to personal devices and the sensor and network technologies, or within the organisational culture and practice of those delivering connected places.

5.1 Trade-offs of Connected Places

Our analysis of the available literature regarding the influence of public perspective on the security of connected places revealed three trade-offs, which we discuss in this section.

5.1.1 Secure Places Vs Friction-less Experiences

If connected places provide convenient solutions, members of the public may accept security and privacy risks [13]. Moreover, the lack of awareness of how to avoid privacy and security risks results in the inability to prevent them [14]. This can lead to the lack of perceived authority over users' security and privacy, or so-called learned helplessness, which further strengthens users' preference towards functionality over privacy. However, we need end-users to actively take care of their security, not only for their sake but also for the sake of the system.

Users will utilise personal and public devices. Thus, connected places must develop a new side of security responsibility that would apply to both individual and collective privacy and security. However, one needs to remember the diffusion of responsibility, which can take place on the level of public vs other stakeholders, but also on the public level itself, among the end-users.

5.1.2 Sustainability vs Security

As pointed out in the section 4.2.2, personal smartphones are essential for the sustainability of connected places [4], but they are the biggest security threat [19, 5, 2, 13]. It needs to be clarified where the responsibility lies. As personal belongings, such as smartphones or smart cards, interact with connected places technology, it is still being determined who is responsible for citizens' security, when and how. Moreover, the perception of the citizens may change depending on whose responsibility it is.

5.1.3 Responsibility vs Authority

Along with transparency, clear responsibility and agency over security and privacy, there is a need to define the public users of connected places more clearly. The gap in research on the influence of public perception has been acknowledged; however, as we pointed out at the beginning of this section, stakeholders are not precisely defined. For example, if managers of connected places are end-users, it needs to be clarified. Furthermore, it is still being determined who has authority over data, and in what circumstances; too much on the government's side may be perceived as surveillance [1], and too little may be perceived as citizens are not getting their human right to security [31, 15, 10].

5.2 Limitations of This Study

Articles reviewed were often not directly addressing our research question, instead, they focus on citizen discontent within a connected place [1, 8, 9], often as a rejection to perceived over-surveillance, and not necessarily relating to the impacts this has on cyber security. Or they consider the role of a citizen in a connected place caught up in cyber-warfare [9]; or, consider public consultation as a necessary part of designing a working and secure connected place [10].

The diverse nature of connected places also generated results that are so wide-ranging, it is difficult to develop universally applicable recommendations for every type of connected place. Articles that did identify a connection between public perceptions and public security behaviours or their adoption

of connected places were often applying broad observations concerning perceptions of the internet and data-driven technologies.

5.3 Recommendations

The four literature reviews included in our review concur with some of our own findings. We agree with their recommendations for more research into mechanisms for assessing connected place threats relating to public perception [10]. We also identified a need to address the imbalanced focus towards technical solutions for connected place security [9] and to conduct more research on how perceptions influence the security behaviours of the public [1]. They all argue for a more socio-technical approach to this challenge, another argument we concur with having evaluated our own findings.

In addition, there is a need to explore models and tools for considering public perceptions and behaviours in connected place design and management. As well as methods through which connected place managers can influence both perceptions and behaviours, if at all. There were some participatory tools suggested by the literature [31, 2, 20, 16]. These need further testing in different contexts but the consensus of these arguments was that if a productive tool could be found, citizens would trust, accept and sustain connected places more if they felt themselves to be 'in the loop'. One article [19] described an open-source platform for connected place sensor data and management in Barcelona, however, they noted that cyber security did not feature frequently in this discourse. A worthwhile study would be to evaluate the tools used for consultation, education and behaviour influence within connected places of the same type, before then comparing the rate of security incidents in these places and analysing the causes of these compromises. Pastiche Scenarios of the future usage of connected places could help discover the nuances of recognized trade-offs. They could unravel different possibilities, which could further help in understanding when and how these trade-offs should be managed. Workshops with various stakeholders, including the public sphere, with different backgrounds, age groups and familiarity with the technology could be a step forward in the more inclusive adoption of connected places.

The lack of clarity on the complex relationship between members of the public and connected place managers requires more investigation. There is a need to conduct research with the public to explore: the way they position themselves within the systems keeping a connected place secure; and their perceptions of their personal data and whose responsibility the protection of this data is in a connected place context. There also is a need for research which researches patterns between specific connected place cyber security incident causes and the methods this place deployed, previously and since, to influence public perceptions.

Lastly, our findings suggest that a lack of awareness can lead to either a lack of acceptance [24] or security [12]. Additionally, because the public may be hesitant to share personal data, it is crucial to recognize when data can and should be anonymous. An analogous example can be the wide acceptance of security and privacy restrictions at the airport. However, such a level of privacy invigilation would not be widely accepted in other public places, such as parks.

6 Conclusion

This literature review highlights the potential importance of public perceptions and behaviours concerning the security and sustainability of connected places, and the need for further research to develop recommendations for minimising the impact of attacks. The authors note that there is a lack of consensus in the literature regarding the aims of attempts to influence public perceptions and behaviours within connected places, with some focusing on protecting the infrastructure and institutions of the place, while others prioritise the privacy and safety of citizens.

We reveal several assumptions within both connected place managers and researchers, including that the interests of the public and place managers are always aligned, that malicious actors are a separate group from public users and place managers, and that privacy is not a subjective personal value. The authors suggest that further research is needed to explore the complex relationship between members of the public and connected place managers in the context of cyber security.

We acknowledge the limitations of this study, including the fact that existing literature is often not directly addressing their research question, and that the diverse nature of connected places makes it difficult to develop universally applicable recommendations. However, we suggest several recommendations for future research, including the need to explore models and tools for considering public perceptions and behaviours in connected place design and management, and the need to conduct research with the public to explore their perceptions of their personal data and who is responsible for protecting it in a connected place.

Acknowledgement

This work has been supported by the PETRAS National Centre of Excellence for IoT Systems Cybersecurity, which has been funded by the UK EPSRC under grant number EP/S035362/1.

References

[1] Anouk van Twist, Erna Ruijer, and Albert Meijer. "Smart cities & citizen discontent: A systematic review of the literature". en. In: *Government Information Quarterly* (Jan. 2023), p. 101799. ISSN: 0740-624X. DOI: 10.1016/j.giq.2022.101799. URL: https://www.sciencedirect.com/science/article/pii/S0740624X22001356 (visited on 02/05/2023).

[2] Liesbet van Zoonen. "Privacy concerns in smart cities". en. In: *Government Information Quarterly*. Open and Smart Governments: Strategies, Tools, and Experiences 33.3 (July 2016), pp. 472–480. ISSN: 0740-624X. DOI: 10.1016/j.giq.2016.06.004. URL: https://www.sciencedirect.com/science/article/pii/S0740624X16300818 (visited on 02/11/2023).

[3] Engin Isin and Evelyn Ruppert. *Being Digital Citizens, Second Edition*. en-us. 2020. URL: https://rowman.com/ISBN/9781786614490/Being-Digital-Citizens-Second-Edition (visited on 02/20/2023).

[4] Alberto Vanolo. "Is there anybody out there? The place and role of citizens in tomorrow's smart cities". en. In: *Futures* 82 (Sept. 2016), pp. 26–36. ISSN: 0016-3287. DOI: 10.1016/j.futures.2016.05.010. URL: https://www.sciencedirect.com/science/article/pii/S0016328716300301 (visited on 01/24/2023).

[5] Franziska Herbert, Gina Maria Schmidbauer-Wolf, and Christian Reuter. "Who Should Get My Private Data in Which Case? Evidence in the Wild". In: *Proceedings of Mensch und Computer 2021*. MuC '21. New York, NY, USA: Association for Computing Machinery, 2021, pp. 281–293. ISBN: 978-1-4503-8645-6. DOI: 10.1145/3473856.3473879. URL: https://doi.org/10.1145/3473856.3473879 (visited on 02/09/2023).

[6] UK Government. *Secure Connected Places Guidance*. Mar. 2023.

[7] Matthew J Page et al. "The PRISMA 2020 statement: an updated guideline for reporting systematic reviews". In: *International journal of surgery* 88 (2021), p. 105906.

[8] Albert Meijer and Manuel Pedro Rodríguez Bolívar. "Governing the smart city: a review of the literature on smart urban governance". en. In: *International Review of Administrative Sciences* 82.2 (June 2016). Publisher: SAGE Publications Ltd, pp. 392–408. ISSN: 0020-8523. DOI: 10.1177/0020852314564308. URL: https://doi.org/10.1177/0020852314564308 (visited on 01/24/2023).

[9] Simona R. Soare. "Smart Cities, Cyber Warfare and Social Disorder". In: 2020. URL: https://www.semanticscholar.org/paper/Smart-Cities%2C-Cyber-Warfare-and-Social-Disorder-Soare/aad6acda0943b7f229ace20f9d9c1357a23d9e25 (visited on 02/20/2023).

[10] Chen Ma. "Smart city and cyber-security; technologies used, leading challenges and future recommendations". en. In: *Energy Reports* 7 (Nov. 2021), pp. 7999–8012. ISSN: 2352-4847. DOI: 10.1016/j.egyr.2021.08.124. URL: https://www.sciencedirect.com/science/article/pii/S2352484721007265 (visited on 02/05/2023).

[11] Vanessa Thomas et al. "Where's Wally? In Search of Citizen Perspectives on the Smart City". en. In: *Sustainability* 8.3 (Mar. 2016). Number: 3 Publisher: Multidisciplinary Digital Publishing Institute, p. 207. ISSN: 2071-1050. DOI: 10.3390/su8030207. URL: https://www.mdpi.com/2071-1050/8/3/207 (visited on 01/11/2023).

[12] Jose L. Hernandez-Ramos et al. "Security and Privacy in Internet of Things-Enabled Smart Cities: Challenges and Future Directions". In: *IEEE Security & Privacy* 19.1 (Jan. 2021). Conference Name: IEEE Security & Privacy, pp. 12–23. ISSN: 1558-4046. DOI: 10.1109/MSEC.2020.3012353.

[13] Scott Harper et al. "User Privacy Concerns in Commercial Smart Buildings1". In: *Journal of Computer Security* 30.3 (Jan. 2022), pp. 465–497. ISSN: 0926-227X. DOI: 10.3233/JCS-210035. URL: https://doi.org/10.3233/JCS-210035 (visited on 01/17/2023).

[14] A. Fayoumi et al. "The Cybersecurity Risks of Using Internet of Things (IoT) and Surveys of End-Users and Providers Within the Domiciliary Care Sector". In: *2022 Sixth International Conference on Smart Cities, Internet of Things and Applications (SCIoT)*. Journal Abbreviation: 2022 Sixth International Conference on Smart Cities, Internet of Things and Applications (SCIoT). Sept. 2022, pp. 1–7. DOI: 10.1109/SCIoT56583.2022.9953634.

[15] Anton Manfreda et al. "Citizens' Participation as an Important Element for Smart City Development". en. In: *Re-imagining Diffusion and Adoption of Information Technology and Systems: A Continuing Conversation*. Ed. by Sujeet K. Sharma et al. IFIP Advances in Information and Communication Technology. Cham: Springer International Publishing, 2020, pp. 274–284. ISBN: 978-3-030-64861-9. DOI: 10.1007/978-3-030-64861-9_25.

[16] Rodger Lea and Michael Blackstock. "Smart Cities: an IoT-centric Approach". In: *Proceedings of the 2014 International Workshop on Web Intelligence and Smart Sensing*. IWWISS '14. New York, NY, USA: Association for Computing Machinery, Sept. 2014, pp. 1–2. ISBN: 978-1-4503-2747-3. DOI: 10.1145/2637064.2637096. URL: https://doi.org/10.1145/2637064.2637096 (visited on 01/24/2023).

[17] Abdulrahman Habib, Duha Alsmadi, and Victor R. Prybutok. "Factors that determine residents' acceptance of smart city technologies". In: *Behaviour & Information Technology* 39.6 (June 2020). Publisher: Taylor & Francis _eprint: https://doi.org/10.1080/0144929X.2019.1693629, pp. 610–623. ISSN: 0144-929X. DOI: 10.1080/0144929X.2019.1693629. URL: https://doi.org/10.1080/0144929X.2019.1693629 (visited on 01/24/2023).

[18] C Louw and B Von Solms. *Free Public Wi-Fi Security in a Smart City Context-An End User Perspective*. English. Ed. by DB Rawat and KZ Ghafoor. SMART CITIES CYBERSECURITY AND PRIVACY. Pages: 127. 2019. ISBN: 978-0-12-815033-7. DOI: 10.1016/B978-0-12-815032-0.00009-3.

[19] Morta Vitunskaite et al. "Smart cities and cyber security: Are we there yet?A comparative study on the role of standards, third party risk management and security ownership". en. In: *Computers & Security* 83 (June 2019), pp. 313–331. ISSN: 01674048. DOI: 10.1016/j.cose.2019.02.009. URL: https://linkinghub.elsevier.com/retrieve/pii/S0167404818310423 (visited on 01/24/2023).

[20] Anna Georgiadou et al. "Hospitals' Cybersecurity Culture during the COVID-19 Crisis". en. In: *Healthcare* 9.10 (Oct. 2021). Number: 10 Publisher: Multidisciplinary Digital Publishing Institute, p. 1335. ISSN: 2227-9032. DOI: 10.3390/healthcare9101335. URL: https://www.mdpi.com/2227-9032/9/10/1335 (visited on 02/09/2023).

[21] M Zwilling et al. "Cyber Security Awareness, Knowledge and Behavior: A Comparative Study". English. In: *JOURNAL OF COMPUTER INFORMATION SYSTEMS* 62.1 (Jan. 2022), pp. 82–97. ISSN: 0887-4417. DOI: 10.1080/08874417.2020.1712269.

[22] C Morisset R Taher M Mehrnezhad. ""I feel spied on and I don't have any control over my data": User Privacy Perception, Preferences and Trade-offs in University Smart Buildings". In: 12th International Workshop on Socio-Technical Aspects in Security, 2022. 2023. URL: https://scholar.google.co.uk/citations?view_op=view_citation&hl=en&user=LPqJnMMAAAAJ&sortby=pubdate&citation_for_view=LPqJnMMAAAAJ:RGFaLdJalmkC (visited on 01/17/2023).

[23] Nissy Sombatruang, M. Angela Sasse, and Michelle Baddeley. "Why do people use unsecure public wi-fi? an investigation of behaviour and factors driving decisions". In: *Proceedings of the 6th Workshop on Socio-Technical Aspects in Security and Trust*. STAST '16. New York, NY, USA: Association for Computing Machinery, Dec. 2016, pp. 61–72. ISBN: 978-1-4503-4826-3. DOI: 10.1145/3046055.3046058. URL: https://doi.org/10.1145/3046055.3046058 (visited on 02/20/2023).

[24] Bert Willemsen and Menno Cadee. "Extending the airport boundary: Connecting physical security and cybersecurity." In: *Journal of Airport Management* 12.3 (2018). Publisher: Henry Stewart Publications LLP, pp. 236–247. ISSN: 17501938. URL: https://search.ebscohost.com/login.aspx?direct=true&db=asn&AN=131227183&site=ehost-live&authtype=ip,shib&user=s1523151.

[25] A Papic, KK Radoja, and D Szombathelyi. "CYBER SECURITY AWARENESS OF CROATIAN STUDENTS AND THE PERSONAL DATA PROTECTION". English. In: *University of JJ Strossmayer Osijek*. Ed. by ML Simic. 2022, pp. 563–574.

[26] Daniel Belanche-Gracia, Luis V. Casaló-Ariño, and Alfredo Pérez-Rueda. "Determinants of multi-service smartcard success for smart cities development: A study based on citizens' privacy and security perceptions". en. In: *Government Information Quarterly* 32.2 (Apr. 2015), pp. 154–163. ISSN: 0740-624X. DOI: 10.1016/j.giq.2014.12.004. URL: https://www.sciencedirect.com/science/article/pii/S0740624X15000222 (visited on 02/11/2023).

[27] Ouidad Saber and Tomader Mazri. "SMART CITY SECURITY ISSUES: THE MAIN ATTACKS AND COUNTERMEASURES". In: *The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences* XLVI-4/W5-2021 (Dec. 2021), pp. 465–472. DOI: 10.5194/isprs-archives-XLVI-4-W5-2021-465-2021.

[28] Federico Cilauro. *THE CONNECTED PLACES MARKET IN THE UK*. en. Dec. 2021.

[29] *Connected Places Cyber Security Principles*. en. 2021. URL: https://www.ncsc.gov.uk/collection/connected-places-security-principles (visited on 01/24/2023).

[30] *Security-Minded approach to developing Smart Cities*. en. Feb. 2022. URL: %5Curl%7Bhttps://www.cpni.gov.uk/security-minded-approach-developing-smart-cities%7D (visited on 01/24/2023).

[31] A. Martinez-Balleste, P. Perez-Martinez, and A. Solanas. "The pursuit of citizens' privacy: A privacy-aware smart city is possible". English. In: *IEEE Communications Magazine* 51.6 (2013), pp. 136–141. ISSN: 0163-6804. DOI: 10.1109/MCOM.2013.6525606.