energies

Article

A Review of Privacy Concerns in Energy-Efficient Smart Buildings: Risks, Rights, and Regulations

Asmidar Abu Bakar [1], Salman Yussof [1], Azimah Abdul Ghapar [1], Sera Syarmila Sameon [1] and Bo Nørregaard Jørgensen [2,*]

[1] Institute of Informatics and Computing in Energy, Universiti Tenaga Nasional, Kajang 43000, Malaysia; asmidar@uniten.edu.my (A.A.B.); salman@uniten.edu.my (S.Y.); azimah@uniten.edu.my (A.A.G.); sera@uniten.edu.my (S.S.S.)

[2] Center for Energy Informatics, The Maersk Mc-Kinney Moller Institute, University of Southern Denmark, 5230 Odense, Denmark

* Correspondence: bnj@mmmi.sdu.dk

Abstract: In the contemporary era, smart buildings, characterized by their integration of advanced technologies to enhance energy efficiency and user experience, are becoming increasingly prevalent. While these advancements offer notable benefits in terms of operational efficiency and sustainability, they concurrently introduce a myriad of privacy concerns. This review article delves into the multifaceted realm of privacy issues associated with energy-efficient smart buildings. We commence by elucidating the potential risks emanating from data collection, storage, and analysis, highlighting the vulnerability of the personal and behavioral information of inhabitants. The article then transitions into discussing the rights of occupants, emphasizing the necessity for informed consent and the ability to opt-out of invasive data collection practices. Lastly, we provide an overview of existing regulations governing the intersection of smart buildings and privacy. We evaluate their effectiveness and present gaps that necessitate further legislative action. By offering a holistic perspective on the topic, this review underscores the pressing need to strike a balance between harnessing the benefits of technology in smart buildings and safeguarding the privacy of their occupants.

Keywords: smart buildings; privacy risk; rights; ethical consent; energy efficient; regulations

check for updates

Citation: Bakar, A.A.; Yussof, S.; Ghapar, A.A.; Sameon, S.S.; Jørgensen, B.N. A Review of Privacy Concerns in Energy-Efficient Smart Buildings: Risks, Rights, and Regulations. *Energies* **2024**, *17*, 977. https://doi.org/10.3390/en17050977

Academic Editor: Senthilarasu Sundaram

Received: 7 December 2023
Revised: 25 January 2024
Accepted: 6 February 2024
Published: 20 February 2024

1. Introduction

Buildings consume a large amount of electricity to maintain indoor temperature, ensure appropriate air circulation, and provide interior brightness. To improve the energy-efficiency of a building, the concept of smart buildings has been introduced. A smart building refers to a building that is able to make efficient use of its resources, such as electricity and water, while at the same time being able to maintain the comfort level of its occupants. This is carried out by measuring environmental parameters around the building and performing smart controls based on the environmental data to ensure an energy-efficient operation. The main goal of a smart building is to achieve sustainability by minimizing energy usage, which would have a positive environmental impact and cause the building to have a lower maintenance cost in the long run.

A smart building integrates various cutting-edge technologies such as the Internet of Things (IoT), data analytics, and artificial intelligence. Environmental data are read using large number of sensors that are positioned throughout the building. These sensors measure various types of indoor environmental data such as temperature, humidity, air quality, CO_2 level, occupancy, the state (open or closed) of windows and doors, and the power consumption of electrical appliances. The data collected are then analyzed to identify proper controls that can be performed to improve energy usage.

Figure 1 below depicts the envisioned advanced features of energy-efficient smart buildings, like sensors for fire detection, temperature monitoring using HVAC, lighting control, monitoring of IoT and smart meters. Alongside these features, there are potential privacy threats or risks associated with these buildings. Despite their numerous advantages in terms of sustainability and operational efficiency, energy-efficient smart buildings raise concerns about privacy that require careful consideration. The incorporation of sensors, smart meters, and automation systems for energy optimization may involve collecting sensitive data related to occupant behavior, preferences, and usage patterns. Analyzing these data may unveil occupants' daily habits, such as identifying their presence and preferred comfort settings. This detailed information can extend to discerning household activities from energy consumption patterns, posing a risk of exposing vulnerable times for potential break-ins. If these data are not securely handled, they may be vulnerable to privacy breaches, unauthorized access, or misuse. Striking a balance between advancing energy efficiency and safeguarding individual privacy is a challenging aspect of the development and deployment of such buildings.

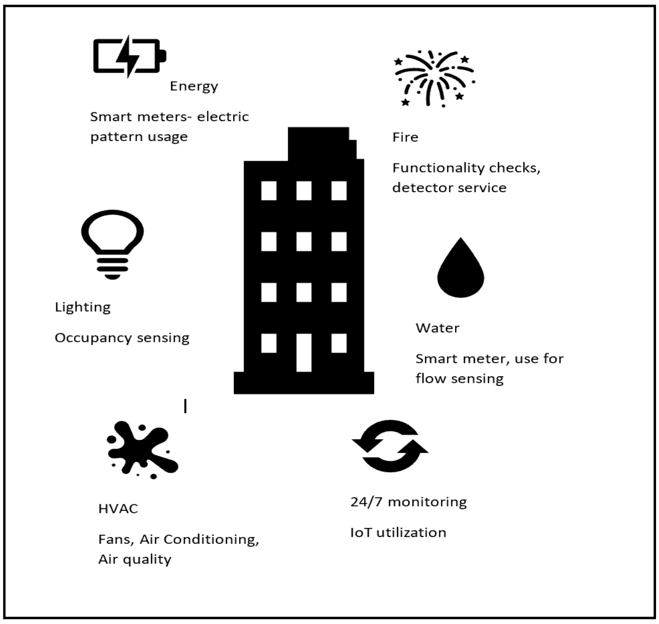
Energy
Smart meters- electric pattern usage
Fire
Functionality checks, detector service
Lighting
Occupancy sensing
Water
Smart meter, use for flow sensing
HVAC
Fans, Air Conditioning, Air quality
24/7 monitoring
IoT utilization

Figure 1. Smart buildings.

One of the issues of any system that collects data related to people is privacy. The collection and processing of data is considered as violating privacy if it can result in the identification of a person. In many countries, privacy is protected through a Personal Data Protection Act (PDPA) [1]. Many countries have their own PDPA, which may vary slightly from one country to another [1]. The most widely adopted privacy protection regulation is the European Union's General Data Protection Regulation (GDPR) [2]. However, the GDPR and all such privacy acts were developed to protect privacy in general: it may be unclear how they can be applied to address data privacy in energy-efficient smart buildings.

In the existing literature, there are only a handful of review papers related to privacy in smart buildings [3–6]. The authors in [4,5] provide a review on both security and privacy issues in smart buildings. A review of existing solutions using cryptographic standards, an intrusion detection system (IDS), and anonymization techniques is also provided by [5]. The authors of [3] review the privacy issues of occupancy detection technology commonly deployed in smart buildings. The authors in [6] provide a review on the use of differential privacy for preserving the privacy of data collected in smart buildings. However, none of these review papers above discuss privacy issues and solutions from the point of view of occupancy rights and privacy regulations.

This article explores the various aspects of privacy concerns in energy-efficient smart buildings, including the risks involved and the rights of their occupants. It also looks at the laws and policies that have been developed to strike a balance between taking advantage of advanced technology and the preservation of individual privacy.

The objectives of this review article can be described as follows:

1. To review the potential privacy risks associated with data collection, storage, and analysis in energy-efficient smart buildings.
2. To assess the rights of smart building occupants, emphasizing the importance of informed consent and the option to opt out of intrusive data collection practices.
3. To review and evaluate existing legal regulations governing the relationship between smart buildings and privacy.

It needs to be noted that this article only focuses on energy-efficient smart buildings. Therefore, it only focuses on the collection and processing of data that are required for energy efficiency purposes. It is acknowledged that there are other features of smart buildings, such as those used to improve security, which may collect more privacy-intrusive data. However, such applications are out of the scope of this paper. Furthermore, this article only reviews existing works related to privacy risks, rights, and regulations. Other works on privacy preservation mechanisms and algorithms are also not part of the scope of this paper.

The paper is structured as follows: Section 2 provides an overview of preliminary studies, highlighting key topics. In Section 3, the methodology section discusses the approach used in conducting the research. Section 4 presents the results, followed by a discussion in Section 5. Finally, the paper concludes in Section 6 under the conclusion section.

2. Preliminary Studies

This section presents the key topics discussed in this review paper, offering an understanding of the main ideas and issues explored in the work.

2.1. Smart Building Definitions

The concept of smart buildings originates from the growing integration of modern technology into buildings and their systems. This integration allows for remote operation and control of the whole life cycle of a building, resulting in convenience, comfort, cost efficiency, and energy efficiency [7–9]. The common consensus is that incorporating new technologies is an essential requirement for the successful implementation of smart buildings, also referred to as intelligent buildings. This encompasses various aspects such as deploying sensors, engineering and analyzing big data, utilizing cloud and fog computing, developing software engineering, and implementing algorithms for human–computer interactions.

Residential buildings and non-residential buildings, such as workplaces, airports, and shopping malls, are equipped with sophisticated networking and automation systems to enhance convenience and reduce energy consumption. Smart homes, although they are smaller than smart buildings, may include similar characteristics that classify them as smart buildings. The focus of our research revolved around smart buildings, encompassing smart homes, smart offices, and smart commercial structures, all falling within the definition of smart buildings.

2.2. Privacy in Energy-Efficient Smart Buildings

Smart buildings employ IoT (Internet of Things) devices, sensors, cameras, and other technology to optimize operations, boost security, and enhance energy efficiency. Prioritizing the security of IoT-connected devices is crucial due to the remarkable growth in their numbers and applications. Compromising any device within IoT systems may lead to a data breach, posing significant threats to privacy, risks to people's lives, and potential material losses.

Privacy in energy-efficient smart buildings includes the protection of individuals' personal information and behavioral data within the context of smart buildings designed for enhanced energy efficiency [10,11]. As these buildings utilize advanced technologies to optimize energy consumption, concerns arise regarding the collection, storage, and analysis of the related data obtained via diverse sensors, devices, and systems incorporated within these structures [12]. The challenge lies in balancing the benefits of energy efficiency with the need to safeguard the privacy rights of individuals. This involves addressing potential risks, ensuring informed consent, and navigating existing regulations to create a secure and privacy-respecting environment in smart buildings. The existing privacy laws and regulations address the entitlement of individuals to safeguard their private data. Some of the regulations that pertain to privacy include the General Data Protection Regulation (GDPR) [2] used by the European Union and other acts such as the California Consumer Privacy Act (CCPA) [13], Australian Privacy Principles, and a few others [14].

3. Methodology

This article follows the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) methodology for conducting the review procedure [15]. This framework offers a systematic and complete structure for researchers to transparently document their techniques and conclusions while performing systematic reviews of scientific literature.

Figure 2 illustrates the flow of the processes involved in constructing this article. The initial stage started with formulating the research questions and developing the Boolean string to facilitate the retrieval of the most suitable articles for this systematic literature review (SLR). For this purpose, three online databases, specifically ACM Digital Library, Scopus, and IEEE, were used for this study.

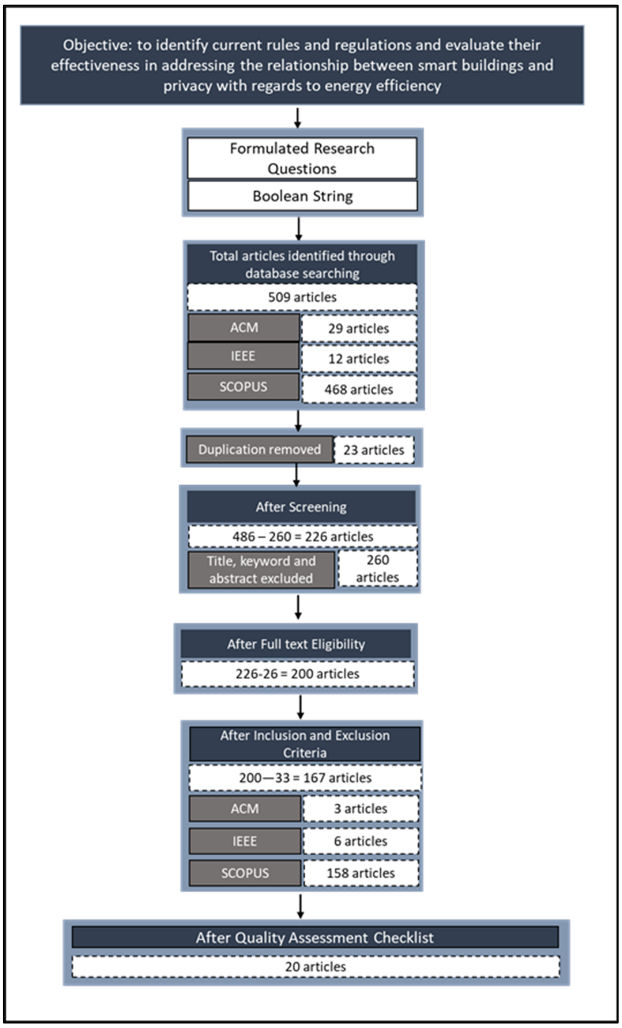
Objective: to identify current rules and regulations and evaluate their effectiveness in addressing the relationship between smart buildings and privacy with regards to energy efficiency
Formulated Research Questions
Boolean String
Total articles identified through database searching
509 articles
ACM
29 articles
IEEE
12 articles
SCOPUS
468 articles
Duplication removed
23 articles
After Screening
486 – 260 = 226 articles
Title, keyword and abstract excluded
260 articles
After Full text Eligibility
226-26 = 200 articles
After Inclusion and Exclusion Criteria
200—33 = 167 articles
ACM
3 articles
IEEE
6 articles
SCOPUS
158 articles
After Quality Assessment Checklist
20 articles

Figure 2. Flow of the SLR process.

A total of 509 articles were found using the search string. After removing 23 duplicates, a total of 486 were left. The articles were then filtered based on their title, keywords, and abstract. Among these, 260 articles were excluded as they did not align with the topic. The remaining 226 articles underwent a full article review. Of these, 26 were further excluded due to factors such as a focus on privacy in different domains, a general application of privacy in the IoT rather than in smart buildings, or repetitive studies. The articles were thereafter subjected to further filtration based on the predetermined inclusion and exclusion criteria that had been set. Following the completion of this process, a total 167 articles were selected and subsequently evaluated using the Quality Assessment Checklist (QAC). Upon the completion of the QAC process, 20 articles were selected for the purpose of data synthesis.

3.1. Research Questions

In order to achieve our objectives, three research questions were formulated, as shown in Table 1.

Table 1. Research questions.

RQ1	What are the specific data collection, storage, and analysis methods used in energy-efficient smart buildings, and how do they pose privacy risks to inhabitants?
RQ2	What legal and ethical rights do occupants in energy-efficient smart buildings have concerning data privacy and informed consent, and how are these rights upheld through existing mechanisms, technologies, and regulatory frameworks?
RQ3	How effective are current regulations in addressing privacy concerns in smart buildings, and what are the gaps and limitations that require additional legislative action to safeguard the privacy of occupants in these environments?

3.2. Review Protocol

This section explains the methods used in this SLR, including the search strategy, inclusion and exclusion criteria, data extraction, quality assessment, and data synthesis.

3.2.1. Search Strategies

The search strategies began with an automated search across three databases. The automated search phrases include the keywords privacy, smart building, or energy building, and risk or right or regulation. Initially, 509 articles were obtained during this automated search. The automated search results were filtered based on their title, keywords, and abstract.

The articles were then filtered through the inclusion and exclusion criteria shown in Table 2. In this SLR, articles on smart buildings that were not related to the study of privacy in energy efficiency were excluded.

Table 2. Inclusion and exclusion criteria used in the review.

No	Inclusion Criteria	Exclusion Criteria
1.	Articles published in the English language	Articles published in a language other than English
2.	Articles containing “smart building”	Articles that discuss implementing smart buildings
3.	Articles about energy-efficient buildings	Articles that do not discuss energy efficiency
4.	Articles about privacy in smart buildings	Articles that do not discuss privacy in smart buildings related to energy efficiency

3.2.2. Assessment of Quality

The screening procedure conducted above resulted in the identification of a total of 167 articles. All of these articles were then processed through a Quality Assessment Checklist (QAC) to make sure that each addressed a minimum of one RQ. The QAC questions are listed in Table 3. After the QAC process, only 20 articles were shortlisted. These articles were then evaluated in the subsequent stage.

Table 3. Quality Assessment Checklist questions.

	QAC Questions
1	Does the paper mention data collection, storage, and analysis methods used in energy-efficient smart buildings, and how they might pose privacy risks to inhabitants?
2	Does the paper describe any legal and ethical rights of occupants concerning their data privacy and consent? If so, how are these rights being implemented through any mechanisms/technologies/regulatory frameworks?
3	Does the paper discuss the effectiveness of current regulations in addressing privacy concerns in smart buildings?

3.2.3. Data Synthesis

We have listed the 20 articles that satisfy the QAC criteria in Table 4 below. Some articles adhere to the QAC requirements more comprehensively than others, and there are also articles that meet all of the criteria specified within the QAC. The majority of the articles, 60% in total, were derived from the Scopus database, while the remainder of the articles were equally from IEEE and ACM, as shown in Figure 3.

Table 4. Summary of existing work.

Ref	**RQ1**	**RQ2**	**RQ3**	**Database**	**Year**
[16]	√			SCOPUS	2016
[17]	√			SCOPUS	2016
[3]	√			SCOPUS	2021
[18]	√	√		ACM	2020
[9]	√	√	√	SCOPUS	2020
[19]	√			IEEE	2022
[20]	√	√	√	SCOPUS	2021
[21]	√			SCOPUS	2014
[22]	√	√		IEEE	2019
[23]	√			ACM	2017
[24]	√	√	√	IEEE	2023
[25]	√			IEEE	2020
[26]	√	√		SCOPUS	2017
[27]	√	√		SCOPUS	2023
[28]		√	√	SCOPUS	2020
[29]		√		ACM	2019
[30]		√		SCOPUS	2019
[31]		√		SCOPUS	2019
[32]			√	SCOPUS	2018
[33]	√	√		ACM	2020
TOTAL	15	12	5		

The symbol √ indicates that the articles answering the research questions as stated in Table 1.

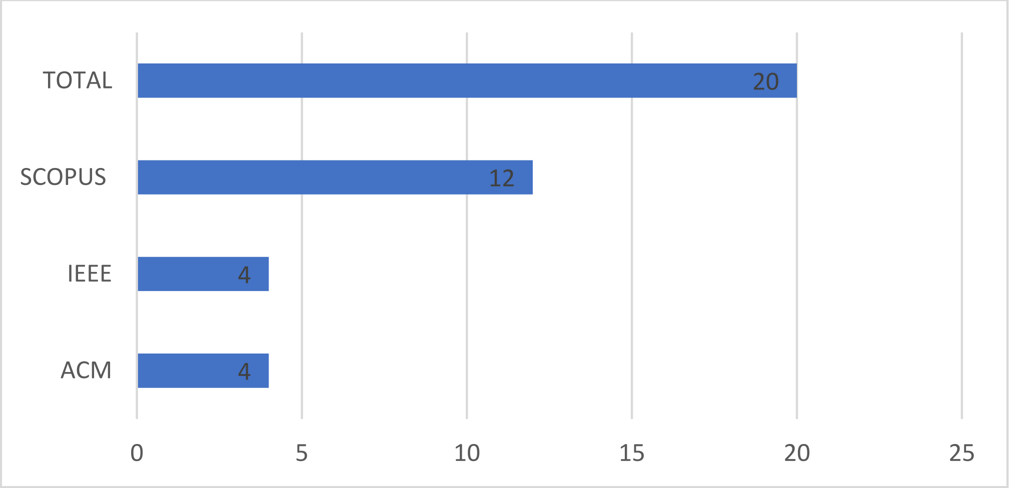

Figure 3. Articles retrieved from the three databases.

Figure 4 shows the distribution of the articles based on the RQs. As shown, the majority of the articles covered RQ1, followed by RQ2 and RQ3. The percentage of articles relating to RQ3 suggests that there is limited research investigating the effectiveness of existing regulations concerning privacy in energy-efficient smart buildings.

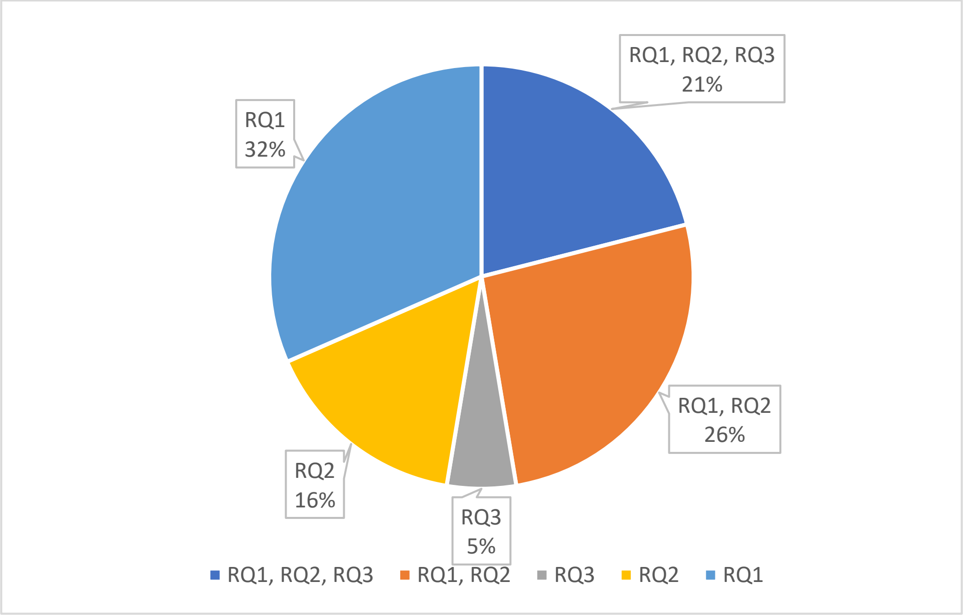

Figure 4. Distribution of articles based on the research questions.

Figure 5 displays the distribution of articles addressing each research question. Most articles have concentrated on RQ1 since 2014, with RQ1-related debates ongoing to the present. In contrast, discussions around RQ2 and RQ3 only commenced in 2017. The trend suggests that studies encompassing all of the research questions covered in this review only started emerging in 2020.

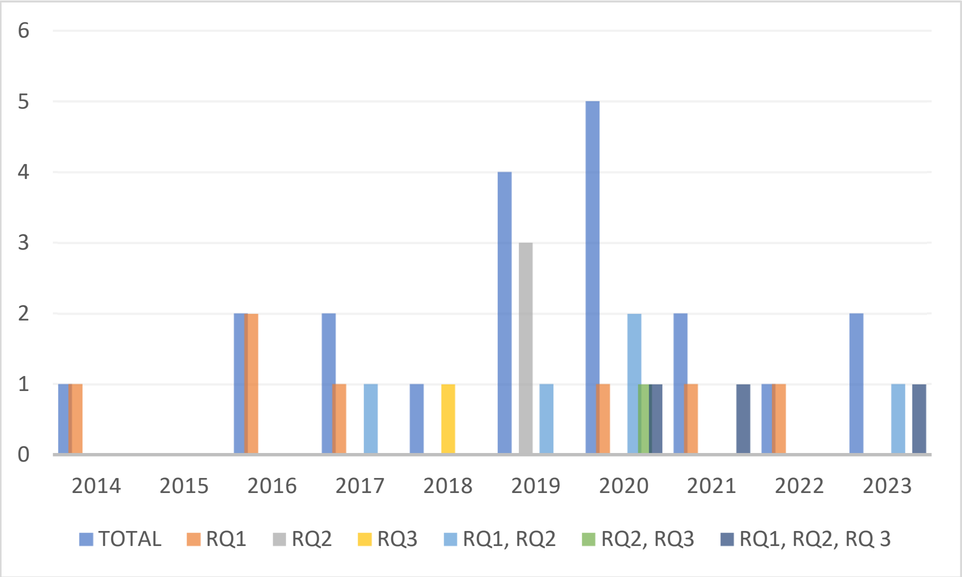

Figure 5. Total distribution of the articles over the years based on the RQs.

In the following section, we provide a comprehensive discussion of our detailed research findings.

4. Results

We have documented our findings based on the three primary objectives of our review. Our first objective was to assess the potential privacy risks associated with data collection, storage, and analysis in energy-efficient smart buildings. Privacy risks emerge when the data collected with the intent of improving energy efficiency inadvertently unveil the activities of the occupants, whether in smart homes or smart buildings. In our second objective, we explored the rights that occupants of smart buildings possess, examining existing regulations and ethical considerations related to safeguarding occupants' privacy.

Our third objective was to evaluate the existing legal regulations that govern the relationship between smart buildings and privacy. We have scrutinized whether current regulations are sufficient to protect individuals' privacy in the context of smart buildings. This comprehensive approach allowed us to analyze and address the various aspects of privacy concerns in energy-efficient smart buildings.

4.1. Privacy Risks in Smart Buildings

A privacy risk is defined in [18] as any loss of control over personal data and information. Out of the 20 articles we reviewed from the provided Table 4 in Section 3.2.3 above, 15 articles, or 75% of the reviewed articles, specifically address privacy risks within energy-efficient smart buildings. We have identified four distinct categories for classifying data in the realm of energy-efficient smart buildings. These categories, namely sensor data, smart meter data, occupancy data, and IoT device data, each play a crucial role in advancing energy efficiency. Collectively, these data types create an environment where resources are utilized more effectively, resulting in reduced energy consumption, enhanced environmental sustainability, and cost savings. In the following sub-section, we elaborate on the ongoing research efforts in this domain.

4.1.1. Sensor Data and Privacy Risks

Sensor data encompasses a wide range of information, including environmental data like temperature, humidity, and air quality, as well as the status of devices like doors and windows. Additionally, these sensors capture user-generated data, providing input for HVAC systems and including information about users' preferences and behavior, crucial for monitoring and optimizing building operations. The findings from articles [9,16,18,25] collectively highlight the privacy risks associated with sensor data collection in energy-efficient smart buildings. These papers delve into the specifics of how sensors, positioned strategically within buildings, can monitor various factors, such as personnel presence, social behavior analysis based on interactions with building management systems, and surveillance in smart office buildings. Concerns are raised about the potential exposure of sensitive data, particularly in office settings where occupants share confidential information.

4.1.2. Smart Meter Data and Privacy Risks

Research focusing on smart meter data, as outlined in articles [19,20,26,27], explores how the use of smart meter data introduces privacy risks for users. The ability to infer detailed information about a household's or individual's activities and lifestyle is a key concern. For example, analyzing patterns of energy consumption captured from smart meter data may reveal when a residence is typically vacant, presenting an opportunity for a break-in. Continuous monitoring of energy usage with smart meters could disclose specific habits and routines, leading to privacy violations such as stalking, targeted advertising, or unauthorized profiling.

4.1.3. Occupancy Data and Privacy Risks

The authors of [3,21–24] extensively explore the privacy implications associated with the collection of occupancy data in smart buildings. Occupancy data, which are collected via occupancy detection sensors, gather information about the presence and location of occupants within a building. While this information is crucial for tasks like the real-time control of building systems, its comprehensive collection without adequate privacy protections can result in a breach of user privacy. Monitoring these data can be perceived as intrusive, as it involves collecting information on the presence and movements of building occupants, potentially revealing their personal routines, habits, and lifestyle information.

4.1.4. IoT Device Data and Privacy Risks

In [17], it is highlighted that IoT devices in smart homes, designed to enhance energy efficiency, introduce privacy and security risks due to extensive connectivity. This enhanced connectivity can potentially result in privacy breaches, identity theft, and financial losses. Similarly, article [33] discusses the utilization of IoT technologies to enhance operations and services within smart buildings. However, this practice opens the door to the collection of sensitive data without users' awareness or control, thereby posing a privacy risk.

We have summarized our findings in Table 5, below. Our analysis indicates that in energy-efficient smart buildings, four types of data are collected. This data collection is facilitated by infrastructure built upon the Internet of Things (IoT) and sensors, which serve as the foundation of these smart buildings. These sensors are seamlessly integrated into the IoT environment, creating an energy-efficient and ecologically conscious environment. Together, these sensors accumulate various types of data that cater to the requirements of the smart buildings and their occupants. Nonetheless, a significant challenge arises from the inability of sensors to differentiate between environmental data and data related to users or occupants. This analysis highlights the necessity of addressing and mitigating these privacy risks, which is essential to strike a balance between the benefits of energy-efficient smart buildings and preserving individual privacy.

Understanding the privacy risks linked to energy-efficient smart buildings necessitates familiarity with rights, ethical consent practices, and current regulations tailored to address privacy issues in this domain. These aspects were explored in the following subsection.

Table 5. Reviews on works related to privacy risks.

Data Type	Ref No.	Definition of Data Type	Example of Privacy Risk
Sensor Data	[9,16,18,25]	Data gathered from sensors within a building, including environmental conditions and device status.	Revealing occupants' daily routines by analyzing environmental data, e.g., identifying when they are present and their preferred comfort settings.
Smart Meter Data	[19,20,26,27]	Data collected via smart meters, recording energy use and consumption by occupants in the buildings.	Inferring detailed information about household activities and lifestyles from energy consumption patterns, potentially indicating vulnerable times for break-ins.
Occupancy Data	[3,21–24]	Data collected from occupancy detection sensors, providing information about the presence of occupants.	Intrusion into occupants' personal lives by revealing when they are present at home, their daily routines, and specific room occupancy, creating a sense of constant surveillance.
IoT Device Data	[17,33]	Data from Internet of Things (IoT) devices in smart buildings, related to energy efficiency and connectivity.	Privacy and security risks due to extensive connectivity, including privacy breaches, identity theft, and financial losses through unauthorized access to IoT devices.

4.2. Privacy Rights, Ethical Consent, and Regulations

Privacy rights operate as rules that protect a user's personal data from being accessed or used without the user's explicit consent [34]. Consent must be defined as a genuine choice that was freely given or presented in a voluntary form [33]. Hence, ethical consent practices refer to moral principles that provide guidance on the responsibilities in managing personal information, applicable to both individuals and organizations. On the other hand, regulation, for example, the GDPR [28], refers to laws or guidelines that are put in place by a regulatory body, usually the government, to monitor, control, or direct different facets of activities that take place in a certain industry or jurisdiction. These regulations are intended to defend the public interest, assure compliance, preserve order, encourage safety, respect moral principles, and deal with a range of societal issues. They work together to guarantee the security and privacy of personal data in this digital world. We examined the collected papers to determine whether there are studies that focus on explaining the legal and ethical rights of occupants concerning their data privacy and consent as well as regulations. We tabulated our findings in Table 6, below.

Table 6. Overview of each article's contributions in the areas of privacy rights, ethical consent, and regulations.

Ref. No.	Privacy Rights	Ethical Consent	Regulations
[18]			√
[9]			√
[20]			√
[22]			√
[24]	√		√
[26]			√
[27]		√	
[28]			√
[29]			√
[30]		√	
[31]			√
[33]		√	

Through our reviews, we identified a solitary article focusing on privacy rights, while three articles delved into ethical considerations, and nine articles scrutinized current regulations pertaining to privacy. The summarized findings are presented in Table 7, where the √ indicates which articles covering which areas.

Table 7. Key points extracted from the reviewed articles.

Ref. No.	Main Focus	Key Point in Relation to Rights, Regulations, and Ethical Concerns
[18]	Current privacy regulations and data sharing practices in certain countries	Discusses how various privacy regulations in different countries, including the EU's GDPR, e-privacy laws, the California Consumer Privacy Act (CCPA), and Australian Privacy Principles, govern the sharing of information.
[9]	Privacy regulations, the GDPR, and CCPA in smart environments	Addresses privacy regulations and their impact on data controllers and service providers in smart environments. Focuses on enhancing data collection and processing while complying with GDPR and CCPA requirements.
[20]	Comparison between national policies across different countries, such as the FIPP and GDPR	Discusses the common approaches taken to establish privacy regulations and principles for residential energy consumers with regard to Advanced Metering Infrastructure (AMI) or smart meter data in many countries, such as Canada, France, the Netherlands, Norway, the UK, and the US. The methods for adopting these privacy principles are outlined below. • Opt-Out Choice: Allowing customers to use their discretion in determining whether they wish to share certain data obtained from smart meters. • Data Guidelines: Establishing protocols for the collection and dissemination of data to safeguard privacy. • Secure Data Handling: Employing secure techniques for storing and managing smart meter data. • Enforcement Agencies: Establishing organizations to oversee and implement privacy regulations.

Table 7. *Cont.*

Ref. No.	Main Focus	Key Point in Relation to Rights, Regulations, and Ethical Concerns
[22]	Establishment of appropriate data access levels for different stakeholders using the Socio-Technical Ethical Process	Introduces the Socio-Technical Ethical Process (STEP), which aims to determine appropriate degrees of data access for different stakeholders. It considers both the General Data Protection Regulation (GDPR) act and the privacy choices of the people in the building. An important observation is the lack of a well-defined method to gain agreement from residents for accessing their data. Occupants are unsure about the level of disclosure that should be applied to their occupancy data, including location information, within smart buildings.
[24]	GDPR and personal data processing	Discusses the EU's GDPR as a regulatory framework for personal data processing in smart buildings, emphasizing individual rights such as the right to be informed, right to rectification, right to restrict processing, right to object, and right to data portability.
[26]	GDPR's impact on IoT devices and businesses	Discusses how the GDPR directly impacts IoT devices. Includes results from a survey indicating that 55% of European businesses have a good understanding of the GDPR and how it affects the handling of customer data. Companies that handle European customer data must also adhere to GDPR requirements. It is emphasized that any service provider wishing to offer services to customers must obtain their consent in order to access their data. The GDPR establishes overall requirements regarding the protection of natural persons with regard to the processing of personal data. Companies violating these EU privacy regulations could face penalties of up to 4% of their worldwide revenue.
[27]	Privacy and ethical challenges associated with IoT devices, with specific attention paid to smart meters	Highlights the importance of addressing the ethical implications of IoT technologies, particularly in the context of smart meters, and the need to establish guidelines for addressing privacy issues. Also highlights research conducted by GPEN, revealing significant findings: 59% of IoT devices do not adequately explain their collection, processing, and usage of personal data; 68% lack a clear explanation of how the collected information is stored; approximately 72% do not provide information on data deletion; and 38% do not offer contact details for customers to voice privacy concerns. The GDPR requires that personal data collected via smart meters and IoT devices must be processed in a manner that is both secure and transparent. This processing must include appropriate measures to ensure the protection of individuals' privacy.

Table 7. *Cont.*

Ref. No.	Main Focus	Key Point in Relation to Rights, Regulations, and Ethical Concerns
[28]	GDPR-compliant smart IoT systems	Emphasizes designing GDPR-compliant IoT systems for intelligent buildings, particularly hotels, while considering the GDPR's regulatory framework for data privacy.
[29]	GDPR empowerment of consumers to control their personal data, especially in IoT devices	Suggests using smart contracts to transform the GDPR's standards, enabling automated verification of changes to personal data using IoT devices. This approach has the potential to enhance data protection and privacy.
[30]	Data ownership and informed consent	Addresses data ownership and informed consent in multi-owned buildings with IoT infrastructure, indirectly considering regulatory frameworks for data privacy. The issue with IoT-generated datasets is that it is unclear who owns the data collected from the sensors and to what extent it is legitimate to capture data in a built environment.
[31]	Building-related energy data and legal frameworks	Discusses the ENERFUND tool's development and procedures for examining the legal framework conditions related to data protection in building-related energy data.
[33]	User-centric informed consent model for IoT data collection	Discusses the need for a user-centric informed consent model in the context of IoT data collection. Emphasizes the GDPR's right to control data collection and the challenges in smart buildings due to data sharing across sectors and borders.

After reviewing these articles, it is noticeable that regulatory frameworks predominantly favor the GDPR over other mechanisms. Within the European Union (EU), all processing of personal data is governed by the GDPR [24]. In [27], the authors demand that personal data gathered from smart meters and IoT devices be processed in a secure and transparent manner to guarantee the safety of user data as stated in GDPR articles, as follows:

- Article 5 states that personal data must be processed to ensure appropriate security, including protection against authorized or unlawful processing, accidental loss, destruction, or damage.
- Article 25 requires that data protection be enforced by design and default: data protection measures must be built into smart meters and IoT devices from the outset and this default setting must ensure the highest level of privacy for the user.
- Article 30 requires organizations to record their processing activities.
- Articles 35 and 36 require organizations to use smart meters and IoT devices to conduct data protection impact assessments to assess and minimize potential privacy risks.

For the papers reviewed above, privacy rights and ethical considerations are not explicitly mentioned in most of the papers. It is implied that when a regulatory framework such as the GDPR is used, all of the privacy rights are taken care of. However, this may not be entirely true.

4.3. Privacy Regulations and Compliance

To ensure the privacy of smart building occupants, most researchers and building operators turn to existing privacy regulations such as the GDPR and CCPA for guidance [9,20,24,28]. However, the GDPR was designed for general privacy protection, and it is not clear how it should be applied to energy-efficient smart building infrastructure [20]. Furthermore, the integration of IoT devices and various sensors in smart building may blur the distinction between environmental data and data related to occupants [24]. In many cases, even though individual sensor data cannot be used to identify individuals and cause privacy breaches, combining different data from multiple sensors may make it possible for individuals and their activities to be inferred. This makes it difficult to ensure GDPR compliance.

In practice, the following approaches are used to comply with the GDPR:

- Provide the option to opt in/opt out of energy efficiency initiatives [9,20];
- Use independent data storage [20];
- Provide rules for data sharing [20];
- Establish a separate monitoring and enforcement agency [20];
- Provide the option to implement privacy preservation techniques such as anonymization, randomization, and perturbation [9];
- Implement data aggregation during data collection [32].

On top of the above, there have also been attempts to incorporate GDPR principles into each IoT layer and operation of a smart building, as described in [28]. However, such approaches remain largely theoretical and at best implemented at a prototype level. No thorough evaluation has ever been conducted to verify whether such approaches can ensure GDPR compliance.

Another factor that makes GDPR compliance difficult is that individual rights and freedom cannot be easily quantified. Furthermore, people's perception of and tolerance towards privacy vary between individuals, and this makes assessment difficult. It has been observed that building occupants are more likely to share data if they believe it is for a purpose that benefits them [24]. This also suggests that even the same person's perception towards privacy may change over time depending on their beliefs and knowledge.

Going forward, it is important to establish a standard protocol and a clear assessment method to determine high-risk data processing in relation to individual rights and freedom. To address the varying perceptions of privacy between individuals, empirical studies need to be conducted to understand occupants' views towards privacy risks in smart buildings so that a correct assessment guideline from the perspective of building occupants can be established [24].

5. Discussion

Based on the literature review conducted, there are actually quite a lot of papers on privacy in smart buildings and smart homes. However, most of them discuss the use of security cameras or smart devices that could potentially cause privacy breaches. Only a small number of these papers talk about energy-efficient smart buildings, where the devices installed are mostly IoT gateways and sensors that collect environmental and energy usage data. The small number of works in this area of research may also imply that most researchers do not consider IoT installation in energy-efficient buildings as presenting any serious privacy issues.

However, as discussed in Section 4.1, the sensor readings collected in an energy-efficient smart building could still cause privacy issues. Even though individual sensor reading may not cause a privacy breach, it is possible for an individual's activity and their whereabouts to be identified by combining data from multiple sensors together over a period of time, thus causing a privacy breach. Realizing this, a number of researchers have attempted to mitigate privacy issues by turning to existing privacy preservation mechanisms and privacy regulations.

With respect to privacy regulations, most researchers refer to the GDPR. The GDPR provides guidelines on the collection and processing of personal data. However, applying the GDPR to energy data collection in smart buildings may not be straightforward because it is difficult to identify whether a particular type of data collected can be linked to an individual or not. As mentioned earlier, even though a particular type of data collected may not be linked to individuals, and therefore not subjected to the GDPR, it may turn out to be otherwise when combined with other types of data. This makes it difficult to ensure

GDPR compliance when evaluating data collection and processing in an energy-efficient smart building.

Another aspect that makes measuring GDPR compliance difficult is the nature of privacy itself. There is no general consensus on what is and is not acceptable when it comes to privacy. Different individuals view privacy differently. In general, when an individual sign an agreement that allows for the collection and processing of their personal data, then privacy is no longer an issue. In fact, this is the approach taken by many service providers, including smart home service providers. However, this may not be possible in a smart building environment where there are a large number of occupants and visitors.

Researchers can help to alleviate this issue by making it easy for building occupants to make an informed decision regarding their privacy. With respect to energy-efficient smart buildings, perhaps what is needed is a method to evaluate the privacy level of a building based on the installed devices, types of data collected, and the kind of processing performed on the data. With the privacy level clearly identified and made known to building occupants, they can then make an informed and conscious decision with respect to their use of the building.

6. Conclusions

This article delves into the consideration of privacy within energy-efficient smart buildings, examining the associated risks, occupants' rights, and relevant regulations. It highlights the underexplored nature of this field, emphasizing the scarcity of works addressing rights and regulations in the context of smart buildings. Our analysis identifies four distinct data types linked to privacy risks: sensor data revealing occupants' routines, smart meter data providing insights into household activities, occupancy data delving into personal lives, and IoT device data introducing privacy and security considerations.

Our review of existing regulatory frameworks, including the GDPR, CCPA, and Australian Privacy Principles, reveals their crucial role in safeguarding user privacy in smart buildings. However, challenges emerge in bridging the gap between established regulations and the evolving smart building landscape, requiring attention be paid to defining data ownership, establishing informed consent mechanisms, and addressing IoT device deployment and personal data protection.

There is a need for the continuous adaptation and refinement of these regulations, which are essential to effectively addressing the multifaceted nature of smart buildings. It is imperative to develop comprehensive regulatory and ethical guidelines that not only harness the benefits of energy-efficient smart buildings, but also safeguard individual privacy, ensuring a harmonious balance between technological advancements and personal data protection.

Author Contributions: Conceptualization, B.N.J., A.A.B., S.Y., A.A.G. and S.S.S.; investigation B.N.J., A.A.B., S.Y., A.A.G. and S.S.S., methodology, A.A.G. and S.S.S.; writing—original draft preparation, A.A.B., S.Y., A.A.G., S.S.S. and B.N.J.; writing—review and editing, A.A.B., S.Y., A.A.G., S.S.S. and B.N.J.; visualization, A.A.G. and S.S.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research was supported by the Tan Sri Leo Moggie Research Fund, Universiti Tenaga Nasional.

Data Availability Statement: This paper generates no data.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Data Protection and Privacy Legislation Worldwide. Available online: https://unctad.org/page/data-protection-and-privacy-legislation-worldwide (accessed on 1 December 2023).
2. EUR-Lex—32016R0679—EN—EUR-Lex. Available online: https://eur-lex.europa.eu/eli/reg/2016/679/oj (accessed on 1 December 2023).

3. Ahmad, J.; Larijani, H.; Emmanuel, R.; Mannion, M.; Javed, A. Occupancy detection in non-residential buildings—A survey and novel privacy preserved occupancy monitoring solution. *Appl. Comput. Inform.* **2021**, *17*, 279–295. [CrossRef]
4. Naria, I.P.; Sulistyo, S.; Widyawan. Security and Privacy Issue in Internet of Things, Smart Building System: A Review. In Proceedings of the 2022 International Symposium on Information Technology and Digital Innovation (ISITDI), Padang, Indonesia, 27–28 July 2022; IEEE: New York, NY, USA, 2022; pp. 177–180. [CrossRef]
5. Llaria, A.; Santos, J.D.; Terrasson, G.; Boussaada, Z.; Merlo, C.; Curea, O. Intelligent Buildings in Smart Grids: A Survey on Security and Privacy Issues Related to Energy Management. *Energies* **2021**, *14*, 2733. [CrossRef]
6. Janghyun, K.; Barry, H.; Tianzhen, H.; Marc, A.P. A review of preserving privacy in data collected from buildings with differential privacy. *J. Build. Eng.* **2022**, *56*, 104724. [CrossRef]
7. Buckman, A.H.; Mayfield, M.; Beck, S.B.M. What is a Smart Building? *Smart Sustain. Built Environ.* **2014**, *3*, 92–109. [CrossRef]
8. Metallidou, C.K.; Psannis, K.E.; Egyptiadou, E.A. Energy Efficiency in Smart Buildings: IoT Approaches. *IEEE Access* **2020**, *8*, 63679–63699. [CrossRef]
9. Ghayyur, S.; Pappachan, P.; Wang, G.; Mehrotra, S.; Venkatasubramanian, N. Designing privacy preserving data sharing middleware for internet of things. In Proceedings of the DATA 2020—3rd Workshop on Data Acquisition to Analysis, Part of SenSys 2020, BuildSys 2020, Virtual Event, 16–19 November 2020; Article No. 30, pp. 1–6. [CrossRef]
10. Taher, R.; Mehrnezhad, M.; Morisset, C. '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 *Socio-Technical Aspects in Security, STAST2022*; University of Luxemburg: Esch-sur-Alzette, Luxembourg, 2022; pp. 1–20.
11. Harper, S.; Mehrnezhad, M.; Mace, J. User Privacy Concerns in Commercial Smart Buildings1. *J. Comput. Secur.* **2022**, *30*, 465–497. [CrossRef]
12. Schwee, J.H.; Sangogboye, F.C.; Kjærgaard, M.B. Evaluating Practical Privacy Attacks for Building Data Anonymized by Standard Methods. In Proceedings of the International Workshop on Security and Privacy for the Internet-of-Things, Montreal, QC, Canada, 15 April 2019; pp. 11–14.
13. California Consumer Privacy Act of 2018. Available online: https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CIV&division=3.&title=1.81.5.&part=4.&chapter=&article= (accessed on 1 December 2023).
14. U.S. Government Accountability Office. Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information. 2008. Available online: https://www.gao.gov/products/gao-08-536 (accessed on 1 December 2023).
15. Moher, D.; Liberati, A.; Tetzlaff, J.; Altman, D.G. Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement. *Int. J. Surg.* **2010**, *8*, 336–341. [CrossRef] [PubMed]
16. Mundt, T.; Wickboldt, P. Security in building automation systems—A first analysis. In Proceedings of the 2016 International Conference on Cyber Security and Protection of Digital Services, Cyber Security 2016, London, UK, 13–14 June 2016; pp. 1–8. [CrossRef]
17. Plachkinova, M.; Vo, A.; Alluhaidan, A. Emerging trends in smart home security, privacy, and digital forensics. In Proceedings of the AMCIS 2016: Surfing the IT Innovation Wave—22nd Americas Conference on Information Systems, San Diego, CA, USA, 11–14 August 2016; pp. 1–9.
18. Schwee, J.H.; Sangogboye, F.C.; Salim, F.D.; Kjærgaard, M.B. Tool-chain for supporting Privacy Risk Assessments. In Proceedings of the BuildSys 2020—Proceedings of the 7th ACM International Conference on Systems for Energy-Efficient Buildings, Cities, and Transportation, Virtual Event, 18–20 November 2020; pp. 140–149. [CrossRef]
19. Bos, J.W.; De Vis, M.; Faes, C.; González-Deleito, N.; Hristoskova, A.; Klein, S.; Rajendran, S. Unsupervised, Federated and Privacy-Preserving Detection of Anomalous Electricity Consumption in Real-World Scenarios. In Proceedings of the 2022 IEEE Sustainable Power and Energy Conference, iSPEC 2022, Perth, Australia, 4–7 December 2022; pp. 1–5. [CrossRef]
20. Lee, D.; Hess, D.J. Data privacy and residential smart meters: Comparative analysis and harmonization potential. *Util Policy* **2021**, *70*, 101188. [CrossRef]
21. Wang, X.; Tague, P. Non-Invasive User Tracking via Passive Sensing. In Proceedings of the 2014 Workshop on Artificial Intelligent and Security Workshop, Scottsdale, AZ, USA, 7 November 2014; ACM: New York, NY, USA, 2014; pp. 113–124. [CrossRef]
22. Mace, J.C.; Morisset, C.; Smith, L. A Socio-technical Ethical Process for Managing Access to Smart Building Data. In *Living in the Internet of Things (IoT 2019)*; Institution of Engineering and Technology: Stevenage, UK, 2019; pp. 1–6. [CrossRef]
23. Jia, R.; Dong, R.; Sastry, S.S.; Spanos, C.J. Privacy-enhanced architecture for occupancy-based HVAC control. In Proceedings of the 2017 ACM/IEEE 8th International Conference on Cyber-Physical Systems, ICCPS 2017 (Part of CPS Week), Pittsburgh, PA, USA, 18–20 April 2017; pp. 177–186. [CrossRef]
24. Leesakul, N.; Morisset, C. Position Paper: The role of law in achieving privacy and security measures in smart buildings from the GDPR context. In Proceedings of the 8th IEEE European Symposium on Security and Privacy Workshops, Euro S and PW 2023, Delft, The Netherlands, 3–7 July 2023; pp. 619–626. [CrossRef]
25. Alisic, R.; Molinari, M.; Pare, P.E.; Sandberg, H. Ensuring privacy of occupancy changes in smart buildings. In Proceedings of the CCTA 2020—4th IEEE Conference on Control Technology and Applications, Montreal, QC, Canada, 24–26 August 2020; pp. 871–876. [CrossRef]
26. Mateev, M. Iot, smart energy systems, personal data and encryption in the gdpr. *Int. Multidiscip. Sci. GeoConference Surv. Geol. Min. Ecol. Manag. SGEM* **2017**, *17*, 921–928. [CrossRef]

27. Vishi, K. Privacy and Ethical Considerations of Smart Environments: A Philosophical Approach on Smart Meters. In *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*; LNCS: Berlin, Germany, 2023; Volume 14112, pp. 303–313. [CrossRef]
28. Metallidou, C.; Psannis, K.E.; Alexandropoulou-Egyptiadou, E. An Efficient IoT System Respecting the GDPR. In Proceedings of the 2020 3rd World Symposium on Communication Engineering (WSCE), Thessaloniki, Greece, 9–11 October 2020; IEEE: New York, NY, USA, 2020; pp. 79–83. [CrossRef]
29. Barati, M.; Petri, I.; Rana, O.F. Developing GDPR compliant user data policies for internet of things. In Proceedings of the UCC 2019—Proceedings of the 12th IEEE/ACM International Conference on Utility and Cloud Computing, Auckland, New Zealand, 2–5 December 2019; pp. 133–141. [CrossRef]
30. Atazadeh, B.; Olfat, H.; Rismanchi, B.; Shojaei, D.; Rajabifard, A. Utilizing a Building Information Modelling Environment to Communicate the Legal Ownership of Internet of Things-Generated Data in Multi-Owned Buildings. *Electronics* **2019**, *8*, 1258. [CrossRef]
31. Geissler, S.; Charalambides, A.G.; Hanratty, M. Public Access to Building Related Energy Data for Better Decision Making in Implementing Energy Efficiency Strategies: Legal Barriers and Technical Challenges. *Energies* **2019**, *12*, 2029. [CrossRef]
32. Livingston, O.V.; Pulsipher, T.C.; Anderson, D.M.; Vlachokostas, A.; Wang, N. An analysis of utility meter data aggregation and tenant privacy to support energy use disclosure in commercial buildings. *Energy* **2018**, *159*, 302–309. [CrossRef]
33. Pathmabandu, C.; Grundy, J.; Chhetri, M.B.; Baig, Z. An informed consent model for managing the privacy paradox in smart buildings. In Proceedings of the 35th IEEE/ACM International Conference on Automated Software Engineering Workshops, Virtual Event Australia, 21–25 September 2020; ACM: New York, NY, USA, 2020; pp. 19–26. [CrossRef]
34. Alibeigi, A.; Munir, A.B.; Karim, M.E. Right to privacy, a complicated concept to review. *Libr. Philos. Pract.* **2019**, *2019*, 2841. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.