information

Systematic Review

How Do Public Perceptions Affect the Security of Connected Places? A Systematic Literature Review †

Agnieszka Dutkowska-Zuk [1], Joe Bourne [1], Chengyuan An [1], Xuan Gao [1], Oktay Cetinkaya [2], Peter Novitzky [3,4], Gideon Ogunniye [3], Rachel Cooper [1,*], David De Roure [2], Julie McCann [5], Jeremy Watson [3], Tim Watson [6] and Eleri Jones [7]

1 Lancaster University, Lancaster LA1 4YW, UK; j.bourne@lancaster.ac.uk
2 University of Oxford, Oxford OX1 2JD, UK; oktay.cetinkaya@eng.ox.ac.uk
3 University College London, London WC1E 6BT, UK; p.novitzky@ucl.ac.uk
4 Avans University of Applied Sciences, 4817 LL Breda, The Netherlands
5 Adaptive Emergent Systems Engineering, Imperial College London, London SW7 2BX, UK
6 The Alan Turing Institute, London NW1 2DB, UK
7 Independent Researcher, Bangor LL57 2DG, UK; elerij@gmail.com
* Correspondence: r.cooper@lancaster.ac.uk
† This work is an extended version of the report commissioned by the Department for Science, Innovation and Technology (DSIT) under the title: "To what extent do public perceptions of connected places affect the security and sustainability of connected places?".

Abstract: This systematic literature review explores the scholarly debate around public perceptions and behaviors in the context of cybersecurity in connected places. It reveals that, while many articles highlight the importance of public perceptions and behaviors during a cyberattack, there is no unified consensus on how to influence them in order to minimize the attack's impact and expedite recovery. Public perceptions can affect the success and sustainability of connected places; however, exactly how and to what extent remains unknown. We 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. Furthermore, 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. Lastly, we identify the requirements to investigate the complex relationship between the public and connected place managers, define all stakeholders clearly, and explore the patterns between specific connected place cybersecurity incidents and the methods used to transform public perceptions.

Keywords: connected places; public perception; cybersecurity; sustainability

Citation: Dutkowska-Zuk, A.; Bourne, J.; An, C.; Gao, X.; Cetinkaya, O.; Novitzky, P.; Ogunniye, G.; Cooper, R.; De Roure, D.; McCann, J.; et al. How Do Public Perceptions Affect the Security of Connected Places? A Systematic Literature Review. *Information* **2024**, *15*, 80. https://doi.org/10.3390/info15020080

Academic Editors: Jose de Vasconcelos, Hugo Barbosa and Carla Cordeiro

Received: 19 November 2023
Revised: 22 December 2023
Accepted: 23 January 2024
Published: 31 January 2024

1. Introduction

We, the authors, define connected places as a community that uses information and communication technologies with the Internet of Things (IoT) technology to "collect and analyse data to deliver new services to the built environment, and enhance the quality of living for citizens" following the National Cyber Security Centre's definition [1]. However, in addition to the promise of improved quality of living, these places also present new and potentially urgent challenges for their designers and managers: as the public interacts with data-driven technology (DDT) and the IoT within built environments, it is unknown to what extent public perceptions and behavior present security and sustainability threats.

One of the underlying technologies of connected places is the Internet of Things. Bibri defines IoT as:

> "a computationally augmented everyday environment where the physical world (everyday objects) and the informational world are integrated within the ever-growing Internet infrastructure via a wide range of active and smart data-sensing devices [...]." [2] (p. 234)

IoT is mainly associated with ubiquitous computing [2], and its most popular application is the concept of smart cities [3]. Connected places can be seen as IoT applications, as long as they work as part of smart city architecture [4].

Along with the growing threat of cyberattacks on IoT and edge devices, cybersecurity has become one of the most important areas of the Internet of Things (IoT). The purpose of cybersecurity is to protect digital devices, our personal data and the services we access through them. (This research is informed by NCSC's description of cybersecurity [5]: "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.") One of the challenges in IoT networks will be their security [6]. It applies to all aspects of IoT technology: hardware, network and data [7]. The user's responsibilities in the connected places' security are debatable. Hernandez-Ramos et al. [8] believe that technical solutions should not be an end user's concern in connected places. Vitunskaite et al. [9] express a similar sentiment, i.e., security should be embedded into IoT devices, and responsibility should not be placed on the people in the loop. On the other hand, Nizetic et al. found that the challenge we would face in smart cities is the operation of different sensing technologies, which "must be followed with the proper education of the population" [3] (p. 27). Connected places must withstand future attacks, be resilient and sustainable (in the way they respond and rebuild), and be accepted and adopted by citizens within them.

Therefore, in this review, we systematically investigate the concept of a *sustainable connected place* , as a connected place that continues to deliver new services to the built environment and enhance the quality of life for the public indefinitely. In this endeavor, the role of *connected place managers*, currently an under-investigated concept, which lacks a proper definition, is also the focus of our review. For the purposes of this research, we define place managers as any person with responsibility for the procurement, installation and maintenance of technologies; the handling, management, analysis and sharing of data; or, the design and enforcement of policy for the application of these technologies. It is currently unclear whether they should be responsible for the security of connected places or should be seen as users. In general, place managers are a new addition to scholarly debate and remain an overlooked area of research in the IoT field. There is a need to create tools for monitoring network operations [10] and their maintenance that could serve place managers.

While the research mentioned in this section discusses IoT environments in general, our work provides a new perspective as we specifically focus on the IoT in public spaces, where technology might not be visible at first sight to their users. Such a set-up creates a distinct synergy between public perception, cybersecurity and the sustainability of these places.

In summary, our systematic literature review (SLR) provides an overview of the current scholarly debate "*to what extent do public perceptions of connected places affect the security and sustainability of connected places?*". The actual public perceptions of these technologies, and their acceptability, safety, and trustworthiness, are increasingly complex. Our aim is to provide a systematic state of the current knowledge, review themes in the literature, and inform future research directions concerning this emerging challenge.

2. Methods

Our SLR [11] employs the PRISMA framework [12]. The PRISMA framework guides us through the search and eligibility screening for this review. We then synthesize our findings following a qualitative thematic analysis, reporting patterns or contradictions in the literature. Our search strategy includes also the grey literature, relevant to connected places in the United Kingdom, using the same query syntax for web search.

Using the PRISMA framework, due to the emerging nature of our field of investigation, 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 rigor, relevant publications were retrieved using the search strategy shown in Figure 1. This strategy is discussed in detail in Section 2.1.

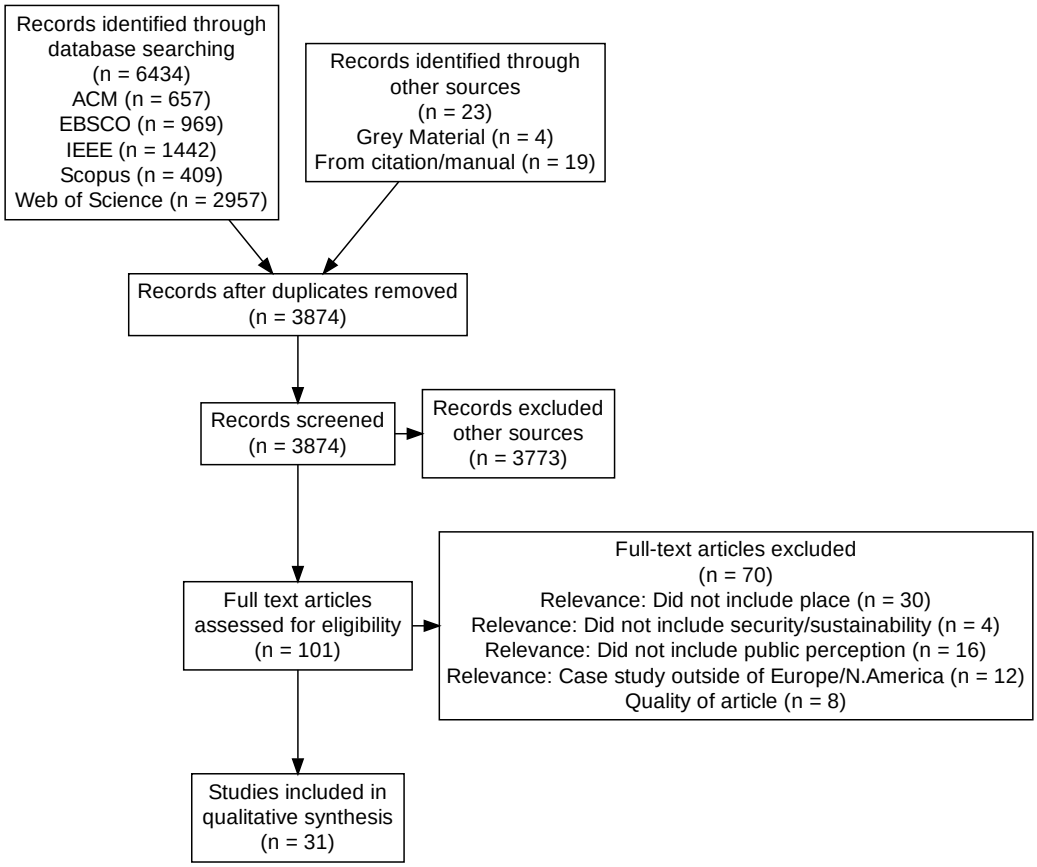

Figure 1. PRISMA Flow Diagram.

2.1. Search Strategy

After conducting initial test searches of likely databases, we refined our query syntax and eligibility criteria to create a comprehensive data set. The tests immediately revealed 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 identified the key terms that could uncover research relating to public perceptions 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"

The databases searched were EBSCO, IEEE, ACM, Web of Science, and Scopus. These databases were selected to provide a comprehensive list of possible articles. Each database was manually searched between 9 January and 28 January 2023, with all articles found using the above query syntax added to a shared reference manager.

2.2. Eligibility Criteria

Search results were screened by at least two different researchers against the following eligibility criteria:

- *Language*: Full-text article written in English.
- *Title relevance*: Mentions user perceptions or a variable thereof; an aspect or type of connected place; and an aspect or synonym of cybersecurity and/or sustainability.
- *Abstract relevance*: Mentions user perceptions or a variable thereof; an aspect or type of connected place; and an aspect or synonym of cybersecurity and/or sustainability.
- *Geography of case studies*: Given the UK policy orientation of this review purpose, the authors agreed with DSIT's Secure Connected Place Team that only the case studies in the UK, Europe, and North America would be eligible for inclusion given their likely cultural, democratic and legal proximity; and similarity in technological readiness level.

During the screening stage by title or abstract, we excluded 3773 publications due to the nature of our broad search terms. Our aim was to find articles relevant only to specific types of connected places or referencing another article that was. The remaining articles were included in a full-text eligibility check, which evaluated the relevance and quality of an article by at least two researchers.

3. Results

This section presents the background characteristics of the process and results of our data analysis, including the details on the articles included in the literature review.

3.1. Background Characteristics

In this literature review, we screened 3874 articles before selecting 27 journal and conference articles and four pieces of grey literature that 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. The extent to which different technologies were referenced in the literature can be seen in Table 2. This table in itself contributes to our definition of connected places and supports the transferable nature of our findings, i.e., our findings may still be useful to a place that is not formally defined as a 'connected place' by the place owners or users, but which deploys and/or utilizes the technologies in this table. Four literature reviews within selected articles agree that the number of articles investigating the security impact of public perceptions is still relatively small [13–16]. Those who have investigated public perceptions tend to orient more around privacy than security [16]. The case studies included in the reviewed articles lack attention to the safety, sustainability, equity, and resilience of connected places [15].

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

3.1.1. Characteristics of Results against Query Syntax Variables

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

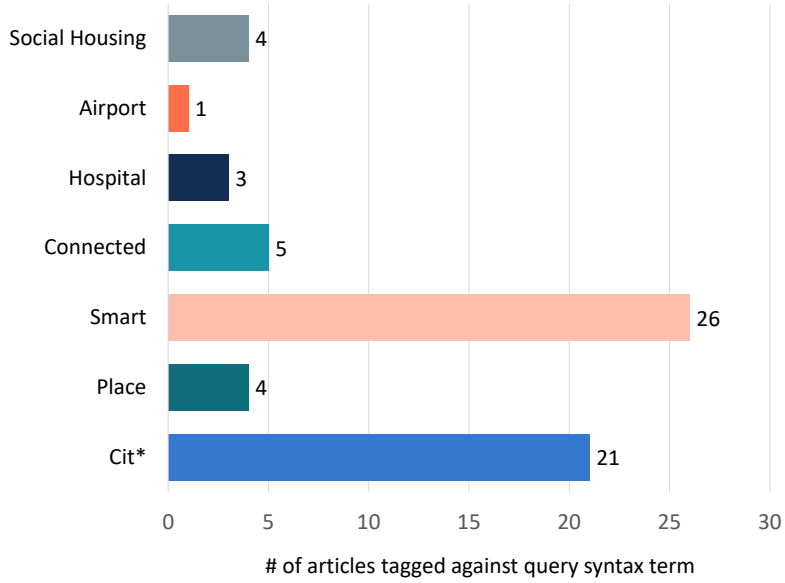

Figure 2. Connected place variable tags.

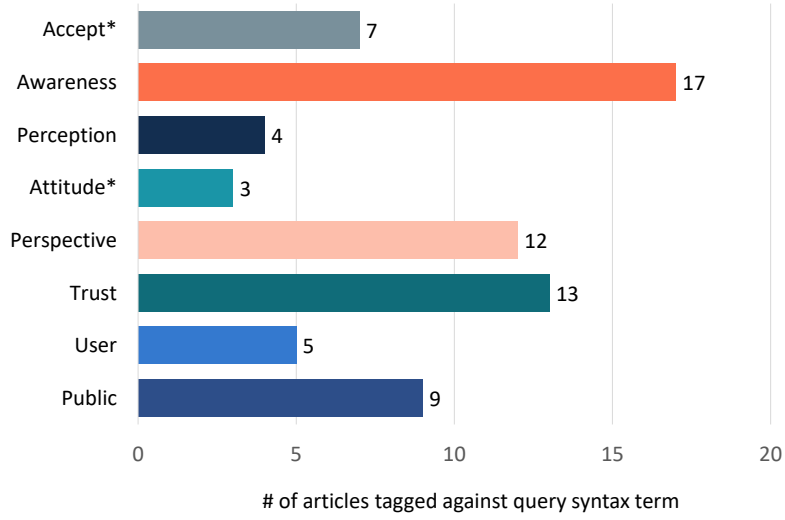

Figure 3. Public perspective variable tags.

3.1.2. Characteristics of Results by Geographic Focus

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

4. Findings

This section captures the synthesis of the literature concerning how public perceptions of connected places affect the security and sustainability of connected places. We capture

both theoretical and empirical findings, to build a conceptual framework. We gather related concepts to provide a broader understanding of the research question.

4.1. Public Perceptions Influencing Public Security Behaviors

The reviewed literature suggests that the majority of the public will be oblivious to connected places [17], let alone desirable security behaviors within them [8,18]. At the same time, public perceptions and security behaviors in connected places are being influenced by different elements: the value offered by connected place technology [19]; the clarity of risks and security procedures communicated [20,21]; the ability to express concerns and participation in design and development [17,21–23]; perceptions of privacy and risk [13,23,24]; trustworthiness [8,9,16,25]; and the type and purpose of data collection [18,23].

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 [19]. Fayoumi et al. [20] present a correlation between the explanation of security and privacy issues in an IoT system and the resulting enhanced user awareness and ability to avoid risks. However, the wide-ranging pre-existing levels of awareness amongst public users of connected places use a one-size-fits-all approach for the explanation of security and privacy issues, which is challenging. For example, many members of the public have a good understanding of network and data security processes but with low awareness of threats [26], or the information being shared by their devices in a connected place [8,18].

The degree to which the public perceives the connected place to be actively protecting them from these harms further complicates the landscape: it could lead to neglecting cybersecurity due to misleading feelings of being protected, and the controls are being taken care of elsewhere [27]. Similarly, while the public's increased awareness and risk aversion of threats is no doubt an attractive goal for connected place managers, this risk aversion may result in an unwanted consequence of residents avoiding connected places or specific technologies within them [24].

The privacy factors affecting a user's perception of security are (a) the purpose for which *data* is collected, i.e., (a.1) service or surveillance [23]; (a.2) personal or impersonal [23]; (b) the *context* that data sharing is taking place within, e.g., users are more willing to share data in the event of a friend being endangered [18]; and (c) who is collecting data, e.g., the government [13].

It is not clear from the literature to what extent security behaviors in a connected place are influenced by behaviors and experiences in cyberspace. Taher et al. [28] suggest students' privacy concerns in 'smart campus buildings' 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 cyberattack in cyberspace, as opposed to in a (a) *cyber–physical environment* (connected place [28]); (b) *demographic differences* (age, gender [18,29]); and (c) *pre-existing awareness* of cybersecurity vulnerabilities and controls [26]. However, none of these findings are comprehensively investigated enough to draw any applicable conclusions from.

Publications refer to privacy and security concerns that alter the likelihood of engaging with a connected place by the public. Willemsen and Cadee [30] link increased security measures with increased user-experience friction, potentially affecting the acceptability of a connected place and increasing the likelihood of a user disengaging. Van Twist et al. [13] argue that rejection of a connected place can be considered a threat to security itself. Data may become unreliable, and—in extreme instances—rejection related to mistrust can render the public themselves a threat to security [13]. This topic is further explored in Section 4.2.3.

4.2. Perspectives on Public Security Behaviors Affecting Security, and Sustainability of Connected Places

4.2.1. Reasons Public Perceptions Affect Connected Place Security and Sustainability

Hernandez-Ramos et al. [8] point to examples, e.g., the Mirai botnet attack, to demonstrate the potential for compromised IoT devices used in attacks against Information and

Communications Technology (ICT) systems and critical infrastructure (CI). They highlight that a single citizen's lack of awareness, and the resulting poor cybersecurity hygiene, could be a threat to the security of the general public and systems within a smart city [8].

A survey of 1444 residents of the US city of Denton revealed 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*" [24] (p. 618). Smart city users value safety and security, supporting increased regulation to this end. Consequently, residents are more likely to show interest in using smart city services when the applications are perceived to be innovative and privacy is assured [24].

Although intertwined, the literature suggests that privacy appears to matter slightly more to the public than (cyber)security in connected places [17]. Liesbet van Zoonen [23] argues for the importance of recognizing the public's privacy concerns to sustain support and participation. Habib et al. [24] also identify perceived cybersecurity as key to public acceptance. However, Twist et al. [13] warn that over-surveillance, often motivated by public safety, can lead to the public rejecting a connected place, hindering its sustainability. Manfreda et al. [21] list perceived privacy, innovation concept, and service quality as key factors of acceptance, with cybersecurity notably absent.

Security measures creating friction with the public need to be addressed within the context of a connected place. Willemsen and Cadee [30] present airports as public spaces, in which the trade-off between security and friction is more actively considered by place managers (i.e., the need to manage passenger comfort, processing efficiency, and security). Manfreda et al. [21] highlight the immense importance "*to analyze the trade-off between city's effectiveness and its security*" [21] (p. 277).

4.2.2. Specific Technical Vulnerabilities Affected by Public Perception

Vanolo [31] argues that personal devices are essential for the sustainability of connected places given the way an intelligent environment receives feedback from residents' smartphones. At the same time, end-user devices present the greatest security threat to connected places [9,18,19,23]. Many users' perceptions of the importance of security are very low [8,18], and often do not maintain security updates and patches. Herbert et al. [18] (p. 283) cite a 2019 study by Ali et al. [32], where more than half of 3000 global smartphone users surveyed were not aware of smartphone security and privacy. This result correlates with the findings of Ipsos Mori's "*Consumer Attitudes Towards IoT Security" Report* [33], highlighting that only 24% of Wi-Fi router owners have changed the password since purchase, and only 20% report checking the minimum support period when purchasing a smart device. Vitunskaite et al. [9] argue that the only way to control user-generated vulnerabilities of connected places is to control what is on the market.

Personal devices are often the point of access to a connected place for the public via public Wi-Fi [31]. A university-based study by Papic et al. [34] found that 43% of 110 students at Osijek University, Croatia never felt safe when using public Wi-Fi. The manner in which devices remember and automatically reconnect to Wi-Fi may present vulnerabilities to outsider attacks [25], with user behavior being key in addressing this weak link in connected place infrastructure, especially when users frequently misjudge the risky situations in the wild [29]. Willemsen and Cadee [30], writing about the arguably more security-critical environment of an airport, argue for limiting the possibility for the public to access networks in connected places, both through reducing access points and by separating public networks from internal networks.

The final technology to feature to a notable extent is 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 [35]. Indeed, they are seen by the public, according to Bellanche-Gracia et al. [35], as guaranteeing secure transmission of sensitive data and 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*" [35] (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. These are not typically public-user-oriented and therefore not surprising in their absence. Where sensors are public user-oriented it is in a passive way with regards to user experience, i.e., the user is likely to be unaware of being 'sensed'. The literature in which sensors are featured [9,13,36] 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 Place Security and Sustainability

Public users are positioned within the literature as influential threats [8,13] to connected place security and sustainability in various ways:

- Naive or optimistic users who may unintentionally threaten a place's security through inaction [19] or being victim to the influence of bad actors, in particular via social engineering [37];
- Allies of the place managers who are aware of threats [19] 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 traveling in both directions [16,24,25];
- Malicious actors themselves due to the ease of causing significant damage though low-skilled cyberattacks [9,36] or rejecting surveillance through non-technical tampering, data obfuscation, or vandalism [13,36];

Isin and Ruppert [36] call for a new type of digital citizenship in which the complexities of the above can be discussed in a way that considers the multiple possible roles any member of the public may play at any time in a connected place.

4.2.4. Public Perspectives before, during, and after a Cyberattack on a Connected Place

A number of different articles focus on the public at different parts of a cybersecurity 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 [8,16,18,38]. A few articles [15,24,26,27] explore public perceptions during an attack and suggest that the importance of the public's role in the system increases significantly during this time: minimizing the impact of an attack in terms of technical damage [26] while keeping themselves safe from physical harm due to an awareness of the way an attack will affect a place's infrastructure and the mitigating actions they may have to take. 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 [15]. Finally, the way in which the experience of an attack affects the public perceptions of a connected place's security is disputed. Zwilling et al. [27] argue it has no effect, while Habib et al. [24] argue that it can increase rejection of connected places and present a future threat to a place's security and sustainability 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 Cybersecurity Research and Guidance

Related to the need for research on the multiple positions and motivations a user may manifest [25], 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 place technologies. This was also

common across the grey materials, with government guidance using the term 'user' to refer exclusively to place managers and operators [1,38,39].

4.3.2. The Influence of Connected Place Managers and Their Relationship with the Public

The literature is divided on the influence a place manager can have on public perceptions and behaviors. Federico Cilauro [38] points towards the significance of technical factors or process factors in securing the connected place to suggest that people factors matter not. However, Vitunskaite et al. [9] point to the actions of fourth and fifth parties, i.e., those producing devices that enter the connected place, as being so critical to security that managers are powerless to influence these risks. Cilauro [38] warns against focusing on user-oriented concerns, as they may lead to over-investment in end-point security. Cilauro [38] is also critical of councils in particular, reporting that a connected place commissioner believed "*most councils do not know enough about technology or cybersecurity to procure technology*" [38] (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 by trying. Others, on the other hand, suggest that place managers must take a 'user-centric' approach to fully understand and overcome the security threats in connected places [25]. The gap in research on the influence of public perceptions was raised in four articles [13,15,16,21]. Liesbet van Zoonen [23] argues that connected place managers must acknowledge public concerns about privacy 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 [16,21,40] and that it is the duty of the government to regulate connected places in a way that protects individuals' data [14]. They argue that it is the place that is the risk to the public security, not the public 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 [40], privacy impact assessments [23], cybersecurity culture frameworks [26] and citizen-centric approaches of connected place design and development such as living labs, crowdsourcing and citizen participation [22,23].

Technical solutions include privacy-enhancing technologies [23] which align with the argument that public engagement is futile and the level of risk afforded to any public should be minimized to the point of irrelevance. Hernandez-Ramos et al. [8] take this further by identifying the deployment of certified devices and systems, i.e., solutions that must be created far up the connected place supply chain from the connected place manager's influence, as ways to build public trust in smart city services. However, they do not articulate how you communicate certification to the public. Louw and Van Zolms [25] make an argument for end-user information security portals or dashboards, which is 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*" [25] (p. 125).

5. Discussion

In this section, we discuss the confusion and contradictions in the available literature regarding the influence of the public perspective on the security of connected places. Moreover, our analysis revealed three trade-offs, which we examine in this section. Next, we provide information regarding the limitations of our study. Lastly, based on our analysis, we provide recommendations for future research.

5.1. Confusion and Contradictions

Many of the articles reviewed point to the heightened importance of public perceptions and behavior during a cyberattack on a connected place [8,15,16,18,24,26,27,38]. However, there is no consensus on how perceptions and behavior can be influenced to minimize the impact of, and expedite recovery from, a cyberattack. This question requires further research, which can deliver up-to-date and technology-specific recommendations alongside best practices.

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 [8]. Similarly, are devices a point of security vulnerability in a connected place, or a point of data leakage, privacy threat, and over-surveillance for the member of the public within a connected place?

There is a disagreement across the literature concerning who the public is, 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 concerning the aims of attempts to influence public perceptions and behaviors within connected places: are they to keep the place itself safe, i.e., its infrastructure, institutions and operations, or should they protect the public'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.

The existing literature tends to reveal the following common assumptions within connected place managers:

- Connected place 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 and 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 regulations applied to personal devices and the sensor and network technologies or within the organizational culture and practice of those delivering connected places.

5.2. Trade-Offs of Connected Places

5.2.1. Secure Places vs. Friction-Less Experiences

If connected places provide convenient solutions, members of the public may accept security and privacy risks [19]. Moreover, the lack of awareness of how to avoid privacy and security risks results in the inability to prevent them [20]. 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 utilize 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.

Another area needing further research is the understanding of whether those who experience a data breach are more privacy and security-conscious as a result.

5.2.2. Sustainability vs. Security

As pointed out in Section 4.2.2, personal smartphones are essential for the sustainability of connected places [31], but they are the biggest security threat [9,18,19,23]. 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 the public's security, as well as when and how. Moreover, the perception of the public may change depending on whose responsibility it is.

5.2.3. 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.

It is also debatable whether place managers should consider 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 with the aim of making them resilient to user behaviors.

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 [13], and too little may be perceived as the public being denied their its human right to security [16,21,40]. We argue though that controlling the market [9] would not control a user's behavior with a device, particularly their likelihood to maintain antivirus or security updates and patches [25].

5.3. Limitations of This Study

Articles reviewed were often not directly addressing our research question; instead, they focus on the public discontent within a connected place [13–15], often as a rejection to perceived over-surveillance, and not necessarily relating to the impacts this has on cybersecurity, or they consider the role of an individual in a connected place caught up in cyberwarfare [15] or consider public consultation as a necessary part of designing a working and secure connected place [16].

The diverse nature of connected places also generated results that are so wide-ranging that 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 behaviors or their adoption of connected places often applied broad observations concerning perceptions of the internet and data-driven technologies.

5.4. Recommendations for Future Research

5.4.1. Socio-Technical Approach towards Security

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 [16]. We also identified a need to address the imbalanced focus towards technical solutions for connected place security [15] and to conduct more research on how perceptions influence the security behaviors of the public [13]. They all argue for a more socio-technical approach to this challenge, another argument we concur with having evaluated our own findings.

5.4.2. User in the Loop

In addition, there is a need to explore models and tools for considering public perceptions and behaviors in connected place design and management, as well as methods through which connected place managers can influence both perceptions and behaviors, if at all. There were some participatory tools suggested by the literature [22,23,26,40]. These need further testing in different contexts, but the consensus of these arguments was that if a productive tool could be found, the public would trust, accept and sustain connected places more if individuals felt themselves to be 'in the loop'. One article [9] described an open-source platform for connected place sensor data and management in Barcelona; however, they noted that cybersecurity did not feature frequently in this discourse.

5.4.3. Transparency and Awareness Lead to Acceptance

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, their perceptions of their personal data and whose responsibility the protection of these data is in a connected place context. There also is a need for research that researches patterns between specific connected place cybersecurity 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 [30] or security [8]. 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. Conclusions

This literature review highlights the potential importance of public perceptions and behaviors concerning the security and sustainability of connected places and the need for further research to develop recommendations for minimizing 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 behaviors within connected places, with some focusing on protecting the infrastructure and institutions of the place, while others prioritize the privacy and safety of the public.

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 cybersecurity.

We acknowledge the limitations of this study, including the fact that the existing literature does often not directly address 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 behaviors 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.

Author Contributions: Conceptualization, A.D.-Z., J.B., O.C., P.N. and G.O.; methodology, J.B., O.C., P.N. and G.O.; validation, R.C.; formal analysis, A.D.-Z., J.B., C.A. and X.G.; investigation, A.D.-Z., J.B., C.A. and X.G.; data curation, A.D.-Z., J.B., C.A. and X.G.; writing-original draft preparation, A.D.-Z., C.A. and X.G.; writing-review and editing, A.D.-Z., J.B., C.A., X.G., O.C., P.N., G.O., R.C., D.D.R., J.M., J.W., T.W. and E.J.; supervision, O.C., P.N. and R.C.; project administration, A.D.-Z.

and J.B.; funding acquisition, J.B. All authors have read and agreed to the published version of the manuscript.

Funding: 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.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest. The funding sponsors had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, and in the decision to publish the results.

References

1. Connected Places Cyber Security Principles. Available online: https://www.ncsc.gov.uk/collection/connected-places-security-principles (accessed on 24 January 2023).
2. Bibri, S.E. The IoT for smart sustainable cities of the future: An analytical framework for sensor-based big data applications for environmental sustainability. *Sustain. Cities Soc.* **2018**, *38*, 230–253.
3. Nižetić, S.; Šolić, P.; Gonzalez-De, D.L.D.I.; Patrono, L. Internet of Things (IoT): Opportunities, issues and challenges towards a smart and sustainable future. *J. Clean. Prod.* **2020**, *274*, 122877.
4. Perković, T.; Damjanović, S.; Šolić, P.; Patrono, L.; Rodrigues, J.J. Meeting challenges in IoT: Sensing, energy efficiency, and the implementation. In Proceedings of the Fourth International Congress on Information and Communication Technology: ICICT 2019, London, UK, 6–8 September 2023; Springer: Berlin/Heidelberg, Germany, 2020; Volume 1; pp. 419–430.
5. NCSC. What Is Cyber Security? Available online: https://www.ncsc.gov.uk/section/about-ncsc/what-is-cyber-security (accessed on 9 November 2023).
6. Almusaylim, Z.A.; Alhumam, A.; Jhanjhi, N. Proposing a secure RPL based internet of things routing protocol: A review. *Ad. Hoc. Netw.* **2020**, *101*, 102096.
7. Kaushik, K.; Singh, K. Security and trust in iot communications: Role and impact. In *Intelligent Communication, Control and Devices: Proceedings of ICICCD 2018*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 791–798.
8. Hernandez-Ramos, J.L.; Martinez, J.A.; Savarino, V.; Angelini, M.; Napolitano, V.; Skarmeta, A.F.; Baldini, G. Security and Privacy in Internet of Things-Enabled Smart Cities: Challenges and Future Directions. *IEEE Secur. Priv.* **2021**, *19*, 12–23. https://doi.org/10.1109/MSEC.2020.3012353.
9. Vitunskaite, M.; He, Y.; Brandstetter, T.; Janicke, H. Smart cities and cyber security: Are we there yet? A comparative study on the role of standards, third party risk management and security ownership. *Comput. Secur.* **2019**, *83*, 313–331. https://doi.org/10.1016/j.cose.2019.02.009.
10. Kakkavas, G.; Gkatzioura, D.; Karyotis, V.; Papavassiliou, S. A review of advanced algebraic approaches enabling network tomography for future network infrastructures. *Future Internet* **2020**, *12*, 20.
11. Snyder, H. Literature review as a research methodology: An overview and guidelines. *J. Bus. Res.* **2019**, *104*, 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039.
12. Page, M.J.; McKenzie, J.E.; Bossuyt, P.M.; Boutron, I.; Hoffmann, T.C.; Mulrow, C.D.; Shamseer, L.; Tetzlaff, J.M.; Akl, E.A.; Brennan, S.E.; et al. The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. *Int. J. Surg.* **2021**, *88*, 105906.
13. van Twist, A.; Ruijer, E.; Meijer, A. Smart cities & citizen discontent: A systematic review of the literature. *Gov. Inf. Q.* **2023**, *40*, 101799. https://doi.org/10.1016/j.giq.2022.101799.
14. Meijer, A.; Bolívar, M.P.R. Governing the smart city: A review of the literature on smart urban governance. *Int. Rev. Adm. Sci.* **2016**, *82*, 392–408. https://doi.org/10.1177/0020852314564308.
15. Soare, S.R. Smart Cities, Cyber Warfare and Social Disorder. In *Cyber Threats and NATO 2030: Horizon Scanning and Analysis*; CCDCOE: Tallinn, Estonia, 2020.
16. Ma, C. Smart city and cyber-security; technologies used, leading challenges and future recommendations. *Energy Rep.* **2021**, *7*, 7999–8012. https://doi.org/10.1016/j.egyr.2021.08.124.
17. Thomas, V.; Wang, D.; Mullagh, L.; Dunn, N. Where is Wally? In Search of Citizen Perspectives on the Smart City. *Sustainability* **2016**, *8*, 207. https://doi.org/10.3390/su8030207.
18. Herbert, F.; Schmidbauer-Wolf, G.M.; Reuter, C. Who Should Get My Private Data in Which Case? Evidence in the Wild. In Proceedings of the Mensch und Computer 2021, New York, NY, USA, 5–8 September 2021; MuC '21; pp. 281–293. https://doi.org/10.1145/3473856.3473879.
19. Harper, S.; Mehrnezhad, M.; Mace, J.; Groß, T.; Viganò, L. User Privacy Concerns in Commercial Smart Buildings. *J. Comput. Secur.* **2022**, *30*, 465–497. https://doi.org/10.3233/JCS-210035.

20. Fayoumi, A.; Sobati-Moghadam, S.; Rajaiyan, A.; Oxley, C.; Montero, P.F.; Dahmani, A. The Cybersecurity Risks of Using Internet of Things (IoT) and Surveys of End-Users and Providers within the Domiciliary Care Sector. In Proceedings of the 2022 Sixth International Conference on Smart Cities, Internet of Things and Applications (SCIoT), Mashhad, Iran, 14–15 September 2022; pp. 1–7. https://doi.org/10.1109/SCIoT56583.2022.9953634.
21. Manfreda, A.; Ekart, N.; Mori, M.; Groznik, A. Citizens' Participation as an Important Element for Smart City Development. In Proceedings of the Re-imagining Diffusion and Adoption of Information Technology and Systems: A Continuing Conversation, Tiruchirappalli, India, 18–19 December 2020; Sharma, S.K., Dwivedi, Y.K., Metri, B., Rana, N.P., Eds.; Springer: Cham, Switzerland, 2020; IFIP Advances in Information and Communication Technology; pp. 274–284. https://doi.org/10.1007/978-3-030-64861-9_25.
22. Lea, R.; Blackstock, M. Smart Cities: An IoT-centric Approach. In Proceedings of the 2014 International Workshop on Web Intelligence and Smart Sensing, New York, NY, USA, 1–2 September 2014; IWWISS '14; pp. 1–2. https://doi.org/10.1145/2637064.2637096.
23. van Zoonen, L. Privacy concerns in smart cities. *Gov. Inf. Q.* **2016**, *33*, 472–480. https://doi.org/10.1016/j.giq.2016.06.004.
24. Habib, A.; Alsmadi, D.; Prybutok, V.R. Factors that determine residents' acceptance of smart city technologies. *Behav. Inf. Technol.* **2020**, *39*, 610–623. https://doi.org/10.1080/0144929X.2019.1693629.
25. Louw, C.; Von Solms, B. Free Public Wi-Fi Security in a Smart City Context-An End User Perspective. In *Smart Cities Cybersecurity and Privacy*; Elsevier: Amsterdam, The Netherlands, 2019; p. 127. https://doi.org/10.1016/B978-0-12-815032-0.00009-3.
26. Georgiadou, A.; Michalitsi-Psarrou, A.; Gioulekas, F.; Stamatiadis, E.; Tzikas, A.; Gounaris, K.; Doukas, G.; Ntanos, C.; Landeiro Ribeiro, L.; Askounis, D. Hospitals' Cybersecurity Culture during the COVID-19 Crisis. *Healthcare* **2021**, *9*, 1335. https://doi.org/10.3390/healthcare9101335.
27. Zwilling, M.; Klien, G.; Lesjak, D.; Wiechetek, L.; Cetin, F.; Basim, H. Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. *J. Comput. Inf. Syst.* **2022**, *62*, 82–97. https://doi.org/10.1080/08874417.2020.1712269.
28. Tawer, R.; Mehrnezhad, M.; Morisset, C. "I feel spied on and I do not have any control over my data": User Privacy Perception, Preferences and Trade-offs in University Smart Buildings. *Socio-Tech. Asp. Secur.* **2022**, *2023* , 1–20.
29. Sombatruang, N.; Sasse, M.A.; Baddeley, M. 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, New York, NY, USA, 5 December 2016; STAST '16; pp. 61–72. https://doi.org/10.1145/3046055.3046058.
30. Willemsen, B.; Cadee, M. Extending the airport boundary: Connecting physical security and cybersecurity. *J. Airpt. Manag.* **2018**, *12*, 236–247 .
31. Vanolo, A. Is there anybody out there? The place and role of citizens in tomorrow's smart cities. *Futures* **2016**, *82*, 26–36. https://doi.org/10.1016/j.futures.2016.05.010.
32. Ali, M.; Rahman, M.L.; Jahan, I. Security and Privacy Awareness: A Survey for Smartphone User. *Int. J. Adv. Comput. Sci. Appl.* **2019**, *10*, 483–488. https://doi.org/10.14569/2156-5570.
33. Ipsos MORI. Consumer Attitudes towards IoT Security. Available online: https://assets.publishing.service.gov.uk/media/607d7e588fa8f57358f07e60/Consumer_Attitudes_Towards_IoT_Security_-_Research_Report.pdf (accessed on 31 October 2023).
34. Papic, A.; Radoja, K.; Szombathelyi, D. *Cyber Security Awareness of Croatian Students and the Personal Data Protection*; Simic, M., Ed.; University of JJ Strossmayer Osijek: Osijek, Croatia, 2022; pp. 563–574.
35. Belanche-Gracia, D.; Casaló-Ariño, L.V.; Pérez-Rueda, A. Determinants of multi-service smartcard success for smart cities development: A study based on citizens' privacy and security perceptions. *Gov. Inf. Q.* **2015**, *32*, 154–163. https://doi.org/10.1016/j.giq.2014.12.004.
36. Isin, E.; Ruppert, E. *Being Digital Citizens*, 2nd ed.; Rowman & Littlefield Publishers: Lanham, MD, USA, 2020.
37. Saber, O.; Mazri, T. Smart City Security Issues: the Main Attacks and Countermeasures. *Int. Arch. Photogramm. Remote. Sens. Spat. Inf. Sci.* **2021**, *XLVI-4/W5-2021*, 465–472. https://doi.org/10.5194/isprs-archives-XLVI-4-W5-2021-465-2021.
38. Cilauro, F. *The Connected Places Market in the UK*; 2021. Available online: https://assets.publishing.service.gov.uk/media/633d9e3ee90e0709df741cb8/The_connected_places_market_in_the_UK_2022.pdf (accesed on 20 December 2023).
39. Security-Minded Approach to Developing Smart Cities, 2022. Available online: https://www.protectuk.police.uk/advice-and-guidance/awareness/security-minded-approach-developing-smart-cities (accesed on 20 December 2023).
40. Martinez-Balleste, A.; Perez-Martinez, P.; Solanas, A. The pursuit of citizens' privacy: A privacy-aware smart city is possible. *IEEE Commun. Mag.* **2013**, *51*, 136–141. https://doi.org/10.1109/MCOM.2013.6525606.