International Journal of Intelligent Information Systems
2022; 11(3): 39-50
http://www.sciencepublishinggroup.com/j/ijiis
doi: 10.11648/j.ijiis.20221103.12
ISSN: 2328-7675 (Print); ISSN: 2328-7683 (Online)

Transnational Flow of Personal Data in Home and Office Devices

Robert Walters[1], Sinta Dewi Rosadi[2]

[1]Victoria Law School, Victoria University, Melbourne, Australia
[2]Faculty of Law, University of Padjajaran, Bandung, Indonesia

Email address:
Robert.Walters@vu.edu.au (R. Walters)

To cite this article:
Robert Walters, Sinta Dewi Rosadi. Transnational Flow of Personal Data in Home and Office Devices. *International Journal of Intelligent Information Systems*. Vol. 11, No. 3, 2022, pp. 39-50. doi: 10.11648/j.ijiis.20221103.12

Received: May 18, 2022; **Accepted**: June 9, 2022; **Published**: July 18, 2022

Abstract: The world is embracing Artificial Intelligence (AI) at a rapid rate, and over the forthcoming decade it is likely to pervade the daily lives of everybody. Countries are developing, embracing and adopting AI at varying rates, some more rapidly than others. On the one hand, the application of AI in managing the smart home infrastructure will pave the way for personal data to be gathered from the automated devices. It will be that advanced, the technology will be able to predict user behaviour, provide maintenance data, help enhance data security and privacy. This can be achieved, by connecting devices throughout the homes by many different devices. Nonetheless, as people begin to adopt new technology in the home, or otherwise known as Smart Home technology (robots, televisions, fridges, toys etc.), the access to personal data will be on an unprecedented level. Conversely, the privacy intrusions may out-weigh the benefits of the technology. Apart from the social and economic benefits that AI will bring into the home, it will have it downsides. There is an emerging debate as to the safety of personal data, and privacy from these devices. In other words, what has emerged is the notion of dataveillance or behavioural data that, is able to detect and store specific data on and individual, enabling others to learn intimate knowledge of actions, moods and expression, amongst others. Arguably, some of the most vulnerable cohorts will be children, the disabled and elderly, from the use of this technology, and the personal data that entities are able to capture, and subsequently use for financial gain. Furthermore, problematic is the development of 'behavioural data'. Behavioural data, has the ability to create significant bias based on race, ethnicity, religion, disability and language. Put another way, behavioural data has many similarities to dataveillance. This paper will briefly highlight how transnational data flows from the devices have the potential to create and restrict competition. The paper further confirms that a recent study in 2021, demonstrated that as this economic activity (data flows) grows there are increasing security concerns and issues that expose personal and commercial data. Further research is needed to reconcile the law with the technology, to ensure data flows are providing their intended economic benefits, with that of protecting the personal data captured and used by in home and office devices.

Keywords: Privacy, Data Flows, Smart Home-Office Devices, Law

1. Introduction

Artificial Intelligence (AI) is rapidly developing, and it is predicted that over the coming decade people will find AI technology in the home, office, business and general community on a large scale. [1] Robert Walters and Marko Novak are of the view that AI will pervade nearly every aspect of our lives in the coming decades. The world is seeing the transformation of AI technology being used by governments and the broader community for security. Over the past decade people only have to travel to the major airports around the world and through the central business districts of major cities to find AI surveillance at work. [3] When coupled with data protection and cyber security, Roger Clarke and Graham Greenleaf use the term dataveillance. The authors highlight how 'dataveillance is not new and can be traced back to the 1980s. In their view, this form per data use is best described as the systematic creation and/or use of personal data for the investigation or monitoring of the actions or communications of one or more persons'. [2]

Today, AI can be found in many devices already in our

homes that we call "smart" because they operate in a more intelligent way that (technical) machines used to operate, for example, smart phones, smart watches, robot vacuum cleaners and lawn mowers, self-driving cars, and personal drones. Centrally, AI is emerging in robotics, technological industry, healthcare (in particular, medical diagnosing and surgery). The technology can be found in transportation, military, government and public administration, insurance, finance, art, amongst many others. The authors go onto say that, it has been incrementally used in the area of law, especially by law firms (predictive justice meaning the prediction of judicial decisions). AI is already being developed to be able to predict whether an entity is in financial stress [2], and may declared insolvency. This predictive technology while having many economic benefits, when used privately exposes people to significant levels of compromise in their personal data.

This article will highlight some of the issues emerging in this area of law and technology. The article demonstrates that there is a lack of international agreement on what AI constitutes, and nation states are largely going it alone to develop their own legal framework. Moreover, AI is going to challenge individuals across the community, particularly vulnerable groups such as children, those with a disability and elderly to be captured by this technology is only beginning to be understood. The potential ramifications for bias and discrimination based on sex, ethnicity, and religion, amongst others could be enormous. As AI evolves a more comprehensive study will be needed to better understand whether the developers of the technology have been successful in building adequate safeguards into the systems and platforms to protect personal data from illegal collection and use. It will also require to confirm whether current trade-consumer practices law is adequate to regulate this at the point of sale of these devices, particularly in relation to protecting personal data. [4]

Yet, as AI begins to take a hold in the home, it is becoming increasingly apparent that this technology depends on the collection and processing of vast amounts of data which can potentially include personal and even sensitive data. Anonymization techniques – which have served as a wildcard, allow companies to process anonymised personal data, which could be more easily circumvented with the use of AI. [6] More problematic is the very small amount of data that is needed to uniquely identify an individual. In a recent study, it was found that 87% of the population in the United States could be uniquely identified based only on cross-referencing a 5-digit ZIP code, gender, and date of birth. [5] AI exponentially strengthens data processing capabilities. If anonymised personal data becomes part of a large data set, AI can de-anonymise this data based on inferences from cross-referencing information. More problematic, it this blurs the distinction between personal and non-personal data, which is a cornerstone of present legislation. [6] Walters and Novak make the point that, here in lies a significant issue, whereby, the current data protection laws are at odds with AI technology. Furthermore, they argue that 'it is not apparent, at this early stage whether the technology has advanced enough whereby AI developers have devised a way to secure and protect personal data. As the technology evolves, there is a good chance that this is likely to be realised'. [6] However, the lack of a clear definition of AI, has, to date, been not only problematic, it allows states to assert their sovereign needs by developing their own definition. Thus, it is argued that, at a minimum, states need to have a broader discussion and engage one another to develop an internationally agreed definition of AI, particularly for those devices that will be used in the residential home and office.

Road Map

Part I of this paper discusses the current laws surrounding AI. It will demonstrate how there is a lack of a formal legal definition. On the other side, personal data has been comprehensively defined, however, its alignment with AI is not well understood. Part II highlights the current penetration of the Internet and how that will relate to AI devices, and the potential for large scale collection of personal data. It highlights how data flows through and over smart homes and office devices can restrict and create competition issues. Part III, concludes this paper and provides a way forward to reconcile the issues faced by smart home devices.

2. Artificial Intelligence Defined

However, there is no internationally agreed definition of AI. [6] To date, there is no single definition of AI that has been accepted by all technology practitioners, or legal practitioners. Walters and Coghlan have identified that some define or otherwise categories AI broadly as a computerized system exhibiting behavior commonly thought of as requiring intelligence. However, others define AI as a system, capable of rationally solving complex problems or taking appropriate action to achieve its goals in real-world circumstances. The authors trace the beginnings of an emerging definition to 1985, whereby Phillip Jackson, defined AI as the ability of machines to do things that people would say require intelligence. The phrase sometimes refers to intelligent machines themselves. [7] Therefore, artificial intelligence attempts to emulate the mental steps of human beings. Such mental steps include understanding languages, responding to questions, identifying patterns, solving problems, and learning through experience. [8] Thus, the definition from 1985 falls short of what AI is today. Moreover, the Oxford English Dictionary arguably has taken a very broad approach to defining AI. In other words, artificial intelligence has been defined by the Oxford Dictionary to be the field of study that deals with the capacity of a machine to simulate or surpass intelligent human behaviour. While it is noted that at the international level there has been considerable work to gain agreement in relation to AI being used in, and by the military and motor vehicle automation, it is out of scope of this paper to examine these reports of conventions.

The US have developed a definition of AI. During the 115th Congress,[9] thirty-nine bills have been introduced that

have the phrase "artificial intelligence" in the text of the bill. Four of these bills have been enacted into law. Section 238 of the John S. McCain National Defence Authorization Act for Fiscal Year 2019 directs the Department of Defence to undertake several activities regarding AI. [10] Subsection (b) requires the Secretary of Defence to appoint a coordinator who will oversee and direct the activities of the Department "relating to the development and demonstration of artificial intelligence and machine learning."[11] Subsection (g) provides the following definition of AI: (g) in this section, the term "artificial intelligence" includes:

1) 'Any artificial system that performs tasks under varying and unpredictable circumstance without significant human oversight, or that can learn from experience and improve performance when exposed to data sets.
2) An artificial system developed in computer software, physical hardware, or other context that solves tasks requiring human-like perception, cognition, planning, learning, communication, or physical action.
3) An artificial system designed to think or act like a human, Including cognitive architectures and neural networks.
4) A set of techniques, including machine learning that is designed to approximate a cognitive task.
5) An artificial system designed to act rationally, including an intelligent software agent or embodied robot that achieves goals using perception, planning, reasoning, learning, communicating, decision making, and acting.' [11]

Moreover, subsection (f) instructs the Secretary of Defence to delineate a definition of the term artificial intelligence for use within the Department no later than one year after the law's enactment. Arguably, the definition does, in part, direct the community generally on what AI constitutes, arguably as technology continues to evolve this definition is likely to change. The High-Level Expert Group on Artificial Intelligence (AI HLEG), European Commission, released draft AI ethics guidelines. It proposed a broad definition of AI that would include:

'Artificial intelligence (AI) refers to systems designed by humans that, given a complex goal, act in the physical or digital world by perceiving their environment, interpreting the collected structured or unstructured data, reasoning on the knowledge derived from this data and deciding the best action(s) to take (according to pre-defined parameters) to achieve the given goal. AI systems can also be designed to learn to adapt their behaviour by analyzing how the environment is affected by their previous actions. As a scientific discipline, AI includes several approaches and techniques, such as machine learning (of which deep learning and reinforcement learning are specific examples), machine reasoning (which includes planning, scheduling, knowledge representation and reasoning, search, and optimization), and robotics (which includes control, perception, sensors and actuators, as well as the integration of all other techniques into cyber- physical systems).' [12]

However, artificial intelligence has not gained a formal legal definition in the EU. Mihalis Kritikos argues that:

'Defining the precise object of regulation in dynamic technological domains is a challenge in itself. Given that AI is still an open-ended notion that refers to a very wide range of products and applications, there is no transnational agreement on a commonly accepted working definition, neither at the technical nor the legal/policy level. As there is no legal and political consensus over what AI is, a plurality of definitions has emerged in Europe and worldwide that are either too inclusive or too sector- specific. This fragmented conceptual landscape may prevent the immediate development of a *lex robotica* and possibly undermine all efforts to create a common legal nomenclature, which is particularly instrumental for the drafting, adoption and effective implementation of binding legal norms. Alternatively, a broad and technology-neutral definition that is based on the fulfilment of a variety of structural criteria, including the level of autonomy and the function, may be a more plausible option.' [13]

Walters and Novak make the point that this poses significant challenges to not only AI, cyber security but also personal data. [14] In our view a definition of AI is unlikely to be settled at the national or supranational level anytime soon, or, until the courts become involved. Nonetheless, Kritikos goes on to say that the problem of definitional ambiguity is closely associated with the issue of AI's legal classification and the categorization of its various applications. [13] Arguably, this has to be a major impediment to the protecting privacy and personal data that will be collected from home devices. What will emerge is the ever growing interconnectedness between AI and data protection law. Moreover, the definition of personal data varies from country to country and will pose challenges to AI technology.

Personal Data & Privacy - Defined

The challenge for privacy and personal data is how state view these two concepts. While they are interrelated, they are also quite separate. According to Warrens and Louis D. Brandeis (1890) which stated that: "privacy is the right to enjoy life intellectually, emotional life and the heightening of sensation which came with the advance of civilization, which demanded legal recognition. [15] For protection and securing the person Warren & Brandeis also agreed with the invention concept of privacy by Judge Cooley that called as right to be let alone. [16] On the other side, the notion of privacy is proposed by Judith Jarvis Thomson, that technology can amplifying the violation of privacy, although the offender didn't even near to the person. [16] Shoshana Zuboff described information technology have ability to create "*informate*" and "*automate*" and to revealed human behaviour. [17] Thus, privacy must be protected under regulation and the level of protection must anticipate the advent of technology.

The reasons why privacy must be protected is that for some countries and jurisdictions, it is a fundamental right. On the other hand, it is well understood that privacy has little to no place in society, for those countries that have not adopted

Western thought. A good example is Singapore, which does not recognize a right to privacy. The former Prime Minister Lee Kuan Yew's dismissal of the idea is often invoked in such discussions:

> "I am often accused of interfering in the private lives of citizens... Had I not done that, we wouldn't be here today. And I say without the slightest remorse: that we wouldn't be here, we would not have made economic progress, if we had not intervened on very personal matters – who your neighbour is, how you live, the noise you make, how you spit, or what language you use." [18]

This stance by Singapore highlights how not recognising such a right works for them. The EU on the other hand has placed human rights, and the right to privacy over the Internet as a core policy value. That is, the European Union regulation on privacy began in the 1950 European Convention for the Protection of Human Rights (ECHR). This was at a time when European had come out of World War II, which had a profound impact on how future rights would be viewed and applied across the territory. Privacy would become a fundamental right. In reinforcing this point, Article 8 of the ECHR states that: "[e]everyone has the right to respect for his/her private and family life, his/her home and his/her correspondence" (Rights, 1950). [19] This right is broadly interpreted and in terms of technology that is neutral so that it applies to the electronic market and online environment. Therefore, starting from theoretical and normative propositions, all forms of information that identify people, both physical and non- physical (cyber), taken from spaces that are human privacy are referred to as personal data (Library of Congress). This level of recognition of privacy as a right not only competes with other economic and social policy areas, it reinforces the sovereign right of state actors to develop laws that suit their needs.

Nonetheless, and in building relationships with others, someone must cover a part of his personal life so that he/she can maintain his/her position at a certain level. Secondly, someone in his/her life needs time to be alone (solitude) therefore the privacy is needed by someone. Thirdly, the privacy is an independent right and does not depend on other rights, but this right will be lost if the person publishes personal matters to the public. Fourthly, the privacy also includes the right of a person to conduct domestic relations including how a person fosters his/her marriage, fostering his/her family and other people should not know the personal relationship therefore later Warren calls it "the right against the word". Fifthly, another reason why privacy deserves legal protection, because the losses suffered are difficult to assess. The loss is felt to be far greater than the physical loss, because it has disturbed his personal life, so that if there is any loss suffered, the victim must be compensated. Consent and privacy deserve legal protection to elude the losses suffered. The loss is felt to be far greater than the physical loss because it has disrupted personal life or legal *injuria.* [15] In expressing his concept, Warren also argued that privacy is not absolute and can be opened to the public in two ways are: (1) does not close the possibility of publicizing one's personal data in the public interest; and (2) the person concerned has given permission for his/her personal data to be distributed publicly.

According to Post, all form of information (including knowledge of one's personality is information that can be categorized as privacy. [21] Post argument is also similar with Jeffrey Rosen that technology can endanger intimate personal information. [22] Solove explained there are for basic group of harmful activities: 1) information collection, 2) information processing, 3) information dissemination, and 4) invasion. [24] Solove goes onto say that that these groups have a level of impact whether positive or negative to the right to be let alone, ability to have limited access to the self, 3) conceal of secrecy, 4) control over personal information, 5) personhood protection, and 6) intimacy control. Jon Mills describes privacy as a layer that can be mapped into four sphere of privacy, namely: 1) personal information; 2) property; 3) physical space; and 4) autonomy that can be described below. [24]

Jon Mills takes the view that there are four layers to privacy. First, privacy constitute the public disclosure of personal data information, which can be viewed openly be everyone. Second, today there are many platforms on the Internet that, enable this to occur. Moving clockwise, Mills makes the point that everyone has a level of autonomy, and the freedom to choose who they wish to engage. Third, Mills is of the view that physical space is very important. Taking this position, we agree with Mills. However, today technology has blurred to physical space between people over the Internet. In reality, technology has driven people apart, whereby they do not meet in person as much as they used too. Yet, they are more engaged than ever, once connected online. The physical space Mills is referring to is that space on the Internet where people's data is compromised with ease. Lastly, Mills makes the point about property. However, out personal data does not have a property right attached to it – as yet.

Thus, based on the above, privacy is the by-product of data protection and controlling the use of personal data. On the other hand, and highlighted by Graham Greenleaf, personal data has been categorised data that is to be protected according to the national laws. However, data protection law varies from state to state, and subsequently, the definition of personal data varies. One the other hand, it is out of scope of this paper to compare the varying approach taken by national laws to define personal data. He notes that in 2017-18, the number of countries that have enacted data privacy laws has risen from 120 to 132, a 10% increase. These 132 jurisdictions have data privacy laws covering both the private sector and public sectors in most cases, and which meet at least minimum formal standards based on international agreements.[1] While Greenleaf note that, while there has been a significant expansion in data protection law, and the definition of personal data varies greatly. However, and we agree with Greenleaf that when it comes to smart home and personal devices, data protection law means little unless they are enforced effectively. [1]

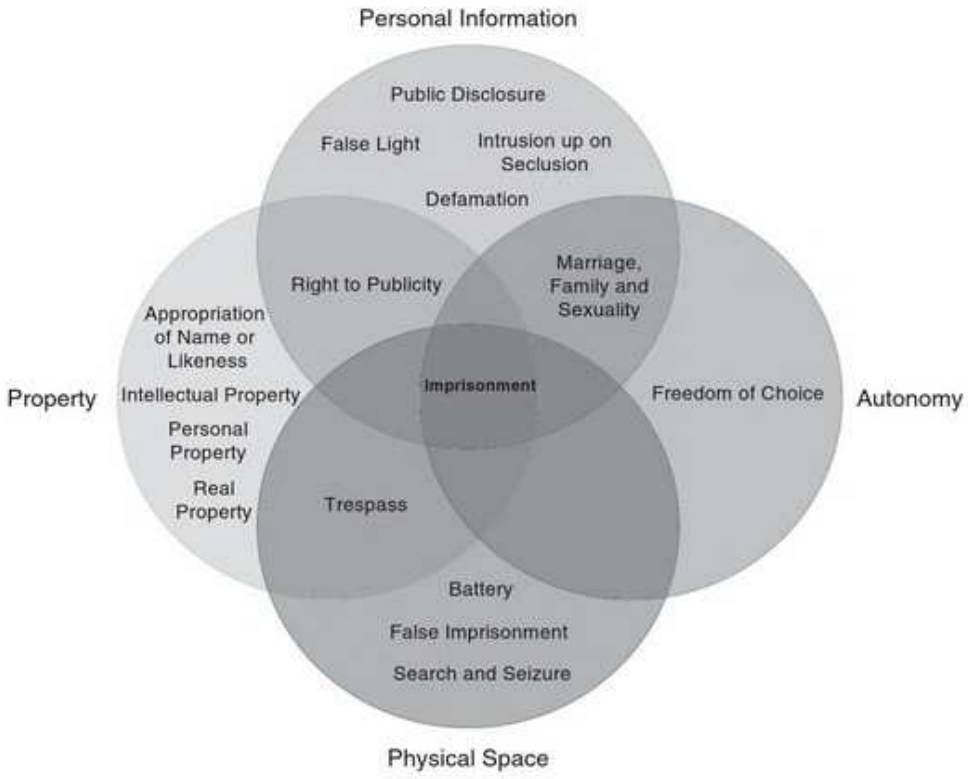

Figure 1. *Four Layers of Privacy [2].*

Nonetheless, as highlighted above, the various types of personal data that can and will be captured by smart homes and personal devices could be significant. Based on this, personal data that is protected under data protection laws can be further categorised as behavioural data and that, under these devices is used for dataveillance. Dataveillance is where various forms of surveillance give rise to recording that data. [30] Roger Clarke and Graham Greenleaf argue that, this type of activity can include but not limited to, physical surveillance that records audio, image or video that can be associated with an individual. It can also constitute the communication between two or more individuals such as ephemeral messages (emails, sms, call data, IPSs logs). More pervasively, dataveillance logs and recordings, search terms used, webpages fetched, reading material downloads, biometrics that can measure heart rate, and identify a person. [2] What is not fully understood is the security around the smart home and personal devices, and how this dataveillance is used by state actors and non-state actors who capture and use this data. On the other side, and out another way, behavioural data [2] can detect and measure the behaviours of individuals. [31] It captures similar data to that described above by Clarke and Greenleaf. On the other side, personal data mining mechanisms and methods are employed patent is extended or adjust under to identify relevant information that otherwise would likely remain undiscovered. [32] Users supply personal data that can be analysed in conjunction with data associated with a plurality of other users to provide useful information that can improve business operations and/or quality of life. Personal data can be mined alone or in conjunction with third party data to identify correlations amongst the data and associated users. Applications or services interact with such data and present to its users in a myriad of manners, for instance as notification so opportunities. [33]

Viewed this way, data protection and privacy have converged primarily as a legal framework to protect people's personal data are defined by the law and as rights. [34] This convergence also includes finding a balance between economic development, innovation and knowledge in the digital economy. Central to this argument is the ability as Graham Greenleaf once put it, the idea of 'knowledge engineering'. [31] While Greenleaf argued that knowledge engineering constitutes both formal domain knowledge and the experience of domain experts ('to somehow mine the jewels from expert professionals' heads'), have at various times been described as 'expert systems', 'knowledge-based systems' or just artificial intelligence ('AI'). [31] Here, human reasoning is what is being modelled, whether based on causal models, heuristics based on experience, or interpretation of formalisms (standards, statutes). These traditional notions of expertise require that such 'expert systems' can give explanations for the conclusions they reach [31] He goes onto say that, there are varieties of successful development of such systems, including those that assist in the completion of tax returns, or determine entitlement to welfare benefits, and 'intelligent agent' software which roam through tax, audit, and accountancy data files looking for exceptions. [31] For example, document assembly systems generating complex documents through interactions with

users are increasingly common, originally for use by lawyers but increasingly for lay use. In addition, online dispute resolution has numerous examples of systems successfully resolving very large numbers of disputes. Another major area of success has been 'predictive coding': using software to determine which documents should be disclosed in very large-scale litigation with more effectiveness than junior lawyers, and now with approval by United Kingdom ('UK') courts. In medicine there are remarkable successes claimed, such as the pharmacy robot known as Epocrates that has issued more than a million prescriptions without error and automated the interaction of different drugs. [31] Expanding on these point, one can conclude similar knowledge engineering can be undertaken through smart home devices. This is because they are indirectly to the systems highlighted by Greenleaf, and, the data they capture will be generally personal data via dataveillance, which can determine behaviour and store vast quantities of knowledge data on an individual at home and in the workplace.

Even though privacy and data protection is an evolving area of law and economic development, it has not matured as a measure of redressing economic and personal harm comparably to the protection of intellectual property, copyright, criminal procedure and international trade law. It is argued that data protection is largely a tool of privacy. [37] Data protection has also been characterized as a tool of 'privacy'. [36] In other words, data protection underpins privacy and constitutes the personal data used to identify a person. Identifying a person by their personal data was historically achieved through state records, such as, a passport or birth certificate. Data protection today is increasingly considered as the implementation of appropriate administrative, technical or physical measures that minimize the risk of or harm caused by unauthorized intentional or accidental disclosure. [37] It is shaped by the technological systems that collect, store and use data. Regulators also increasingly recognize that the technological use of personal data represents the greatest threat to individuals, accentuating their vulnerability and underscoring the need to protect their rights to privacy. [38]

3. Home Appliance[s]

AI can be found in many devices already in our homes that we call "smart" because they operate far more intelligent in technical way such as: smart phones, smart watches, robot vacuum cleaners and lawn mowers, self-driving cars, drones, etc. AI is very much used in robotics, technological industry, healthcare (in particular, medical diagnosing and surgery), transportation, military, video games, government and public administration, insurance, finance and economics, audit, advertising, art, amongst many others. In the notion of rules of robot, that can have similar behaviour with AI, Isaac Asimov set there of law of robotics in 1942. [35] But in the ethical area and specially in privacy perspective the AI or robot responsibility become fundamental question, is it possible to burden responsibility to the AI, the AI maker, or the person who controlled and own the data? By this proposition, the question of the data in home appliance also derived into the cross.

By the ICT phenomenon that moves very dynamic through various innovations, legal question needs to reconceptualize and because there is no unique definition. [40] Although, there is some of the similar principle to the definition of (IoT) that can be drawn as general concept of smart home appliance (special concept), namely: automatization, the connectedness of tools and the capability to communicate between one device and another. [41] The connectivity create a novel paradigm to understand the IoT, also lead some of central issue such as: higher degree of smartness, trust, privacy and security. [42] In the context of smart home appliance some of the type include: smart mattress, smart refrigerator, smart cooking pan, smart toothbrush, smart plate pot, wearable device for sports players, smart closet, internet-connected stuffed animal, smart jump rope, smart toilet. [43] Some of the old game on IT is cyber security to protect from the attacker. In smart home appliance, one of the largest smart home management system Chinese company in 2019 was reported over 2 billion data breach,[40] and the Orvibo customer is from around the world. The consequences of data breach in smart home appliance may not yet taken into account, but in the future, a class action lawsuit might be possible, depending on the jurisdiction. More problematic is the enforceability of these types of intrusions. The data breach will more often than not be compromised by a cyber security breach.

4. Discussion

There is not enough known about the security of smart home appliances. In other words, the thing that is not fully realized is that, smart home devices are collecting data, processing data (data aggregation), and sending user data to bring up a method based on the user's habits. Mustafa and Abidin argue that the pivot of security in IT (includes smart home appliance) is in the security system. [41] However, the habitual person to use smart home appliance is driven by pleasurable needs at home and forgot their intimate space has been watch by their smart devices. Technically, security system in smart home appliance must refer to the basis of the system itself. [42] There are several approaches on security models for smart home appliances, including physical networks, and application layers. [43] However, not all users (end users) have ability to understand the IT system thinking, and do their data protection for the. [44]

Data in the smart home appliance mostly held by the manufacture, by the concept of data and legal responsibility, the data controlled have legal responsibility to protect the data. This concept was referring to the property law concept. Another legal concept of responsibility in IT law is consumer protection. According to the United States Consumer Product Safety Commission 2017 there are at least four types of consumer protection related to electronic devices, namely: 1) loss of safety functions; 2) loss of connectivity; (3) data

integrity; and 4) wearable product hazards. [46] From the four safety provisions set by the CPSC, there is no security guarantee for data from consumer products used by the consumers themselves. In fact, the true function of the tool is to collect user data, and the data is stored in the device itself with a system model determined by the manufacturer. Additionally, Menachem Domb notes that contested area of these devices and their use, transfer and protection of personal data. Domb argues:

> Smart home and IoT will focus on data collection, basic processing, and transmission to the cloud for further processing. To cope with security challenges, cloud may be private for highly secured data and public for the rest. IoT, smart home and cloud computing are not just a merge of technologies. But rather, a balance between local and central computing along with optimization of resources consumption. A computing task can be either executed on the IoT and smart home devices or outsourced to the cloud. Where to compute depends on the overhead tradeoffs, data availability, data dependency, amount of data transportation, communications dependency and security considerations. On the one hand, the triple computing model involving the cloud, IoT and smart home, should minimize the entire system cost, usually with more focus on reducing resource consumptions at home. On the other hand, an IoT and smart home computing service model, should improve IoT users to fulfill their demand when using cloud applications and address complex problems arising from the new IoT, smart home and cloud service model. Some examples of healthcare services provided by cloud and IoT integration: properly managing information, sharing electronic healthcare records enable high- quality medical services, managing healthcare sensor data, makes mobile devices suited for health data delivery, security, privacy, and reliability, by enhancing medical data security and service availability and redundancy and assisted-living services in real-time, and cloud execution of multimedia-based health services. [45]

It is this health and medical data that has been defined by many national data laws as being the most important and sensitive personal information that can be disclosed. It could, when retrieved because of vulnerable networks be used by individuals and entities in an increasing contested world for evil and not good. This has been reinforced by Datta etal asserts that:

> the number and variety of internet-connected devices have grown enormously in the past few years, presenting new challenges to security and privacy. Network adversaries can use traffic rate metadata from consumer Internet of Things devices to infer sensitive user activities. Shaping traffic flows to fit distributions independent of user activities can protect privacy, thus this approach has seen little adoption due to required developer effort and overhead bandwidth. [46]

This in and of itself, highlights how there is technology available to, in part, provide for a high level of security of data and the privacy of that data. However, the technology poses challenges because of the extensive access to internet resources required to undertake such a complex operation. Moreover in reaffirming the above vulnerabilities and the flow of data through these devices, Krishnan and others make the point that:

> Smart Building system where wireless communication happens. RFID, Zigbee and Wi-Fi are the technologies used at these three places. Attacks such as Eavesdropping, Physical Attacks, Denial of Service, Spoofing, Replay Attack, Data Manipulation or Injection, MITM and Packet Rerouting are found to be the potential threats in the system. Data Stealing, tracking of the user based on the hacked data, loss of privacy, data modification, incorrect reports from the aggregator, system malfunctioning, rejecting the request of the legitimate user and many more are the effect of the attacks on the Smart Building system. [47]

Viewed this way, it demonstrates the real, formal and functional threat that data flows through these devices face. It further demonstrates how vulnerable data is when captures and used by devices that are located in countries with less secure internet functions. It confirms that data flows are vulnerable and this in turn will pose significant commercial challenges to entities entering the market. On the one side, they will be in a position where the use of data can be open for anyone to obtain, illegally. On the other side, it can restrict commercial activity because there will be fewer players in the market that do not have the resources or capacity to secure the data flows. In further reaffirming the above, more recent work undertaken in 2021 confirmed the continued vulnerability of data over these devices, through the Internet of Things. Azrour argues:

> Internet of Things (IoT) refers to a vast network that provides an interconnection between various objects and intelligent devices. The three important components of IoT are sensing, processing, and transmission of data. Nowadays, the new IoT technology is used in many different sectors, including the domestic, healthcare, telecommunications, environment, industry, construction, water management, and energy. IoT technology, involving the usage of embedded devices, differs from computers, laptops, and mobile devices. Due to exchanging personal data generated by sensors and the possibility of combining both real and virtual worlds, security is becoming crucial for IoT systems. Furthermore, IoT requires lightweight encryption techniques. [48]

Therefore, the vulnerabilities continue to exist unabated. Personal data plays a key role in data flows and the new digital economy. However, securing this data is going to be problematic, and consumers require confidence and certainty to ensure they participate in the new digital economy. The following tabulates the difference between end-users electronic systems such as social media or software with smart home appliance users. These devices in and of themselves will create a level of anti-competition in the economy. This will be achieved because there are, in our

view, a limited number of entities developing these products. Additionally, the Internet itself is controlled by very few organizations that could restrict or block new devices on the market, by simple making the systems incompatible.

Table 1. *Modern Smart Home Devices.*

Type of Device	Function	Connection	Personal Data
KITCHEN			
Coffee maker	Remote control to make a cup of coffee, maintain user's coffee schedule	Smartphone application Internet WIFI-cable	User preference, habits Email
Fridge	Do various function: ordering food online, browsing food recipes, monitor food available in the refrigerator via cell phone, write a shopping note, writing daily schedule, listen the song, watching TV, send a message, using the features of refrigerator to the voice assistant.	Smartphone application Internet WIFI-cable	User movement, habits, preference Social media, music application, user's voice
Dispenser application	Monitoring the needs of drinking water.	Smartphone application Internet WIFI-cable	User movement, habits Email, phone number, health history
PERSONAL CARE			
Tooth Brush	Cleaning teeth, gums, oral cavity and tongue, provide a report of oral health that can be shown to the dentist.	Smartphone Application Internet WIFI-cable	User movement, habits
Wardrobe	Manage clothes in the wardrobe, advice what will be worn today, and what clothes have been used the day before, provide information which cloth has the highest frequency and has not been used for long time	Smartphone Application Internet WIFI-cable	User movement, habits, preference Email, clothing data, calendar
ENTERTAIMENT			
Pillow	Stream music, audiobooks, podcasts, TV, and others using speaker connected to pillow, analyse user's sleep, sleep habits by giving user daily report.	Smartphone Application Internet WIFI-cable	User movement, habits, preference
TV	Connect to internet browser, assist user to manage their favourite program.	Internet WIFI-cable	User movement, habits, preference
CLEANING			
Mob	Mobbing the floor	Smartphone, GPS Internet WIFI-cable	User movement
Vacuum cleaner	Dust cleaning	Using detection camera Internet WIFI-cable	User movement
SECURITY			
Door lock system	Digital key, share digital keys, notification, monitor	Smartphone application, sensor Internet WIFI-cable	User movement, Habits IP Address, email, fingerprint (to open manually).
Garage door	Open the door/garage automatically, what time the is opened/closed, how long is the time the door will be closed after user leave, and send notification when someone force to open the door	Smartphone Sensor Internet WIFI-cable	User movement, Habits IP Address, email, fingerprint
OUTDOOR			
Gardening	Automatic watering, soil testing, detect the moisture on the ground	Internet WIFI-cable	User movement, habits preference Types of plants, sounds from users
OTHERS			
Vent	Adjust the temperature of rooms, including when the room will be used	Smartphone Application Internet WIFI-cable	User movement, habits preference
AC	Controlling AC	Smartphone Application Internet WIFI-cable	User movement
Baby monitor	Monitor baby activities: detect sleep, body temperature, sound, position, and breath of the baby and send the notification	Smartphone application, Microphone Internet WIFI-cable	User movement, habits preference

The authors in preparing the above table highlight where AI is beginning to find its way into the home, and collecting personal data unwittingly. While not conclusive, the snapshot in the aforementioned provides an early outline of where new technology is likely to head. Based on the above, the function of these technology while being perceived as another item in the home that, people have become familiar with, do not fully understand that once they are connected to the internet, people's data can be compromised with ease. More problematic is how AI in smart home appliances can be easily acquired and the user voluntarily can bring the devices to the intimate space within the home, to record and learn the family members habitual behaviour and actions.

Therefore, what has emerged is how computer programs that have been installed with AI capability, can describe a user's personal habits and behaviour accurately. AI only makes de-identification harder, in two ways. First, it facilitates the demand for more data, for example, from the sensors in cell phones, cars, and other devices. Second, it provides increasingly advanced computational capabilities to work with collected data. Facial features, gate, fingerprint, and other forms of biometric recognition technologies provide an apt example: they collect thousands of discrete, nearly meaningless data points and then combine them in a way to provide reliable identification of individuals. [50]

Moreover, as AI becomes increasingly mainstream, the

pros and cons of this technology is also being realized. In other words, and on the one hand, these technologies are starting to improve our lives in myriad ways, from simplifying our shopping to enhancing our healthcare experiences. Noteworthy too, McKinsey note that concerns raised are serious, and argue that:

> 'AI generates consumer benefits and business value, it is also giving rise to a host of unwanted, and sometimes serious, consequences. And while we're focusing on AI in this article, these knock-on effects (and the ways to prevent or mitigate them) apply equally to all advanced analytics. The most visible ones, which include privacy violations, discrimination, accidents, and manipulation of political systems, are more than enough to prompt caution. More concerning still are the consequences not yet known or experienced. Disastrous repercussions—including the loss of human life, if an AI medical algorithm goes wrong, or the compromise of national security, if an adversary feeds disinformation to a military AI system—are possible, and so are significant challenges for organizations, from reputational damage and revenue losses to regulatory backlash, criminal investigation, and diminished public trust.' [50]

This has been reinforced by technology industry sector itself. For instance, data security and privacy are the major key concerns that any AI and IoT enabled smart home should address as every connected device tends to leave the digital footprints of personal data that needs to be safe and secure. It is further highlighted that there is a need for proper integrations of AI and IoT technology. That is, and put another way, there is a need for proper integration of AI and IoT enables devices to not just perform more automatically with enhanced functionalities. For instance, the security cameras usually alert threats automatically, but with proper AI integration, they will proactively alert humans to take control of the situation when something goes wrong. A further concern is the interoperability of this technology. Centrally, interoperability is one key concern that needs to be addressed by any home automation tool. Smart home devices should be made interoperable and new use-cases like energy conservation, diagnostics of appliances, damage prevention during natural disasters, can be applied to the same smart devices.

A further concern, yet, at the same time a possible positive feature, is the integration of voice identification. For example, integration with voice controls will enable the user to save time, money and ease off certain tedious tasks. Even though some of the proposed AI systems will benefit customers in many ways, it will also extend to improve customer support. Thus, individuals or entities that, provide better and good customer service will always stay ahead of the race.

Moreover, there is a need to know and understand the interconnectedness between AI and data protection is paramount. Moreover, the need to couple AI and data protection with cyber security is just as paramount, to ensure there is a whole of legislative and technology approach. It will take a multi-layered approach to reconcile the challenges faced by AI, its technology to maintain a strong level of security and protect personal data. It will require regulators to be more adaptable than ever before, so as they can rapidly respond to change.

Thus, and on the backdrop of the above, technology over the internet knows no national boundaries. The challenges facing the protection of personal data by AI Smart Home products, requires an international response. These challenges are further compounded by the growth in economic activity of data flows – internationally. They will not be easily addressed in the short term, however, over the longer-term government's maybe be forced to develop and implement similar laws and strategies. Apart from identifying the sovereignty issues facing data protection and AI, this article has also highlighted that they are interconnected. More noteworthy, the interconnectedness of these devices extends to also cyber security, which must be also considered in any such response to AI and data protection.

5. Conclusion

Even though cyber security and AI are evolving at an alarming rate, they do, to varying levels are directly or indirectly connected to personal data. This is because personal data can be compromised and misused through a cyber security intrusion or breach, and some AI technology, is and will be capturing personal data. This paper has confirmed there will potentially be competition issues arising from these devices and their access to the Internet. It has also confirmed that even today, data flows remain highly vulnerable to security incursions. The developments in technology is not as advanced as one thinks, and these devices if not used properly will expose personal and commercial data. It is our view this interconnectedness will be further accentuated as different technologies such as AI continue to be developed that, enable even larger amounts of personal data to be collected and used.

Moreover, the Internet and its supporting technology, including AI will pose significant challenges to government and the broader community. [51] It challenges the very notion of the sovereign state and confers two distinct but related arguments: 1) intermediaries threaten state sovereignty; and 2) as a result of the world moving online, state power is in decline. [51] As large corporations are able to exploit arbitrage opportunities, they raise concerns about the "quasi-sovereign" power of intermediaries. [51] Unlike the development of technology through the industrial revolution, where largely governments had more time to react to change, the new Internet economy is moving so fast that governments and regulators cannot keep up. The ability for governments and regulators to meet the needs of the broader community and maintain elements of sovereignty over the Internet is diminishing.

However, with the fragmented approach to the development of technology, states are also in a position to exert their sovereign power outside the law. This not only

threatens the sovereignty of other states, but also large corporations. It enables other states to dictate, determine and shape the social and political discourse of citizens of other states. Furthermore, and because these large corporations have the flexibility and latitude that is not seen in other sectors or industries, it has been proven that they have unfretted power over customers.

Notwithstanding the above, one of the most pressing issues that is arising from the onset and use of AI technology is in the home and everyday life of individuals. Over the next decade the world is likely to see a significant shift in the devices used in the home, office and business. Smart Home appliances and devices (televisions, radios, IPhone, fridges, amongst others), along with personal robots and drones all constitute forms of AI. These are not only going to provide significant benefits to individuals, but there is a lack of understanding as to their security and how they capture personal data. Arguably more work needs to be undertaken to better understand the potential cybersecurity risks posed to individuals in the home or office from these devices.

More importantly, any study requires a comprehensive analysis of the extent to which behavioural data or put another way dataveillance exists within these forms of AI. The potential for vulnerable groups such as children, those with a disability and elderly to be captured by this technology is only beginning to be understood. Furthermore, capturing of this data will create an environment for potentially increased surveillance, understanding peoples' behaviour along with knowledge of person or persons and their daily interactional. The potential ramifications for bias and discrimination based on sex, ethnicity, religion, amongst others is enormous. Additionally, as AI evolves a more comprehensive study will be needed to better understand whether the developers of the technology have been successful in building adequate safeguards into the systems and platforms to protect personal data from illegal collection. Further work will also be required to confirm whether current trade-consumer practices law (in other countries this will be different) is adequate to regulate this at the point of sale of these devices.

It has been highlighted in this article how the definition of AI is far from agreed or settled at the national or even international level. While the article did not examine the international agreements or laws in regards as to whether, there has been some agreement or proposal put forward by states to clearly define what is and is not military AI. There are already calls for the legislation frameworks in relation to AI and data protection, and to a lesser extent to take into consideration the three areas as a collective. It has been demonstrated that to do so, governments and regulators have a significant challenge in the road ahead due to the need to balance innovation with the need to keep personal data secure and ensure its protection. The lack of any international framework only heightens this dilemma. Furthermore, there has been little discussion to the mainstream day to day appliances that will be adopted by individuals in the home that will be AI, they will be connected to the Internet and subject to security breaches, and collect, store and use personal data.

Finally, the protection on the privacy of personal data of users (end-users) on electronic devices have differences with user privacy protection of software. Getting the balance between data flows and the economic benefits it's provides will be complex and difficult to achieve. Regulators will need to provide a framework that facilitates trust, confidence and certainty. It will require opening up and enabling more competition. Centrally, the location of the most striking difference is the accountability of the user's personal data usage, which is caused by the mastery of the goods in the users (consumers). For software users, the responsibility lies in the organizer of the electronic system. This brings to the legal consequences that consumers of smart home appliance users are fully responsible for the goods and for data from their electronic devices. In some conditions, IoT on smart home appliances communicates with each other, which in fact is considered to be excluded from the manufacturer's control. Therefore, the protection of personal data on the smart home appliance requires reconceptualization, because the form is unique and different from the end-user of the software user.

References

[1] Graham Greenleaf, Global data privacy in a networked world, in Brown, I (ed) Research Handbook on Governance of the Internet Cheltenham: Edward Elgar, (2012). p 1.

[2] Roger Clarke, Graham Greenleaf, Dataveillance Regulation: A Research Framework, Journal of Law and information Science, 25, 1 (2018).

[3] Robert Walters, Marko Novak, Artificial Intelligence, Data Protection, Cyber Security and the Law, Springer (2021).

[4] Leon Trakman, Robert Walters, Cross Border Insolvency and Restructuring, Routledge, forthcoming.

[5] Mapping the challenges and opportunities of artificial intelligence for the conduct of diplomacy, Diplo Foundation Ministry of Foreign Affairs Finland, https://www.diplomacy.edu/AI-diplo-report

[6] Robert Walters, Matthew Coghlan, Data Protection and Artificial Intelligence Law: Europe Australia Singapore - An Actual or Perceived Dichotomy, American Journal of Science, Engineering and Technology 2019; 4 (4): 55-65. This paper does draw in elements of this earlier work by Walters and Coghlan.

[7] Phillip Jackson, Introduction To Artificial Intelligence 1, Dover Publ'n, Inc., 2d ed. (1974), 192-338.

[8] World Intellectual Property Organization Technology Trends, Artificial Intelligence, https://www.wipo.int/edocs/pubdocs/en/wipo_pub_1055.pdf

[9] Law library of Congress, Regulation of Artificial Intelligence in Selected Jurisdictions, January 2019, https://www.loc.gov/law/help/artificial-intelligence/regulation-artificial-intelligence.pdf

[10] Ibid, John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. 115-232, § 238, 132 Stat. 1658 (2018), https://www.congress.gov/115/bills/hr5515/BILLS-115hr5515enr.pdf.

[11] Ibid, FAA Reauthorization Act of 2018, Pub. L. 115-254, § 548, 132 Stat. 3186, https://www.congress.gov/115/bills/hr302/BILLS-115hr302enr.pdf.

[12] AI HLEG, A Definition of AI: Main Capabilities and Scientific Disciplines (2018), https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=56341

[13] Mihalis Kritikos, European Parliamentary Research Service Scientific Foresight Unit (STOA) PE 634.427 – March 2019, https://www.europarl.europa.eu/at-your-service/files/be-heard/religious-and-non-confessional-dialogue/events/en-20190319-artificial-intelligence-ante-portas.pdf

[14] Robert Walters, Marko Novak, Cyber Security, Artificial Intelligence, Data Protection, and the Law, Springer (2021).

[15] Samuel D. Warren and Louis D. Brandeis, The Right to Privacy, Harvard Law Review, IV (5), (1890), 195.

[16] Judith Jarvis Thomson, The Right to Privacy, Philosophy & Public Affairs, Vol. 4 No. 4 (1975), 295.

[17] Shoshana Zuboff, Big Other: Surveillance Capitalism and The Prospect of an Information Civilization, Journal of Information Technology (2015). Palgrave Macmillan. 76.

[18] In quotes: Lee Kuan Yew, 2015, https://www.bbc.com/news/world-asia-31582842

[19] European Convention for the Protection of Human Rights 1950 https://www.echr.coe.int/documents/convention_eng.pdf

[20] Warren and Brandeis, op.cit, p. 213.

[21] Robert C. Post. Three Concept of Privacy. The Georgetown Law Journal, Vol. 89, (2001), 2088.

[22] Jeffrey Rosen, The Unwanted Gaze: The Destruction of Privacy in America, 2000. Vintage Book. 7.

[23] Daniel J. Solove, A Taxonomy of Privacy, University Pennsylvania Law Review, (2006) 488.

[24] Daniel J Solove, Conceptualizing of Privacy, California Law Review, 90 (4), (2002), 1092.

[25] Jon L. Mills, The Lost Right. New York: Oxford University Press, (2008), 14.

[26] Graham Greenleaf, Global Data Privacy Laws 2019: 132 National Laws & Many Bills 157 Privacy Laws & Business International Report, (2019) 14-18.

[27] Alam, Mohammad Arif Ul; ROY, Nirmalya; MISRA, Archan; and TAYLOR, Joseph. CACE: Exploiting behavioral interactions for improved activity recognition in multi-inhabitant smart homes. (2016). 2016 IEEE 36th International Conference on Distributed Computing Systems (ICDCS): Nara, Japan, June 27-30: Proceedings. 539-548. Research Collection School of Information Systems.

[28] Muhammad Habibur Rehman, Chee Sun Liew, Teh Ying Wah, Junaid Shuja and Babak Daghighi, Mining Personal Data Using Smartphones and Wearable Devices: A Survey, Faculty of Computer Science and Information Technology, 2015-15, 4431-4440.

[29] United States Patent, No. 7, 930, 197, B2. https://patentimages.storage.googleapis.com/ee/8f/2c/0bd80a64ef6a52/US7930197.pdf

[30] Robert Walters, Leon Trakman, Bruno Zeller, (2019) Data Protection Law: A Comparative Analysis of Asia-Pacific and European Approaches, Springer.

[31] Graham Greenleaf, Thematic: Technology and the Professions, UNSW Law Journal Volume 40 (1) (2017), 310.

[32] De Hert p, Gutwirth S, (2006) Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power, in Claes E, Duff A, Gutwirth S, Privacy and the Criminal Law, Antwerp-Oxford, Intersentia, pp. 61-104, in Robert Walters, Leon Trakman, Bruno Zeller, (2019) Data Protection Law: A Comparative Analysis of Asia-Pacific and European Approaches, Springer.

[33] International Organisation for Standardisation/IEC 2382-1-1993 and its successors.

[34] Kokott J, Sobotta C, The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR, International Data Privacy Law, Oxford University Press, vol 3, Issue 4, (2013), 222–228, in Robert Walters, Leon Trakman, Bruno Zeller, (2019) Data Protection Law: A Comparative Analysis of Asia-Pacific and European Approaches, Springer.

[35] See: Isaac Asimov, I Robot, Round Around, Street & Smith Publication. (1942), 9.

[36] Momayya Madakam, R. Ramaswamy, Siddharth Tripathi, Internet of Things (IoT): A Literature Review, 2015. 165.

[37] See: Defra, Delivering the Benefits of Smart Appliances. London: Department for Environment, Food and Rural Affairs, (2017), 10.

[38] L. Atzori, et al., The Internet of Things: A Survey. Comput. Netw. doi: 10.1016/j.comnet.2010.05.010. (2010), 19.

[39] PWC. (2017) Smart Home, Seamless Life Unlocking a Culture of Convenience. Paris: Price Waterhouse Coopers France, 22, https://www.pwc.fr/fr/assets/files/pdf/2017/01/pwc-consumer-intelligence-series-iot-connected-home.pdf.

[40] RiskBased Security, (2019). Data Breach Quick View Report 2019, https://pages.riskbasedsecurity.com/hubfs/Reports/2019/Data%20Breach%20QuickView%20Report%202019%20Q3%20Trends.pdf.

[41] Mustafa A. Mustafa, Sara Cleemput, Abdelrahaman Aly, and Aysajan Abidin, Secure and Privacy-preserving Protocol for Smart Metering Operational Data Collection. IEEE Transactions on Smart Grid. (January 2018), p. 2.

[42] Benjamin Fabian, Tobias Feldhaus, Privacy-Preserving Data Infrastructure for Smart Home Appliances Based on the Octopus DHT. Computers In Industry, (2014), 3.

[43] Marlen Bissaliyev. IoT: Security and Privacy in Future Home appliances. International Journal of Applied Engineering Research, 12 (20), (2017), 10455.

[44] Jae-young, L. Analysis and Responsive Measure of Smart Home Security Threat in IoT. International journal of criminal study, 4 (1), (2019), 5.

[45] Menachem Domb, Smart Home Systems Based on Internet of Things, IoT and Smart Home Automation Intechopen, p 5-8, https://cdn.intechopen.com/pdfs/65877.pdf

[46] Datta T, Apthorpe N, Feamster N. Developer-friendly library for smart home IoT privacy-preserving traffic obfuscation, IoT S&P 18. In: Proceedings of the 2018 Workshop on IoT Security and Privacy. ACM; (2018) pp 43-48.

[47] Silpa Krishnan, Anjana M. S., Sethuraman N. Rao Security Considerations for IoT in Smart Buildings Amrita Center for Wireless Networks & Applications (AmritaWNA), 2017 IEEE International Conference on Computational Intelligence and Computing Research (2017), p 3.

[48] Mourade Azrour, Jamal Mabrouki, Azidine Guezzaz, Ambrina Kanwal, Internet of Things Security: Challenges and Key Issues, Security and Communications Networks, Volume 2021 |Article ID 5533843, https://doi.org/10.1155/2021/5533843, (2021), p 1.

[49] Benjamin Cheatham, Kia Javanmardian, Hamid Samandri, McKinsey, https://www.mckinsey.com/business-functions/quantumblack/our-insights/confronting-the-risks-of-artificial-intelligence

[50] Qualetics, How AI & IoT Are Driving Intelligence & Automation in Smart Homes, https://qualetics.com/how-ai-iot-is-driving-intelligence-automation-in-smart-homes/

[51] Remesh Tamachandran, How Artificial Intelligence Is Countering Data Protection Challenges Facing Organizations AI technology can help enterprises in endpoint security, data privacy and against phishing, malware and ransomware attacks. https://www.entrepreneur.com/article/343267.