Ensuring compliance of IoT devices with their Privacy Policy Agreement

1st Alanoud Subahi
School of Computer Science and Informatics
Cardiff University
Cardiff, United Kingdom
subahiat@cardiff.ac.uk

2nd George Theodorakopoulos
School of Computer Science and Informatics
Cardiff University
Cardiff, United Kingdom
Theodorakopoulos@cardiff.ac.uk

***Abstract*—In the past few years, Internet of Things (IoT) devices have emerged and spread everywhere. Many researchers have been motivated to study the security issues of IoT devices due to the sensitive information they carry about their owners. Privacy is not simply about encryption and access authorization, but also about what kind of information is transmitted, how it used and to whom it will be shared with. Thus, IoT manufacturers should be compelled to issue Privacy Policy Agreements for their respective devices as well as ensure that the actual behavior of the IoT device complies with the issued privacy policy. In this paper, we implement a test bed for ensuring compliance of Internet of Things data disclosure to the corresponding privacy policy. The fundamental approach used in the test bed is to capture the data traffic between the IoT device and the cloud, between the IoT device and its application on the smart-phone, and between the IoT application and the cloud and analyze those packets for various features. We test 11 IoT manufacturers and the results reveal that half of those IoT manufacturers do not have an adequate privacy policy specifically for their IoT devices. In addition, we prove that the action of two IoT devices does not comply with what they stated in their privacy policy agreement.**

***Index Terms*—IoT privacy policy; IoT policy; policy test bed; IoT privacy policy agreement; Compliance; GDPR**

I. Introduction

The Internet of Things (IoT) is a multi-domain (physical and digital) environment. It is made up of multiple services and devices, which are linked up and used to gather and exchange data. Objects are connected to the Internet, so that they can produce and share information. While there are numerous benefits to this, the issue of security continues to be a big challenge [1]. According to most analysts, the massive growth of IoT devices is inevitable in the future. It has so far been estimated by Gartner that 4.9 billion devices will be connected as of 2015 increasing to 25 billion by the year 2020. Cisco's IoT group forecasts that, by 2020, the number of connected devices will be more than 50 billion. IoT wearable devices are predicted to reach a total of 45.7 million by 2015 and 126.1 million units in 2019 according to IDC, which will result in a five-year compound annual growth rate of 45.1% [2], [3]. The diversity of IoT application domains is obvious, covering many aspects like smart cities, building and home automation, logistics and transportation, environmental monitoring to smart enterprise environments etc. and other smart wearable devices [4]. However, data security and privacy are the primary obstacles to the widespread application of the IoT applications. Certainly, the fear that sensitive information will be lost or exposed is one of the main reasons why so many people still avoid this kind of technology. Thus, it is fair to say that data security is a key factor in determining the efficiency and viability of the IoT [5]. Yet, the majority of IoT users do not understand what kind of information is being collected about them or their environment. In fact, a significant proportion of users are not fully aware that they are sharing information in the first place [6]. Privacy is not only about access authorization and encryption; rather, it also emphasizes on the type of transmitted information [7], and on how it will be used and shared by the legitimate recipient (e.g. IoT manufacturer). To tackle IoT privacy issues, governments along with industry stakeholders have established several regulations and policies to standardize and ensure IoT privacy such as the following: Before using an IoT-connected device, users must be fully informed in a Privacy Policy Agreement (PPA) of the ways in which their data will be used, and they must give their consent to these terms [8]. However, it is important for IoT manufacturers not only to have a sufficient PPA for their respective devices, but also to comply with what they state in their PPA.

To the best of our knowledge, most academic research focuses only on IoT attacks and violations. So, we are the first who highlight the importance of enforcing IoT manufacturers to issue a sufficient PPA as well as monitor the behavior of such IoT devices. Therefore, this study focuses on identifying to what extent those devices comply with their issued PPA. Our main contributions are the following:

1) We provide a theoretical overview of issues around IoT privacy and why there is an urgent need to update the IoT privacy law.
2) We focus on the language used within data privacy policies and, by merging and analyzing the existing privacy principles, we systematize them into 8 data privacy criteria. We argue that each IoT manufacturer should adhere to those criteria when they issue their privacy policy for their respective IoT device.
3) We design and implement a practical test bed for eval-

978-1-5386-7503-8/18/$31.00 ©2018 IEEE
DOI 10.1109/FiCloud.2018.00022

uating the level of compliance of the Internet of Things data disclosure with their privacy policy.

4) We use this test bed to evaluate the compliance of the actual behavior of 2 IoT devices with their PPA and with the 8 criteria, and present our conclusions which prove that the 2 IoT devices do not fully comply to what they state in their PPA.

The rest of the paper is organized as follows: In Section 2 we discuss the related work. We identify the terms of PPA and why it is important for IoT devices as well as we discusses some differences between website PPAs and IoT PPAs in section 3, while in section 4 we discuss our proposed model including the main 8 privacy criteria that should be applied to any IoT device; we apply those 8 criteria to 11 IoT devices; and we analyze the adherence of those IoT devices to the mentioned 8 criteria. Also, our test bed design and results is explained in detail in this section. The conclusion is presented in Section 5.

II. Related Work

Existing research has focused on analyzing IoT devices in terms of their security and privacy issues in order to discover any security vulnerabilities. The foremost intended contribution of this paper is to clarify and emphasize on the problem of IoT compliance with the device's privacy policy, which has not been in focus in the field of IoT devices. In this section, we examine the available IoT literature focusing on IoT security and privacy test bed as well as different attacks and vulnerabilities targeting various types of IoT devices related to user data disclosure. We see that the literature is limited to unauthorized access to personal data (e.g. anticipating the users behavioral pattern by sniffing wireless traffic exclusively), while no attention has been given to risks and vulnerabilities related to the type of personal information being collected from IoT devices, nor to the level of compliance to the corresponding privacy policy agreement.

A state-of-the-art test bed for wearable IoT devices was proposed by Siboni et al. [9]. Its main goal is to apply a set of security requirements against wearable IoT devices in order to test their security level. Also, it tests the behavior of these wearable IoT devices under several conditions, for example when different applications are running.

Wang et al. [10] present a contextual attack system called MoLe (Motion Leaks through Smart watch Sensors) using a smart watch device. They find that it is possible to recognize and identify the words typed with reasonable accuracy, thus violating user privacy.

Tekeoglu and Tosun [11] find security and privacy issues of the NetCam device, as it does not encrypt the images sent to the cloud. In addition, encrypted traffic can be decrypted with little effort.

In our study, we use the same Netcam device and we confirm the findings by Tekeoglu and Tosun. However, we use a different a test bed model, and our intention in collecting data traffic is to prove the level of compliance between what the NetCam sends and what is stated in their PPA.

A system called IoTScanner, which analyzes an IoT environment, has been proposed by Siby et al. [12]. This system can scan traffic in the Wi-Fi, Zigbee, and Bluetooth Low Energy frequencies. It also gives an overview of IoT devices that are currently active in a particular environment as well as the communication taking place between them. They find that it is possible to violate user privacy by classifying Wi-Fi enabled devices in an active environment based on the ratio analysis of sent-to-received traffic.

Torre et al. [13] discover a new kind of privacy risk related to personal data leakage when users share their data with third parties while using IoT applications. They define a number of algorithms in order to conduct inference attacks as well as offer strategies to avoid such attacks. An Adaptive Inference Discovery Service has been proposed by them which helps users configure their permissions to share personal data and to allow them to identify any risks related to this shared information. Notice that the proposed system works as an add-on to personal data managers PDMs as a recommended system.

Cyr et al. [14] applied a comprehensive security test on the Fitbit Flex fitness device which is a popular tracker device. They mainly examine the Bluetooth connection between the tracker device and its paired Android smartphone device, which includes the Fitbit application. They analyze the communication between the Fitbit application and its web service. Interestingly, they find that sensitive information such as the BLE credential is sent in plaintext from the Fitbit web server to the smartphone application. This means that any attacker could obtain this information with a Man-in-the-Middle-Aattack (MITM). Also, they point out that smartphones could eavesdrop on any close Fitbit devices and send their MAC addresses to the Fitbit server; notice that these security issues will allow anyone to track other Fitbit users.

III. Privacy Policy Agreement definition and its importance for IoT devices

According to the Internet Security Glossary [15], data privacy is described as "the right of an entity (normally a person), acting in its own behalf, to determine the degree to which it will interact with its environment, including the degree to which the entity is willing to share information about itself with others" [16]. The purpose of a privacy policy is to inform users about the type of information that will be captured, why it is being collected, and what will be done to prevent this process from becoming detrimental to the user. The problem is that many people still do not read privacy policies. Nowadays, most governments do treat data privacy as an essential human right [17]. It is now the norm for businesses to be obligated to state precisely why they want the information and what they plan to do with it [18]. However, existing privacy laws and regulations are not focused on IoT devices specifically. We argue that they are insufficient to capture important differences between general data protection scenarios and IoT-specific scenarios. In this study, we explain why it is important to have a separate PPA for IoT devices:

1) IoT devices are being manufactured for close, personal use. For example, a smart watch could be worn for most of the day, which would collect a huge amount of information about the personal habits and behavior of the wearer [9], [19]. Therefore, the user has the right to have a prior knowledge of what kind of sensitive information is being transmitted.
2) The financial value of IoT users' data is connected to the ability of this data to help manufacturers sell more products (e.g by knowing the user behavior, or the user preferences). It could be argued that IoT manufacturers have a vested interest in collecting user data without informing users about it [9]. In this scenario, to prevent IoT manufacturer from using user's data for their interest, they should issue a sufficient PPA and comply with it.

Therefore, consumers need to be made aware in advance that their information is not completely secure and private. They should also know that outside entities may be able to eavesdrop on their information. This prior knowledge is typically encoded in a PPA, and it covers the whole data lifecycle, from the exact point in time when data packets are captured by the IoT device's sensors until the phase where raw data is effectively deleted, specifically for sensitive data gathering devices [6]. According to the EU Commission report on the IoT [20], privacy and security continue to be the biggest challenge for IoT research that contains privacy-preserving technology for heterogeneous device sets. The Federal Trade Commission (FTC) [21] agrees with this statement. The head of the FTC, Edith Ramirez, mentioned that "The only way for the Internet of Things to reach its full potential for innovation is with the trust of American Consumers. We believe that by adopting the best practices we have laid out, businesses will be better able to provide consumers the protections they want and allow the benefits of the Internet of things to be fully realized."

A study by the Information Commissioner's Office (ICO) [18] reveals that six in ten IoT devices do not come with sufficiently comprehensive privacy agreements. These agreements fail to fully explain why and how personal data is utilized by IoT devices. The study reveals that 59% of IoT device Privacy policies did not clearly explain to the users how their information was going to be collected, used and disclosed, while 68% failed to adequately specify how they stor the information. In addition, a high percentage (72%) of IoT devices did not mention how users could edit their information (delete, update), and finally only 38% adequately explain how users could contact the manufacturer if they have any privacy concerns.

A. Difference between website privacy policy and IoT privacy policy

There are some important differences between IoT privacy policies and traditional privacy policies for websites. IoT privacy has changed the concept of previous website privacy policy content due to the sensitivity of personal data transferred from IoT device to the cloud/server and vice versa. On one hand, the data captured by a wearable device, for instance, which reveals the pattern of the users' life, is transferred from the device to the cloud or server. This information is much more sensitive than what happens when information is collected and transferred while a user is browsing, searching, or even emailing through websites. On the other hand, IoT devices create the data while they are actively connected to the internet. With wearable tech and other IoT devices for example, it is not always necessary to manually connect to the web, so there is the potential for data capture and transfer at times when the user is not aware. Thus, manufacturers need to be thinking about these issues when designing and implementing privacy policy agreements for their IoT devices.

IV. Proposed model

A. Eight criteria for IoT Privacy Policy

This section aims to outline eight key criteria which all IoT privacy agreements should meet. Our goal is to determine the following:

1) How many IoT manufacturers have a PPA that is appropriate for their IoT products?
2) To what extent do these IoT manufacturers adhere to the eight criteria outlined in this section?
3) Which criteria are most and least likely to be sufficiently met?

To achieve these objectives, we conduct two separate studies. The first one is an analysis of 11 IoT manufacturers, with the aim of finding out if these companies offer appropriate PPA for their devices. Another aim is to investigate whether the IoT manufacturers provide sufficient information in their PPA, such as what kind of personal data they collect from their IoT device, whether they interact with a third party or not, etc. The 11 IoT manufacturers that we analyze are the following:

1- LIFX	2- AWAIR (Bitfinder)
3- Google Home	4- Tp-link
5- Samsung smart home	6- Belkin
7- Nest Labs	8- Hive
9- Toymail	10- Philips Lighting
11- Honeywell	

The second study focuses on establishing eight criteria that should be implemented by each IoT manufacturer. To create these key criteria, we first conduct research on the responsibilities of modern manufacturers, then we propose the main eight privacy policy criteria for any IoT device in the form of the following obligations of IoT manufacturers:

1) Explain what kind of personal and non-personal information the manufacturer will collect from their IoT device and explain why they need it.
2) Clearly specify to IoT users what specific information will be provided by IoT users themselves, once they create their IoT account.

3) Explain to IoT users what information will be collected from them automatically when they perform specific action with their IoT devices and why the manufacturer needs to collect that information.
4) Explain to IoT users how their information will be used and treated by the IoT manufacturer.
5) The rights of IoT users to control (edit, delete) their data saved in IoT cloud/servers.
6) Clearly specify to IoT users how long they will store their personally identifiable information (PII) on the IoT manufacturer's cloud server.
7) Clearly ask for the IoT user's consent in order to collect/share extra information and explain the reason for this request.
8) Clearly inform the IoT users of the geographical location of the IoT servers where the manufacturer keeps/stores the IoT user's data.

It is important to highlight that these criteria have been supported by the ICO report [18] based on the following considerations:

1) The standards set in place by the General Data Protection Regulation (GDPR) clearly state that any personal data should be processed in highly secured environment and guarantee total privacy of personal data, for instance protecting any type of unauthorized access by using standard security methods. The GDPR has set the criteria for manufacturers on what data needs to be collected about the users through a table created by them. Categories of personal data represent one such information. This point covers criteria number 1,2, and 3.
2) The GDPR underlines the importance of telling users how their data is being used. This point covers criterion number 4.
3) The GDPR is critical on the fact that users have the right to remove their personal data at any time with no restrictions as be totally forgotten. This point covers criterion number 5.
4) The GDPR states that users have the right to know the period of keeping their personal data under the manufacturer's possession. In addition, they have the right to withdraw their consent at any time. This point covers criterion number 6,7.
5) Special restrictions have been imposed by the GDPR on the transfer of personal data outside the European Union, to third countries, or to any international organizations without prior user knowledge and approval, to ensure that the level of individual protection is not undermined.This point covers criterion number 8.

B. Analyze the level of compliance of the 11 IoT manufacturer to the 8 criteria

After our analysis of the PPAs of 11 IoT manufacturers as mentioned earlier, we manually apply the eight key criteria to each IoT manufacturer. Then, we identify the respective levels of adherence of each manufacturer as well as identify which criteria are most likely to be sufficiently met according to this analysis. Tables 1a and 1b illustrate each individual company's compliance (11 IoT manufacturers) to the mentioned 8 requirements. We establish the level of compliance by studying the privacy policy agreement for each IoT manufacturer.

As we can see from Tables 1a and 1b, the most likely criteria to be fulfilled are criteria no 1,2,4 and no 5 with (82%), in other words, 9 out of 11 IoT companies comply to these four criteria, while 8 out of 11 IoT companies comply to only criterion no.3 (73%), followed by criterion 7 which achieved compliance by 7 out of 11 IoT companies (64%). Furthermore, only 6 of the IoT companies comply to criterion no.6 (55%). Finally, there is one criterion which are poorly explained or consistently overlooked, criterion no 8, this criterion achieved compliance by only 4 IoT companies (36%). Figure 1 demonstrates a comparison of levels of compliance to the 8 IoT privacy criteria among the 11 IoT manufacturers. Firstly, the graph shows that only one of the eleven IoT companies (Awair) comply to all eight privacy policy criteria. While four out of eleven companies (88%) comply to seven criteria. Secondly, 63% which represent three out of eleven IoT companies comply only to five criteria, whereas just two IoT companies comply to half of the criteria. Finally, it should be noted that the lowest level of compliance is for one IoT company(LIFX) which comply to only 2 criteria.

Based on our results, we could argue that the 11 IoT companies did not achieve full compliance to the 8 criteria. However, it is crucial for any IoT company to comply to the list of criteria because it could be considered as a definitive breakdown of the things that IoT manufacturers or vendors must tell users both before and after they activate their IoT devices. In addition, according to Edith Ramirez statement [21] , by adhering to this criteria IoT manufacturers will gain transparency, honesty and trustworthy relationship between them and their IoT users/consumers which will have a great impact on the IoT companies' profits

C. IoT Test Bed Architecture

The purpose of this section is to determine to what extent IoT manufacturers are adhering to their own PPA presented in their website. To do this, we need to find out precisely what kind of information is being captured, how it is being used, and whether these processes are sufficiently detailed in the IoT PPA. This involves 'sniffing' the traffic moving between the device and the cloud to see what data is being transferred. Figure 2 illustrates that, in this context, traffic is transmitted (and therefore needs to be monitored) among three points: IoT device, IoT application on a smart phone, and the manufacturer's cloud infrastructure. For this part of the study, we used a basic, low cost wireless IP camera from Belkin called NetCam and a Tp-Link HS110 Wi-Fi Smart Plug. Kali Linux laptop was configured for use as a Wi-Fi hot spot [22] to connect the IoT devices and the Android smart phone to the Internet through Kali Linux.

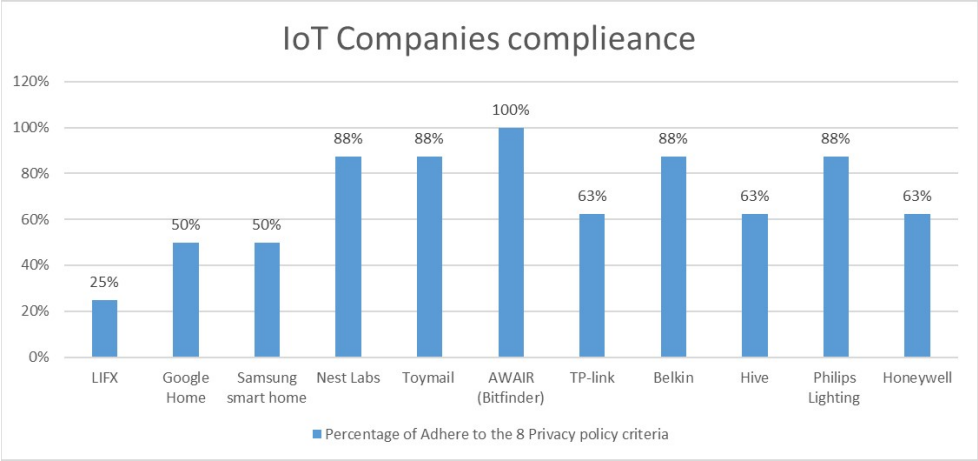

Fig. 1: How many of the 8 privacy criteria does each IoT manufacturer adhere to

IoT company & Privacy policy main criteria	LIFX	Google Home	Samsung smart home	Nest Labs	Toymail
Criteria no.1	X	X	✓	✓	✓
Criteria no.2	✓	✓	✓	✓	✓
Criteria no.3	X	X	✓	✓	✓
Criteria no.4	X	X	✓	✓	✓
Criteria no.5	X	✓	X	✓	✓
Criteria no.6	X	✓	X	X	✓
Criteria no.7	✓	✓	X	✓	X
Criteria no.8	X	X	X	✓	✓

(a) apply the 8 criteria to the first 5 IoT manufacturers

IOT company & Privacy policy main criteria	AWAIR	TP-link	Belkin	Hive	Philips Lighting	Honeywell	The percentage of devices that comply with to each criterion
Criteria no.1	✓	✓	✓	✓	✓	✓	82%
Criteria no.2	✓	✓	✓	X	✓	X	82%
Criteria no.3	✓	✓	✓	✓	✓	X	73%
Criteria no.4	✓	✓	✓	✓	✓	✓	82%
Criteria no.5	✓	✓	✓	✓	✓	✓	82%
Criteria no.6	✓	X	✓	✓	✓	X	55%
Criteria no.7	✓	X	✓	X	✓	✓	64%
Criteria no.8	✓	X	X	X	X	✓	36%

(b) apply the 8 criteria to the last 6 IoT manufacturers

TABLE I: The level of compliance between 11 IoT manufacturers against 8 criteria.

D. IoT compliance experiments

1) Belkin NetCam: **A. Packet analysis using Wireshark:** Using the IoT architecture illustrated in Figure 2, we managed to sniff the data packets moving between the NetCam and its cloud named Seedonk , as well as between the NetCam app and the mentioned cloud. By using wireshark to monitor the traffics, we observed SSL/TLS traffic as well as an un-encrypted traffic. It was clear from wireshark that video files aren't transferred using encrypted methods. After the TCP handshake, a packet is delivered from the camera to the cloud and significant amounts of data can be inferred from this packet such as the user name of the device owner, the MAC address of the IP camera, and the local IP address.

B. Mobile app analysis using Burp suite tool: We use burp suite tool to intercept the SSL/TLS encrypted traffic between the NetCam app and the Seedonk cloud using man in the middle (MITM) attack. We set up burp suite by following [23]. By accessing the burp suite interface, the SSL/TLS traffics were displayed in plain text form. It's worth to say that we could not uncover any user credentials via the NetCam application. Consequently, We attempted to do so in another way. We navigated to the NetCam website (https://NetCam.Belkin.com) from the smart phone. So, we did manage to break the SSL/TLS connection between the smart phone web browser and between the NetCam web servers, via use of the burp suite tool ans uncover the credentials in plain text form.

C. Belkin NetCam Compliance to its PPA:

- As regards information which complies with the NetCam

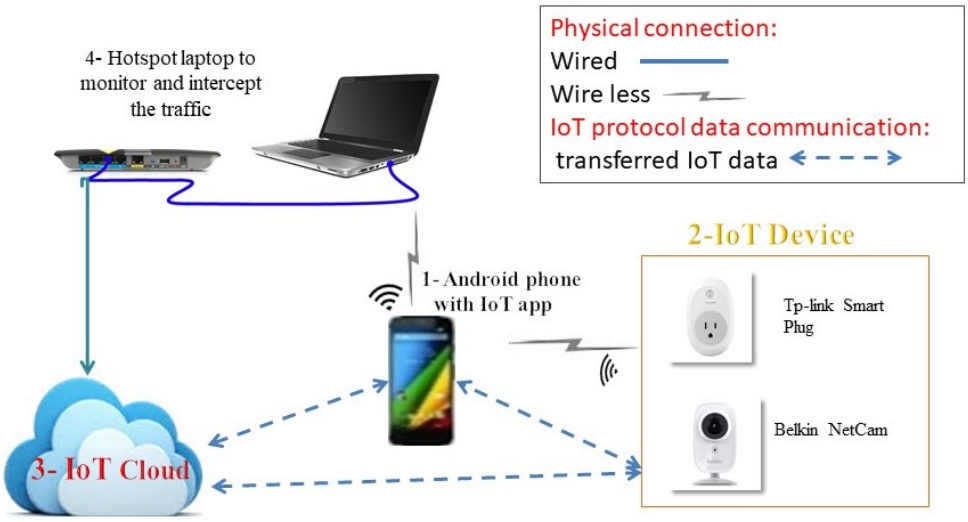

Fig. 2: IoT Architecture

PPA:

1) Netcam application does not transmit information about the exact location of the device. In this case, we did not give consent for this data to be captured. This demonstrates a high level of compliance, because the privacy agreement states that no such information can be collected without permission from the user.
2) NetCam appears to transmit only data which has been expressly permitted and described in the agreement. This includes technical information about the NetCam device (model, version, H.W, S.W, firmware, etc.) and utility settings (resolution, status, size, mode, notifications, etc.)
3) We could not capture any information related to the smart phone such as (O.S, H.W, manufacturer, model number, etc.). This demonstrates a high level of compliance, because the privacy agreement states that no such information can be collected

- As regards information which does not comply with the NetCam PPA:

1) We discover that the Belkin NetCam uses encryption technology to protect PII data as it moves between the application to the cloud (and vice versa). While this encryption is a good way to ensure that personal data is secure, there is no proper mention of this in their PPA. Therefore, the manufacturer needs to think about providing more details about its encryption process. If it does not, customers might feel deceived, and it could reflect badly on the IoT manufacturer and even damage its sales. On the other hand, most users are aware of the importance of employing data encryption methods.
2) Even though the NetCam PPA does not include the name of the cloud server used by them, we are able to discover this information. Also, attempting to uncover the geographical location of the cloud server we find two locations, one server located in Ireland/Dublin and the other located in United States/ Virginia, this finding violates criterion number 8. According to GDPR the user has the right to know the geographical area containing the servers/clouds where their personal data is kept.
3) We found that, although NetCam collects user's images and videos and sent them to the cloud server, there is no clear mention of this process in the NetCam PPA. This critical finding violates two main criteria which are number 1 and number 3. According to FTC [21] and ICO [18] it is highly important to inform the users of what kind of information is being collected about them.

2) Tp-link Smart Plug: **A. Packet analysis using Wireshark:** We attempt to sniff the traffic moving between the Smart Plug and the android application named kasa which controls the Smart Plug and between kasa application and the cloud (refer to Figure 2). After observing the wireshark network traffic, we detect encrypted traffic during the interaction between kasa application and the smart plug. Next, we successfully decompile (reverse engineer) kasa application and find the encryption function that is used to encrypt the traffic between kasa application and the Smart Plug server. We use this encryption file to apply wireshark dissector in LUA code. By plugging in the new LUA file, the traffic will automatically decrypt [24]. As a result, we are able to monitor the communications between kasa application and the Smart Plug on their local WiFi in a plain text

B. Mobile app analysis using Burp suite tool: In order to intercept the SSL/TLS traffic between kasa application and

the cloud via the burp suite tool, we follow the same steps described in Section 5.4.1(B). We find that when we launched kasa application at first time a log-in method is triggered and therefore sends user's credentials to the cloud. However, every time we open the application to perform any action (switch Plug on/off, schedule an event, etc), the helloIoTCloud method triggers and again sends user's credentials to the cloud. Lastly, we uncover eight main methods of requesting/sending personal data to/from the TP-Link cloud which are: login method, helloIoTCloud method, list scenes method, isLinked method, retrieve location method, list Rules method, pass through method, and get device list method. The following types of information are transferred using these methods:

1) Application such as: appName, appType, appVersion
2) Client such as: clientId, geolocation, locale timezoneId, mobileType, userDevice manufacturer, userDevice model, device osVersion, ownerEmail
3) Smart Plug information such as: sw_ver, hw_ver, type, model, mac address, hwId, dev_name, alias, location, fwVer, deviceName, status, deviceType, appServerUrl, deviceModel, deviceMac, isSameRegion

C. Smart Plug Compliance to its PPA:

- As regards information which comply with the Smart Plug PPA:
  The information collected from the Smart Plug and the Kasa application mentioned earlier appears to be in full compliance with the PPA as they mentioned in detail what type of information the smart plug will collect.
- As regards information which does not comply with the Smart Plug PPA.
  1) As with the NetCam, it was discovered that the Smart Plug does utilize encryption technologies, even though there is no mention of this in the PPA.
  2) There was no information provided about the name of their cloud server, but we could find out that the manufacturer uses a TPLinkra cloud server. In addition, we could determine the geographical location of the cloud servers which was located at United States/Virginia, this finding violates criterion number 8. According to GDPR the user has the right to know the geographical area containing the servers/clouds where their personal data is kept.

To conclude this section, our findings prove that there is critical violation in terms of the IoT companies' levels of compliance with their privacy policy agreement. We find that the actual data we obtained from capturing Belkin NetCam and Tp-link smart plug traffic did not comply with what they stated in their PPA. Interestingly, we conclude that Belkin NetCam shows a quite high level of compliance with our 8 criteria (88%) see figure 1 whereas from our experiment we prove that the level of compliance of Belkin NetCam with what they stated in their privacy policy is low as they violate 3 statements with in their PPA which are similar to criteria (no.1, no.3, and no.8). In contrast, we find that the Tp-link smart plug shows a quite high level of compliance to what they stated in their privacy policy as they only did not comply to one statement which is similar to criterion no. 8 whereas it shows only 63% of compliance to the 8 criteria see figure 1.

Unless IoT companies issue an appropriate PPA that comply to the 8 privacy policy criteria and, more importantly, comply to what they state in their own PPA, user's privacy issues will always be compromised.

V. Conclusions

In this paper, we discuss the importance of having a separate PPA for IoT devices as it differ from website PPA and we implement IoT privacy compliance test bed. The main objective is to determine the level of compliance of IoT manufacturers with their respective PPA. We posit eight key criteria and compare them with the actual PPA carried out by each IoT device.

First, we investigate the PPAs of 11 IoT devices. Then we manually compare their respective PPA with the 8 privacy criteria. The results show that only one criterion out of the eight criteria have been fulfilled by eleven IoT manufacturers, while only four out of eleven IoT manufacturers only comply with 88% of the eight criteria. The next step is to construct and execute a test-bed procedure for two selected IoT devices; the Belkin NetCam and the Tp-Link Smart Plug.

We sniff the data packets being moved between the IoT device and the cloud, between the IoT device and the smart phone, and between the smart phone and the cloud. Surprisingly, we find that the Smart Plug adheres to 63% of the established 8 criteria, but as for the terms of their PPA, they show a high level of compliance because they only did not comply to one statement which is similar to criterion (no.8) of the promises contained in its own PPA. Similarly, although we find that the NetCam show a quit high level of adheres to 88% of the established 8 criteria, they failed to adhere to their own PPA because they violate 3 statements which are similar to criteria(no.1,no.3 and no.8).

Yet, it could still be argued that the percentages of the adherence to the 8 criteria are not high enough, particularly in the case of adherence to key data privacy targets. There is a clear need for manufacturers to continue evolving and developing their PPA by either changing the behavior of the device to comply with their PPA, or by modifying the PPA to reflect the actual behavior of the IoT device.

Acknowledgments

The first author's work is sponsored by King Abdul Aziz University in Saudi Arabia.

References

[1] R. Roman, P. Najera, and J. Lopez, Securing the Internet of Things, Computer, vol. 44, no. 9, pp. 5158, Sep. 2011.
[2] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, Internet of Things (IoT): A vision, architectural elements, and future directions, Future Gener. Comput. Syst., vol. 29, no. 7, pp. 16451660, 2013.
[3] C. Perera, C. H. Liu, and S. Jayawardena, The Emerging Internet of Things Marketplace From an Industrial Perspective: A Survey, IEEE Trans. Emerg. Top. Comput., vol. 3, no. 4, pp. 585598, Dec. 2015.

[4] A. Tekeoglu and A. . Tosun, A Testbed for Security and Privacy Analysis of IoT Devices, in 2016 IEEE 13th International Conference on Mobile Ad Hoc and Sensor Systems (MASS), 2016, pp. 343348.
[5] M. Abomhara and G. M. Kien, Security and privacy in the Internet of Things: Current status and open issues, in 2014 International Conference on Privacy and Security in Mobile Systems (PRISMS), 2014, pp. 18.
[6] C. Perera, R. Ranjan, L. Wang, S. U. Khan, and A. Y. Zomaya, Big Data Privacy in the Internet of Things Era, IT Prof., vol. 17, no. 3, pp. 3239, May 2015.
[7] A. Crabtree, Enabling the New Economic Actor: Personal Data Regulation and the Digital Economy, in 2016 IEEE International Conference on Cloud Engineering Workshop (IC2EW), 2016, pp. 124129.
[8] M. Elkhodr, S. Shahrestani, and H. Cheung, The Internet of Things: New Interoperability, Management and Security Challenges, Int. J. Netw. Secur. Its Appl., vol. 8, no. 2, pp. 85102, Mar. 2016.
[9] S. Siboni, A. Shabtai, N. O. Tippenhauer, J. Lee, and Y. Elovici, Advanced Security Testbed Framework for Wearable IoT Devices, ACM Trans. Internet Technol., vol. 16, no. 4, pp. 125, Dec. 2016.
[10] H. Wang, T. T.-T. Lai, and R. Roy Choudhury, "MoLe: Motion Leaks through Smartwatch Sensors," 2015, pp. 155166.
[11] A. Tekeoglu and A. S. Tosun, "Investigating Security and Privacy of a Cloud-Based Wireless IP Camera: NetCam,— in 2015 24th International Conference on Computer Communication and Networks (ICCCN), 2015, pp. 16.
[12]] S. Siby, R. R. Maiti, and N. Tippenhauer, "IoTScanner: Detecting and Classifying Privacy Threats in IoT Neighborhoods," ArXiv170105007 Cs, Jan. 2017.
[13] I. Torre, G. Adorni, F. Koceva, and O. Sanchez, Preventing Disclosure of Personal Data in IoT Networks, in 2016 12th International Conference on Signal-Image Technology Internet-Based Systems (SITIS), 2016, pp. 389396.
[14] B. Cyr, W. Horn, D. Miao, and M. Specter, "Security analysis of wearable fitness devices (fitbit)," Massachusets Inst. Technol., p. 1, 2014.
[15] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges," Ad Hoc Netw., vol. 10, no. 7, pp. 14971516, Sep. 2012.
[16] Internet security glossary. https://www.ietf.org/rfc/rfc2828.txt, 2017.
[17] You need a privacy policy. heres why. https://www.webhostingsecretrevealed.net/blog/blogging-tips/have-a-website-you-need-a-privacy-policy-heres-why/, 2016.
[18] Information commissioner ofce. https://ico.org.uk/, 2017.
[19] Y. Cheng, M. Naslund, G. Selander, and E. Fogelstrom, "Privacy in machine-to-machine communications A state-of-the-art survey," in 2012 IEEE International Conference on Communication Systems (ICCS), 2012, pp. 7579.
[20] H. Sundmaeker, P. Guillemin, P. Friess, and S. Woelf "e. Vision and challenges for realising the internet of things". Cluster of European Research Projects on the Internet of Things, European Commision,3(3):3436, 2010.
[21] Federal Trade Commission. https://www.ftc.gov/, 2017.
[22] How to create WI FI Hotspot in Linux (kali Linux) - Tech Sarjan. http://techsarjan.com/2014/10/how-to-create-wi-fi-hotspot-in-linux.html.
[23] Configuring an Android Device to Work with burp PortSwigger Web Security. https://support.portswigger.net/customer/portal/articles/1841101-configuring-an-android-device-to-work-with-burp.
[24] softScheck. https://www.softscheck.com/en/reverse-engineering-tp-link-hs110/, 2017