You Know Too Much: Investigating Users' Perceptions and Privacy Concerns Towards Thermal Imaging

Lipsarani Sahoo[1][0000−0001−8660−8516], Nazmus Sakib Miazi[2], Mohamed Shehab[1][0000−0002−4189−9118], Florian Alt[3][0000−0001−8354−2195]
Yomna Abdelrahman[3][0000−0002−2859−7297]

[1] University of North Carolina at Charlotte, USA
{lsahoo1,mshehab}@uncc.edu
[2] Northeastern university, USA
m.miazi@northeastern.edu
[3] Bundeswehr University Munich, Munich, Germany
{firstname.lastname}@unibw.de

Abstract. Thermal cameras are becoming a widely available consumer technology. Several smartphones are already equipped with thermal cameras, and integration with personal devices is expected. This will enable compelling application areas for consumers, such as in-home security, energy-saving, non-invasive ways of child care, and home maintenance. However, the privacy implications of this technology remain largely unexplored. We close this gap with an interview study (N=70). Specifically, we assess users' perceptions with and without prior understanding of thermal imaging. We showed one group of the interviewees informative videos, pointing out opportunities and potential threats. Results show that users are most concerned about their privacy in cases where thermal cameras reveal information on their physiological state or invade their private space. Our findings are valuable for researchers, practitioners, and policymakers concerned with thermal cameras, as this technology continues to become widely used.

Keywords: Security · Thermal Imaging · Privacy · Offensive Technology

1 Introduction

Thermal cameras have evolved from specialized and expensive hardware to small, affordable consumer devices. Hence, they have the potential to become a technology to which users have access in their daily life as they are being integrated with personal devices, such as smartphones or wearables (e.g., glasses). This assumption is backed by an analysis from *Global Market Insight*, reporting that the market size of thermal imaging crossed USD 5.5 billion in 2017 and is forecasted to grow yearly by 8% between 2018 and 2024 [42]. The global number of shipped units is predicted to reach 4 million by 2024. FLIR[4], the world's largest thermal imaging device maker, is selling thermal camera add-ons for smartphones for less than $300. Furthermore, smartphones like the Caterpillar Cat S61[5] already integrate thermal cameras.

[4] https://www.flir.com/flir-one/
[5] https://www.catphones.com/en-us/cat-s61-smartphone/

Beyond specific, professional use cases, such as at airports detecting passengers with fever or higher degree of temperature (cf. the COVID-19 outbreak) or firefighters identifying dangerous areas, an increasing number of use cases in the consumer area emerge. These include, but are not limited to, in-home security, personal safety, energy efficiency, child and pet care, pest control, home maintenance, automotive care, and leisure. Abdelrahman et al. investigate domestic use cases [11].

At the same time, thermal imaging does not come without privacy and security implications. For instance, in 2001, the US Supreme Court decided that the use of sensors by the police to detect marijuana plants growing inside a home violated civil liberty, where the thermal cameras could reveal things beyond what a person standing outside a home would not be able to see. For example, whether "the lady of the house might be taking her daily sauna and bath" [2]. Similarly, during the winter in 2011, the city officials in Boston, Massachusetts, used aerial and street thermal cameras to detect heat loss in houses, analyzing 20,000 thermal images per day. There it helped optimize energy usage in the city. However, plans to involve residents to increase energy efficiency led to strong resistance against the proposal, as the approach could potentially reveal residents' movements and behavior inside their houses. The program was put on hold until the administration developed a privacy protection policy for homeowners [3]. Researchers started investigating the implications of thermal imaging on privacy and security. For example, it was shown that thermal imaging could be used to extract PINs from the heat trace [6], to identify people from the hand veins, and to reveal mental states and behavior [20]. Yet, it remains largely unexplored how users perceive this technology and which privacy concerns they might have. Closing this gap is the focus of our work. To this end, we conducted an in-person semi-structured interview study with a total of 70 participants. To obtain a holistic view, we interviewed both people without in-depth understanding and people we demonstrated opportunities and potential privacy threats before the interviews through video showcases. Our analysis shows that participants from all groups are concerned about privacy in general, most notably about the disruption of their private space, physical privacy, the privacy of their cognitive state, and physiological privacy. Our investigation is complemented by discussing the implications of our findings and identifying directions for future research.

Contribution Statement. Our contribution is twofold: First, we investigate users' perception and privacy concerns towards thermal imaging while considering how understanding and priming influence their perception. To this end, we conducted and analyzed 70 interviews, splitting participants into two groups (primed and unprimed). Second, we provide an in-depth discussion of the implications of our findings. We found that users are most concerned about the thermal camera capability of peeking into a person's physiological state and could potentially invade private space.

2 Background & Related Work

Our work builds on three strands of prior work: (1) thermal imaging, (2) users' perceptions of sensing devices, and (3) privacy perceptions across different user groups.

2.1 Thermal Imaging

Thermal imaging operates in the infrared range of the electromagnetic spectrum (0.7 to 30 μm), i.e., it senses wavelength beyond the ones visible to the human eye. Thermal

cameras render thermal energy (heat) into false-color images to extract images that can be seen by human eyes. The images, called 'thermogram,' are analyzed through 'thermography' tools. The first thermal camera was developed for military use. Later, thermal cameras got adopted to many other use cases, for example, detecting icebergs, automated machinery monitoring, analyzing structural integrity, firefighting, surveillance, and managing power line safety. Thermal cameras are also used in the health sector, for example, as a physiological monitoring tool to detect fever in humans and other warm-blooded animals [4]. In the context of the recent COVID-19 outbreak, an extensive use of thermal imaging could be observed at airports and train stations, to identify infected people [5]. Until recently, thermal cameras were considered a relatively expensive technology, with cameras' prices reaching thousands of dollars. Hence, prior applications were often limited to specific domains such as medical, military, and industrial settings. However, with technology advances, affordable thermal cameras operating in the FIR spectrum are becoming available, with costs being around a few hundred dollars. This enabled a wide range of new applications and sparked much interest in the research community. These include in-home security, personal safety, energy saving, pest control, home maintenance, automotive care, and leisure.

Gade and Moeslund reviewed the use of thermal imaging, highlighting the potential of using thermal imaging in different domains [26]. Abdelrahman et al. [11] investigated potential use cases of thermal imaging in domestic setups. Researchers also explored thermal reflection properties to introduce novel interaction technique [33, 39] or for extending our visual perception [7]. Another example is remote physiological motoring [28], where researchers looked at the changes in facial temperature to infer users' internal states (e.g., cognitive load and emotions). From the last example, it already becomes clear that thermal cameras allow sensitive information to be revealed. This becomes even more apparent when looking at security threats. Abdelrahman et al. [6] demonstrated that thermal cameras enable so-called thermal attacks, where thermal imaging can capture heat traces left after touching the surface of a smartphone, allowing the entered PIN or lock pattern to be retrieved. This raises the question of how users perceive this technology – in particular regarding privacy. To close this gap, this work contributes an interview study. As becomes apparent from prior work, there are many use cases and opportunities, many of which are unknown to end-users. Hence, our exploration will focus both on novice and knowledgeable users.

2.2 Perception of Camera-based Technologies

The privacy implications of sensing devices are of great interest to researchers [25, 32]. Cameras demand particular attention due to societal and legal expectations of privacy as they seamlessly and unobtrusively capture users in the field of view. Koelle et al. investigated the privacy perception of body-worn cameras [30] and data glasses [31] from both a legal and a social perspective. They highlighted that despite body-worn cameras having potential benefits, they still impose ethical pitfalls and might affect bystander privacy. Widen extended this space by exploring the privacy concerns of smart cameras [45]. Unlike body-worn cameras and always-on cameras, a smart camera does not passively record information. Instead, it recognizes visual patterns using algorithms. Widen plotted a privacy matrix based on the users' location and vantage point. Researchers discussed the benefits, risks, and legalities of lifelogging [49] and concerns of dashcam video shar-

ing [38]. Beyond cameras, Hassib et al. [27] investigated users' perception of bio-sensing and affective wearable devices and how they influence users' privacy. Recent studies investigated privacy concerns with drones [50], smartwatches [41], Internet-connected toys [35], and autonomous vehicles [15]. Researchers also explored the perception of the emerging field of Internet of Things (IoT) devices integrated into (smart) homes) [55, 47, 53, 23], revealing concerns and challenges.

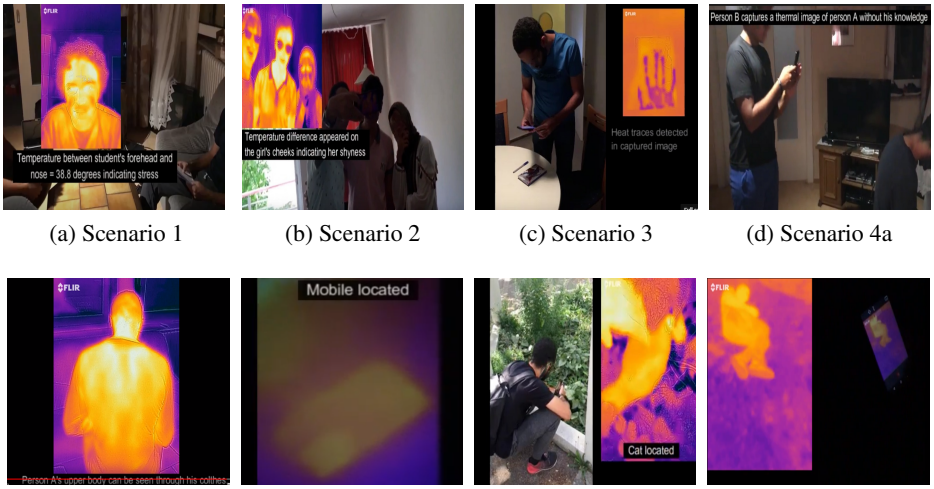
Several approaches exist to mitigate privacy concerns. Examples include attempts to establish best practices among designers and developers when creating applications that deal with sensitive data [13], approaches that try to filter the collected data [16], or proposing solutions in the form of data management [17]. However, as Jacobsson et al. [29] note, a prerequisite to creating meaningful approaches and strategies for privacy protection is to understand users. However, there is no substantial work exploring perceptions of end-users regarding thermal cameras and how their privacy concerns could be mitigated. In this work, we investigate and report end-users suggestions of rules, regulations, censorship for thermal camera usage in public. Thus, our work can serve as a guideline for developer and policymakers.

2.3 Influence on Privacy Perception

Understanding privacy concerns is critical to determine end-users' attitudes and behavior regarding acceptance of a technology [18]. Privacy perception is influenced by different factors, most notably culture [34], country of residence [14], age [46], gender [52] and knowledge [37]. Users can be grouped by a wide range of characteristics beyond culture, including users' behavior, e.g., privacy minimalists, self-censors, and privacy balancers. Wisniewskia et al. [48] categorized users into six profiles depending on their sharing and privacy attitudes in Online Social Networks (OSNs) and offered design implications per user group. Education, and knowledge play a critical role in privacy perception as well. For example, previous work showed that educated people have more privacy knowledge and, hence, are more aware of privacy practices and contemporary privacy and security scenarios [44, 40, 36, 21]. For instance, Culnan at al. [21] investigated the characteristics of users who are aware of privacy preserving features, such as the possibility to have names removed from mailing lists. Users who are unaware of this are less likely well-educated, and are less likely concerned about privacy. Youn [51] reports that teenagers were less prone to giving out personal information and conduced to engage in risk-reducing strategies such as providing incomplete information, moving to alternative web sites that do not ask for personal information if they are aware of information disclosure online. Prior work highlights the challenge of holistically understanding privacy concerns towards a novel technology and the consumer's ability to enhance individual privacy protection through the use of technology [43]. To account for this influence of the understanding of thermal imaging as well as to better understand its implications, we investigate privacy perceptions of thermal imaging among users with different levels of understanding of the technology.

3 Research Approach

To understand privacy concerns towards thermal cameras, we designed an interview study. To assess both the view of people with and without an in-depth *understanding*, we conduct parts of the interviews with people whom we first presented video showcases



(a) Scenario 1 (b) Scenario 2 (c) Scenario 3 (d) Scenario 4a

(e) Scenario 4b (f) Scenario 5 (g) Scenario 6 (h) Scenario 7

Fig. 1: Screenshots from the video showcases used in the interview

(primed) and parts with people not shown the video showcases (unprimed). In this way we account for the fact that thermal imaging is still in the early stage of consumer market penetration and participants generally do not own and, thus, have an in-depth understanding of thermal imaging.

3.1 Video Showcases

The video showcases were inspired by the literature. We came up with several scenarios in which we demonstrated what can be done with the use of thermal cameras. We opted for realistic scenarios that have been explored in prior research. These scenarios are based on current use cases of thermal cameras [8, 12, 10, 28]. We expanded them to reflect privacy / utility trade-offs. Scenarios were designed to highlight opportunities but also point to how this technology could violate users' privacy. The videos were recorded using a FLIR One[6], a thermal camera attachable as an add-on to a smartphone.

Scenario 1 – Detecting Stress / Cognitive Load: This scenario presents an exam situation in which a student is asked questions by an examiner. A thermal camera captures the temperature of the student's forehead and nose. The increased temperature indicates that the student is under stress and increased cognitive load [28] (cf. Figure 1a). The video includes an explanation about the process: the camera captures the temperature. Subsequently, machine learning methods are used to derive the exact temperature and, thus, the stress level and cognitive load. It also discusses that it is possible to capture this information without the student's consent.

Scenario 2 – Detecting Emotions: This scenario shows a situation in which three friends (two males, one female) are having a chat in which they decide to take a selfie with a thermal camera. The selfie reveals a temperature difference on the girl's cheek,

[6] https://www.flir.com/flir-one/

indicating her shyness [28] (Figure 1b). The video explains that this is just one example where thermal imaging can reveal a user's emotion, even though a user (or bystander) might not have intended to reveal that information.

Scenario 3 – Use of Personal Objects: In this scenario, a person is writing in his diary. After he left the room to go for a walk, another person enters the room and starts reading in the diary. After leaving, the person who wrote the diary returns. The thermal image reveals that somebody touched the diary [19] (Figure 1c).

Scenario 4 – Seeing through Clothes: This video shows a scene in which a person captures a thermal image from a bystander from behind their back with the bystander neither noticing nor giving consent [11] (Figure1d). This demonstrates both what the camera can reveal and how easy it is to obtain private information without consent.

Scenario 5 – Locating Objects in Dark: In this video, a person puts a baby to sleep in a bedroom and turns off the light. Then he remembers that he left his phone in baby's room. So, he starts scanning the baby's room with a thermal camera without turning on the light, as he does not want the baby to wake up and finds his phone [11] (Figure 1f).

Scenario 6 – Locating a Pet: The video shows a person walking in the street. He hears a kitten crying behind a bush. Since he cannot see behind the bush, he is unable to locate the kitten. Using the thermal camera to scan the bush allows him to quickly locate the kitten, as its body temperature is different from that of the leaves of the bush [11].

Scenario 7 – Emergency Situation: In this video, two people are walking through a forest at night as one of them suddenly faints. As the other person notices, he immediately starts looking for his friend, but cannot easily locate him due to the darkness. So he starts scanning the surroundings with a thermal camera to quickly locate his friend [8].

3.2 Recruitment & Demographics

We recruited a total of 70 participants through our University's mailing list. The study was carried out between May to September 2019. To obtain a more diverse sample, we complemented recruiting with Snowball sampling, where initial participants suggested additional interviewees. The study was approved by the Institutional Review Board. We had a primed and an unprimed group. Among the 37 *primed* participants, 22 were male and 15 female. The participants were aged from 19 to 61 ($M = 27.1, SD = 8.9$). For the *unprimed group*, we had 33 participants (19 male, 14 female), aging between 19 to 58 ($M = 29.8, SD = 8.9$). Participants had different occupations [7].

3.3 Procedure & Analysis

As participants arrived at the lab, we introduced them to the study's purpose. Afterward, participants filled in a demographic questionnaire. We then asked participants whether they were generally familiar with thermal cameras and whether they had any prior experience with the technology. If they did, we asked them to describe their experience in detail. Afterwards, we explained the structure and functionality of a thermal camera. Finally, we randomly assigned them to either the unprimed or the primed group. We then showed the different videos we introduced in the previous section to the primed group before proceeding with the actual interview. The unprimed group proceeded with the interview immediately. In the interview, we first asked them about their general

[7] https://bit.ly/3ARQ9Dj

perception and what they thought about the use of thermal cameras. We then, more specifically, asked how they would feel if friends, family members, or strangers used a thermal camera while being in their vicinity and vice versa. We also asked about the following aspects: asking others for consent before using a thermal camera in the vicinity of others, censorship, and sharing thermal images in social media [8].

All interviews were transcribed manually for analysis. As the primary coders, two authors conducted inductive coding for 3 sample participants from each group and discussed them. Both coders used the QDA miner software [1]. The authors agreed on a codebook, containing 13 codes for the primed and 10 codes for the unprimed condition. Then, both coders coded the remaining transcripts independently using the codebook with no further changes made to the codebook. When coding was complete, the researchers compared each code and discussed and resolved any disagreements. Disagreements were tracked, and inter-rater agreement was calculated at 89.82% for primed interviewees and 96.4% for the unprimed interviewees. Overall, ten codes were the same between the two settings. As a final step, we compared the results of the primed setting and the unprimed. While discussing the results, we enumerate the participants from P1 to P37 for the primed group, UP1 to UP33 for the unprimed group.

4 General Privacy Perceptions

We start by presenting common themes among interviewees from all study conditions before focusing on differences among interviewees from the primed / unprimed groups in the following sections. To describe the similarities of a point of view in our sample, we frequently specify the numbers of participants while describing a particular perception. We also use keywords like 'majority' to refer to more than 22 participants, 'some' for 10–21 participants, and 'few' for less than 9 participants.

4.1 Disruption of Private Space

The majority of the participants of both groups were highly concerned about their private space being invaded. They talked about the violation of their private space by the use of a thermal camera around. The privacy of personal things or personal space, the possibility of getting physically tracked, being a victim of criminal activities as the thermal camera can see things in the dark, emerged as key perceptions. Users reacted negatively towards these opportunities of misuse.

> " It's like a double edged weapon, good to use in places like airports, but if used on my room or home, it will be disturbing." (*P33*)

> "If the light is off, this maybe means somebody wants some privacy, but using this camera you can get to know what they are doing." (*UP20*)

Overall, there was a negative impression of the thermal camera in the users' minds as they perceived it violates their expectations towards the rights to privacy. Some talked about other violations, like the misuse of the thermal camera for hunting animals, night photography by criminals, and terrorists.

[8] Interviews questionshttps://bit.ly/3ARQ9Dj

4.2 Disclosure of Emotional/Cognitive State

All participants from the primed group, and few participants from the unprimed group talked about the violation of their cognitive and sentimental privacy by the use of a thermal camera around. Though, it was clearly mentioned that users' inner emotions or cognitive state could be revealed with the help of machine learning through a thermal camera. Users talked about this capability without appropriate consent can lead to inappropriate social interactions and track people's emotions and breach someone's right to privacy of thoughts and emotions. In many participants' opinions, a person's stress level can also be interpreted falsely through thermal imaging, causing inappropriate inferences. For instance, concerning inappropriate social interactions:

> "Sometimes people do not want to show [their emotion]. So a discussion might come up like why her emotions are like that. That is, again, an invasion of privacy." (*P11*)

Regarding the privacy of thoughts or feelings:

> "Thoughts and feelings are private. I would not share them. People can express them. But nobody has permission to detect others' emotions." (*P31*)

> "If somebody captures my emotions without taking my permission, then that is a violation of my privacy and unethical." (*P16*)

> "If somebody is anxious or delighted, this could show up on the thermal imaging. I would not be interested in others knowing about it." (*UP32*)

Concerning the interpretation of emotion:

> "Your thoughts are private to you unless you decide to reveal it to another person. Others might interpret the whole conversation in a very different way, for example, if your stress level increased due to a different thought." (*P12*)

In summary, there was a common point of view against the usage of thermal cameras in users' opinions based on the fact that it is possible to reveal their sentiments and mental state without their consent and can even be misused or misinterpreted.

4.3 Privacy of Body Parts

Thermal imaging can potentially reveal body shapes, shapes of private body parts through the clothes. This is a major privacy issue that was eminent among participants' comments. Most participants explicitly spoke about their privacy concerns regarding their body structure in connection with the use of thermal cameras in their vicinity. Moreover, the concerns of physical privacy being invaded, especially for women, became apparent and participants responded strongly against the use of a thermal imaging camera by the general population. A few participants said that the use of a thermal cameras without consent in public can contravene religious practice and offend religious freedom. Not surprisingly, in some participants' opinions, the misuse of a thermal camera to peek through clothes can be humiliating and embarrassing and can be considered a sexual offense.

> "Thermal cameras should be restricted to areas like airports to find illegal weapons underneath clothes. But, if someone [in public] can see through outfit, people would feel insecure. It will invade their privacy." (*P35*)

Furthermore, regarding thermal cameras invading physical privacy of women:

> "In this example, it was just a boy, but there can be girls, so more privacy invasion could occur there." (*P11*)

Also, thermal cameras can contravene religious freedom:

> "I was thinking if it can see through my clothes and as a Hijabi person I don't want anyone to see my body structure with this camera." (*P19*)

Referring to the misuse of the thermal camera UP2 said:

> "If I took a picture using a thermal camera of another person without their consent, it is not an x-ray device. But you can see, you can tell bodily parts underneath clothing. It can be misused in many ways." (*UP2*)

These comments confirms overall strong privacy concerns against thermal imaging camera use without consent, as it potentially violates physical privacy.

4.4 Privacy of Physiological Data

Some participants expressed their concerns about the use of the thermal camera to measure and interpret body temperature without the consent or knowledge of an individual, as this can reveal vital health data to third parties and violate privacy. Unlike conventional methods, a thermal camera can be used to get to know about people's body temperature and other health conditions in a non-invasive and contact-free way. As body temperature can be used to predict particular health conditions, some participants from the primed and unprimed groups shared these concerns.

> "If I have a fever I do not want people to know – but this type of camera can tell that." (*UP20*)

> "If you want to capture an image of any person, you are getting his/her body temperature for different parts [of the body] – so there is the matter of taking consent here." (*UP9*)

Participants pointed out misuse of these data:

> "People can detect if a person is sick without consent and can create a chart of the heat signature of normal and sick people to misuse it. These are threats to my privacy." (*UP20*)

> "In medicine, it [thermal imaging] should be used for identifying issues with the body. But for daily life, it would make sense to block the use of thermal cameras as it reveal others' body heat signature." (*P22*)

> "Thermal cameras extract some health information, which of course, would then present a privacy threat, potentially even revealing very sensitive information about users." (*UP25*)

This demonstrates that users generally have a strong negative opinion against thermal camera usage to collect physiological data without consent.

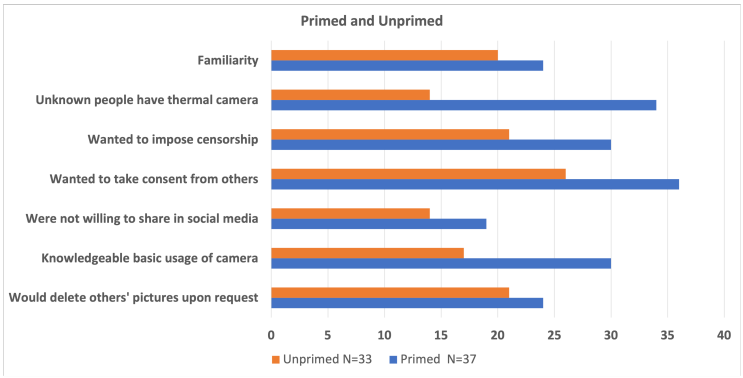


Fig. 2: Contrasting the opinions between the primed and the unprimed groups.

5 Influence of Priming

To understand the influence on an in-depth understanding about thermal imaging, we divided participants into two groups (37 primed participants, and 33 unprimed participants), using uniform random selection.

As mentioned above, we interviewed all participants, asking them about their familiarity with thermal imaging. We then explained them how thermal imaging works. After that, the primed groups watched the videos to demonstrate the use of thermal imaging cameras, including more detail of how information is obtained, thus creating an deeper understanding among participants. The unprimed group did not watch any videos. We finally assessed the opinions of both groups.

In the following we discuss the effects video demonstrations had on the understanding and perception of the primed group members in contrast to the unprimed members. Figure 2 presents a comparison of the differences.

5.1 Familiarity with Thermal Imaging Technology

Twenty four participants from the primed group were familiar with thermal cameras before the introduction to thermal cameras and being shown the videos. The majority of the primed group participants mentioned that they have seen thermal cameras on TV, thus knowing they detect heat and are used by the army, firefighters, for night visions, and for medical procedures. The majority of the participants from the unprimed group were familiar with thermal cameras before. Like the primed group, participants had seen thermal cameras on TV and mentioned use cases like getting heat signatures of living and non-living things and military as well as industrial usage.

5.2 Explanation of Basic Functionality

We explained the basic functionality and made them familiar with thermal cameras before asking participants about their opinions. We used several still images of thermal camera in action as probes and a short description of the thermal imaging procedure. On one hand, most participants from the primed group mentioned that they considered the thermal camera privacy-invasive or a threat that can be misused by impostors. On the other hand, the majority of participants from the primed group also understood the

beneficial usage of thermal cameras in a military context, for security purposes, and for firefighting.

> "It can be used for military purposes where a soldier can sense the threat ahead, [yet] if it's in the wrong hand it will be spoiled. Let's say, if it is in the hand of a thief, once he is entering or breaking into a house he can find out which person is there and in which place and can tackle them very easily." (*P2*)

The majority of the participants from the unprimed group second that thermal cameras can be misused by impostors to track people, hunt animals, spy, rob and so on. some participants also understood the benefits of thermal cameras, for industrial usage, for child and pet care by obtaining their temperature in a non-invasive way, and for military usage.

> "Thermal cameras can be privacy invasive as they see through camping tents and things like that. On the plus side they have a ton of applications in industry and maintenance." (*UP17*)

Overall the understandings of participants from both groups was similar after the introduction and discussion.

5.3 Perception and Opinions About Thermal Camera Use Cases

As mentioned above, the primed group watched the videos of different thermal camera scenarios before being asked about their opinions (compared to participants from the unprimed group who were asked right after the introductory discussion without showing them the videos). When we asked about their perceptions about an unknown person nearby using a thermal camera, there was a clear difference between the groups' opinions. Majority of the participants felt negative about an unknown person using a thermal camera around from the primed group, compared to some participants from the unprimed group. This indicates that the videos closed a considerable gap in understanding between the primed and unprimed groups, which led to differences in their opinions.

> "It can be a bit awkward definitely, if it [the camera] can penetrate through clothes and show temperature. But it does not [show body parts], it just shows some colors."(*UP14*)

This statement is not particularly accurate and shows a lack of understanding as a result of not having watched the videos. As thermal cameras captures the radiating infrared, rather than penetrating surfaces. Hence, thermal cameras cannot penetrate clothes. We explain the differences in perception in more detail.

Imposing Censorship Previously, we have found that the primed group participants are more cautious about the usage of the thermal camera. Similarly, in the context of imposing censorship to thermal cameras, their opinions remain conservative. The majority of the primed participants desired some sort of censorship or restrictions for thermal cameras usage in public, compared to some participants from the unprimed group.

> "Thermal camera manufacturers should not give full access to end users. There have to be guidelines about the sort of intrusion, or capture of data at the [end-user] level. I feel that only certain approved organizations should capture these data. (*P12*")

> "[If] I need to see how well you can see [someone's] body [using a thermal camera], but if it's not super graphic, you should not censor it. I feel 'censored' is a strong word, and it depends on the person.
> (*UP12*")

Although, we cannot clearly say that there is a difference in opinions about the censorship between primed and unprimed groups, we can certainly see a more relaxed attitude in case of unprimed participants regarding censorship.

Interest to give consent to using thermal cameras around them The majority of the participants of both groups reported that they would like to be informed about the use of thermal cameras around them. We assume that the current trend of mobile application having to request permissions to preserve users' privacy is very present among users. Thus, most participants want to be informed if there is a thermal camera in use around them.

> "I would like to know where they are positioned, purpose of use in space. Do I have access to the data or is it possible to have access to the data? I think it's more so from the state of disknowing. Also, it's like the idea of big brothers. Your behavior is different when you know you're being watched versus when you know you're not." (*UP19*)

> "It's an issue of like you're getting documentation of me. That's why I would want information informally or just having a small sign on the wall being like there is a thermal imaging camera. Like, there's security cameras all over the place and when you go into buildings, there is signs of it." (*UP31*)

Interest to ask for consent before using thermal camera When we asked participants about their interest to ask for consent from people before using a thermal camera, majority of the participants of the primed group showed interest in taking consent. In contrast, unprimed participants showed a comparatively relaxed attitude.

> "I think at least people [around me] should be aware or informed that I'm using a thermal camera, so that there is a choice for the other person to say 'yes' or 'no'. Without consent, reaction of the other person depends upon the personality because some people are really sensitive about this kind of issues, and some are not. So, whoever is using it should have the consent of others." (*P19*)

The unprimed group displayed a more relaxed attitude. The primed group showed more interest to take consent from people before using thermal camera.

> "Its only temperature, we are not producing any output we are just checking the general events. I will not take consent because i think there is no harm of using it." (*UP22*)

Willingness to delete recordings of others upon request We asked participants if they captured a thermal image of a random person, and that person asked them to delete that image, whether they would agree to delete it. Some of both primed and unprimed participants agreed to delete the picture upon request. The attitude of both the groups was similar.

> "I will delete it without asking. But if the picture is worth or valuable to me, I will ask for consent, but if they want [it] to be deleted, I will [do that], because I respect my privacy and others', too." (*P3*)

> "If I were in that person's shoes, I would want him to delete that picture. So I will also do the same because I think it is private and it is his / her right to choose what to do with the picture." *(P21)*

> "No,I will not delete. Probably I will never see them again, there are billions of people." *(UP10)*

Interest to share their thermal image or data on social media Regarding sharing thermal images or data in social media, while some primed participants explicitly denied sharing, the majority of unprimed participants were not having issues sharing.

> "It exposes more than I want. It shows something that I want to hide. I will not share it." (*P3*)

> "I don't want my personal things to be out for anyone. " (*P24*)

> "Yes, I don't mind sharing my data, but if [it is] someone else's data, I will ask them."(*UP16*)

> "It's fine if I share my thermal image and readings with anyone. It doesn't show anything." (*UP30*)

Self-expected use of thermal cameras The majority of the participants of the primed group perceived the utility of thermal cameras useful in various ways, for example, finding lost objects or pets, as studying tools, for architecture, in emergencies, during camping and so on. At the same time, only some of the unprimed participants mentioned useful cases, such as night vision and maintenance of the house.

We also found that understanding gaps lead to less sensible decision making by unprimed users. UP11 and UP12 said that they would use the camera to look at friends' bodies to find out their body heat signatures. UP11 and UP7 said that they would use the thermal camera to observe people in public places. Also, UP31 said:

> "I would use it for fun, to see friends reaction or state reflects changes in temperature around their bodies. Some people blush. Their faces feel different, or they get cold or hot or so on."(*UP31*)

Suggestions	Frequency (n=70)
Limited feature access to consumer grade cameras	25
No filming without explicit consent	32
Regulatory body to monitor usage of thermal camera and data	23
Privacy laws for thermal data	34
Censoring or blurring thermogram of private body parts	48
Signage or warning of thermal camera's presence	36
Registration of thermal camera by buyers	37

Table 1: Rules, regulations, and censorships suggested by participants

Understanding update after video (primed) When we asked participants about their points of views on thermal cameras after they watched the videos, we found a negative perception in general about thermal imaging cameras by end-users. Yet, participants were very positive towards thermal cameras use by security officials and other professionals.

> "Earlier I felt thermal camera have only positive use cases. Now I think it is rather a threat in the hand of a common man." (*P27*)

A few participants also said thermal cameras should not be consumer-grade or accessible to common people.

> "I like technology but I don't like it to be consumer grade at all." (*P13*)

5.4 End-users suggestions of rules, regulations, censorship for thermal camera usage in public

We asked the participants – their suggestions of implicit censorship, rules for thermal camera usage by end-users in public. This section lists all the users' suggestions that we gathered in Table 1.

6 Discussion

We explored users' perceptions of thermal cameras, motivated by the fact that thermal imaging is increasingly becoming cheaper and is likely to end up as an everyday accessory in users' hands. Considering this, we investigated the thoughts and opinions of end-users about the risks and opportunities of thermal imaging and their expected behavior as potential thermal camera users. We conducted an interview study with 70 participants in total. We divided the participants into two groups to understand the effects of users having a detailed understanding about the technology.

Our results show that people are greatly concerned about thermal imaging in general. Yet, they recognize the importance of thermal imaging usage in industrial, health, surveillance, and security industries and value thermal imaging potential for personal use. We also found an effect of understanding on users' perceptions of this new technology. We will discuss the implications by reflecting on the results.

6.1 Privacy Implications

People mostly dislike the *extended capability* of thermal imaging cameras. They think it is utterly privacy-invasive as these cameras see the invisible [9], the cameras are even capable of tracking people inside their homes without physically intervening. Thermal cameras are capable of detecting things or humans in the visual field of view and also inconceivable in bare eyes. This raises the question of informed consent. Therefore, making such devices commercially available for end-users requires caution, and appropriate regulations need to be developed. Another popular perception regarding privacy was that thermal cameras could be used to *track behavioral patterns* and, hence, can be privacy-invasive if used publicly without regulations. Similar to other existing technologies that allow for identifying behavioral patterns (cf. research on Behavioral Biometrics), regulations need to be put in place when obtaining such data. For example the GDPR classifies such (biometric) data as particularly protect-worthy and requires user consent once collected and processed.

Moreover, almost all participants discussed the *need for consent* while a thermal camera is being used around them. Most of them agreed to ask for consent from others when they own a camera and use it publicly. Designers and developers of thermal camera applications should be capable of detecting when humans are in the visual field of view and when not, so as to ask for consent first if this is the case, or at least inform the users. This is inline with current technologies where users are informed if they are being in the view of tracking or recording systems. Also, the need for both explicit and implicit censorship was prominent among users' opinions. They also pointed out that if the cameras are available to the end-users, there should be a lesser capability like blurring out the temperature of private body parts. Also, restrictions should be imposed on the devices so that the users should not capture others' private data, like quantifiable data of the human body and mind, without their consent. Thus, thermal imaging applications needs to find the balance of which information to reveal and not to reveal. For instance, prior work suggested to provide usable access control mechanisms to our devices [54]. Additionally, thermal camera applications should only show information derived from thermal imaging data that is needed for its primary purpose and does not let other conclusions to be drawn. For example, if a thermal camera application is used to detect emotion based on the changes of the facial temperature [28], only the inferred emotion should be displayed without showing the facial information.

All these concerns were raised by our participants who are generally more informed. We conclude that the current trend of managing standard privacy practices and the research on managing boundaries in modern applications makes people more aware of keeping their privacy and inherently make them self-conscious.

6.2 Privacy vs. Utility

As discussed above, people are reasonably concerned about their privacy. Nevertheless, if the system provides a sufficiently large benefit for users they consider the *privacy-utility trade-off* (cf. the privacy calculus [22]). For instance, users were generally against thermal camera usage if used on them and without their consent. Yet, if they were lost or in an urgency need, they thought a thermal camera could be a good way of helping them and did not argue about privacy. Besides, we learned that users are highly concerned

about consumers obtaining thermal imaging tools easily due to their low price and availability. Nevertheless, they recognized that cameras being widely available could be useful in supporting children, older adults, pets, and wild animals regarding health, emergencies, and rescue measures.

Moreover, although there was a vital concern about being tracked inside the home, some people wanted to install such devices as home security devices. Some of them even mentioned that they could be used like keeping legal guns at home to protect themselves, following proper regulations. Users' also acknowledged the use of thermal cameras for the health sector. Most users recognized that the use of thermal imaging by authorized personnel could be allowed. However, there was some resistance against the unaccountable use of thermal cameras in security and surveillance. There should also be a purpose to use these cameras by authorized personnel. This can mean there was an apparent tension between managing the personal space and recognizing the need and purpose. For instance, thermal cameras should be used responsibly by authorized personal like the way they use other tools e.g., voice recorders or tracking devices, and not misuse it for non-professional usage.

6.3 Effects of Understanding

We found differences between the primed groups' and the unprimed groups' opinions regarding privacy concerns, imposing censorship and consent. Figure 2 shows that the primed users, in general, were more aware of thermal imaging use and concerned about privacy. Overall, primed users talked about privacy from many more angles than the unprimed users. They were also aware of more thermal imaging use cases and were aware of thermal cameras' risks and benefits. The reason behind these contrasts was the informative video scenarios we showed to the primed users to increase their understanding on thermal camera usage. The challenge is that thermal imaging is not too widely used yet among the general public and that, thus, many of the questions are hypothetical. With out method we (a) mitigate this through priming and (b) show the effects of this. We do believe that our priming method was successful, as the gap in understanding between the two groups were observed and even prompted some unusual decisions from the unprimed users. Furthermore, the lack of a proper understanding led to concerning comments from several participants. For example, some unprimed participants said they would use the camera to look at their friends' bodies to find their body heat signatures. Also, they would use the thermal camera to observe people in public places for fun. Therefore, it is evident that there was a substantial effect of understanding on people's privacy decision making. This suggests that there is a need to better educate people before introducing this technology to the mass market.

The gap in understanding became also apparent while discussing use cases with the unprimed participants. They had misconception on the thermal camera usage. For instance, unprimed participants state that by using a thermal camera it could be revealed who touched their objects. However, the camera only shows that objects have been touched, but not necessarily by whom.

7 Limitations and Future Work

In this work, we explore users' perception of thermal cameras by collecting qualitative feedback. A general challenge is the sample size in such studies. Participants are usually

recruited until reaching data saturation [24]. Yet we agree that this does not allow for strong quantitative comparisons and generalizations. We followed recommendations from prior work. Furthermore, we tried to ensure that participants were demographically diverse. However, we acknowledge that many participants were from a University population and future research including other samples might yield additional insights. Still we believe our participants to be among early adopters and potential main users of thermal cameras. Thermal imaging has numerous applications, of which we showed a few use cases to participants. Showing more scenarios in future studies might lead to additional insights. As thermal imaging is still not widely used by consumers, most of the questions were still hypothetical.

This study is an attempt to identify important starting points for future investigations. Future work might employ other methods, e.g., surveys, to also collect more quantitative insights. Also, it would be interesting to see if different scenarios or media for priming on privacy concerns could lead to additional or different insights. Future work on ways to inform the users that thermal cameras function is essential. Future work could investigate appropriate approaches to censorship and eventually develop a privacy framework for consumer-grade thermal cameras in terms of privacy and censorship.

8 Conclusion

Thermal cameras are likely to be integrated with personal devices in the future. This study investigates users' privacy perceptions of thermal imaging. We contribute timely insights by investigating users' prior knowledge, understanding, opinions, and concerns. We compared perceptions of users with and without in-depth knowledge about thermal imaging by using video showcases. These were inspired by the current use cases from the literature, and pointed out opportunities and potential threats. We found that perceptions were influenced by the prior knowledge of participants. This suggests that people, in general, should be made aware of the strengths and weaknesses – in particular, from a privacy perspective – before this technology becomes widely available and integrated with consumer devices. Researchers might look into methods of creating this awareness in the future. In this way, implications of this technology will become more apparent.

Acknowledgment

This research was supported by dtec.bw – Digitalization and Technology Research Center of the Bundeswehr [Voice of Wisdom].

References

1. Free qualitative data analysis software — qda miner lite, https://provalisresearch.com/products/qualitative-data-analysis-software/freeware/, accessed: 2021-10-12 06:41:14
2. Kyllo v. united states (2001), https://www.law.cornell.edu/supct/html/99-8508.ZO.html. Accessed on March 22, 2022
3. Thermal Imaging Surveillance (Jan 2015), https://theyarewatching.org/technology/thermal-imaging-surveillance. Accessed on March 22, 2022
4. Top Uses and Applications of Thermal Imaging Cameras - Grainger Industrial Supply (2015), https://www.grainger.com/content/qt-thermal-imaging-applications-uses-features-345. Accessed on 02/21/2020

5. Coronavirus outbreak: Safety measures at major airports and airlines (Feb 2020), https://www.airport-technology.com/features/coronavirus-measures-world-airports/. Accessed on 02/21/2020
6. Abdelrahman, Y., Khamis, M., Schneegass, S., Alt, F.: Stay cool! understanding thermal attacks on mobile-based user authentication. In: Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems. pp. 3751–3763. ACM (2017)
7. Abdelrahman, Y., Knierim, P., Wozniak, P., Henze, N., Schmidt, A.: See through the fire: Evaluating the augmentation of visual perception of firefighters using depth and thermal cameras. In: Workshop on Ubiquitous Technologies for Augmenting the Human Mind (2017)
8. Abdelrahman, Y., Knierim, P., Wozniak, P.W., Henze, N., Schmidt, A.: See through the fire: evaluating the augmentation of visual perception of firefighters using depth and thermal cameras. In: Proceedings of the 2017 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2017 ACM International Symposium on Wearable Computers. pp. 693–696 (2017)
9. Abdelrahman, Y., Schmidt, A.: Beyond the visible: Sensing with thermal imaging. Interactions **26**(1), 76–78 (Dec 2018). https://doi.org/10.1145/3297778, https://doi.org/10.1145/3297778
10. Abdelrahman, Y., Velloso, E., Dingler, T., Schmidt, A., Vetere, F.: Cognitive heat: exploring the usage of thermal imaging to unobtrusively estimate cognitive load. Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies **1**(3), 1–20 (2017)
11. Abdelrahman, Y., Woundefinedniak, P.W., Knierim, P., Weber, D., Pfeuffer, K., Henze, N., Schmidt, A., Alt, F.: Exploring the domestication of thermal imaging. In: Proceedings of the 18th International Conference on Mobile and Ubiquitous Multimedia. MUM '19, Association for Computing Machinery, New York, NY, USA (2019). https://doi.org/10.1145/3365610.3365648, https://doi.org/10.1145/3365610.3365648
12. Abdelrahman, Y., Woźniak, P.W., Knierim, P., Weber, D., Pfeuffer, K., Henze, N., Schmidt, A., Alt, F.: Exploring the domestication of thermal imaging. In: Proceedings of the 18th International Conference on Mobile and Ubiquitous Multimedia. pp. 1–7 (2019)
13. Adams, D., Bah, A., Barwulor, C., Musaby, N., Pitkin, K., Redmiles, E.M.: Ethics emerging: the story of privacy and security perceptions in virtual reality. In: Fourteenth Symposium on Usable Privacy and Security ({SOUPS} 2018). pp. 427–442 (2018)
14. Anton, A.I., Earp, J.B., Young, J.D.: How internet users' privacy concerns have evolved since 2002. IEEE Security Privacy **8**(1), 21–27 (2010). https://doi.org/10.1109/MSP.2010.38
15. Bloom, C., Tan, J., Ramjohn, J., Bauer, L.: Self-driving cars and data collection: Privacy perceptions of networked autonomous vehicles. In: Proceedings of the Thirteenth USENIX Conference on Usable Privacy and Security. p. 357–375. SOUPS '17, USA (2017)
16. Buschek, D., Bisinger, B., Alt, F.: Researchime: A mobile keyboard application for studying free typing behaviour in the wild. In: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems. CHI '18, Association for Computing Machinery, New York, NY, USA (2018). https://doi.org/10.1145/3173574.3173829, https://doi.org/10.1145/3173574.3173829
17. Carminati, B., Colombo, P., Ferrari, E., Sagirlar, G.: Enhancing user control on personal data usage in internet of things ecosystems. In: 2016 IEEE International Conference on Services Computing (SCC). pp. 291–298. IEEE (2016)
18. Castañeda, J.A., Montoro, F.J.: The effect of internet general privacy concern on customer behavior. Electronic Commerce Research **7**(2), 117–141 (2007)
19. Cho, K.W., Lin, F., Song, C., Xu, X., Gu, F., Xu, W.: Thermal handprint analysis for forensic identification using heat-earth mover's distance. In: 2016 IEEE International Conference on Identity, Security and Behavior Analysis (ISBA). pp. 1–8. IEEE (2016)
20. Cross, C.B., Skipper, J.A., Petkie, D.: Thermal imaging to detect physiological indicators of stress in humans. In: SPIE Defense, Security, and Sensing. pp. 87050I–87050I. International Society for Optics and Photonics (2013)

21. Culnan, M.J.: Consumer awareness of name removal procedures: Implications for direct marketing. Journal of direct marketing **9**(2), 10–19 (1995)
22. Dinev, T., Hart, P.: An extended privacy calculus model for e-commerce transactions. Information systems research **17**(1), 61–80 (2006)
23. Emami-Naeini, P., Bhagavatula, S., Habib, H., Degeling, M., Bauer, L., Cranor, L.F., Sadeh, N.: Privacy expectations and preferences in an iot world. In: Proceedings of the Thirteenth USENIX Conference on Usable Privacy and Security. p. 399–412. SOUPS '17, USENIX Association, USA (2017)
24. Francis, J.J., Johnston, M., Robertson, C., Glidewell, L., Entwistle, V., Eccles, M.P., Grimshaw, J.M.: What is an adequate sample size? operationalising data saturation for theory-based interview studies. Psychology & Health **25**(10), 1229–1245 (2010). https://doi.org/10.1080/08870440903194015, https://doi.org/10.1080/08870440903194015, pMID: 20204937
25. Friedewald, M., Finn, R., Wright, D.: Seven Types of Privacy, pp. 3–32 (01 2013). https://doi.org/10.1007/978-94-
26. Gade, R., Moeslund, T.B.: Thermal cameras and applications: a survey. Machine vision and applications **25**(1), 245–262 (2014)
27. Hassib, M., Khamis, M., Schneegass, S., Shirazi, A.S., Alt, F.: Investigating user needs for bio-sensing and affective wearables. In: Proceedings of the 2016 Chi conference extended abstracts on human factors in computing systems. pp. 1415–1422 (2016)
28. Ioannou, S., Gallese, V., Merla, A.: Thermal infrared imaging in psychophysiology: potentialities and limits. Psychophysiology **51**(10), 951–963 (2014)
29. Jacobsson, A., Davidsson, P.: Towards a model of privacy and security for smart homes. In: 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT). pp. 727–732. IEEE (2015)
30. Koelle, M., Rose, E., Boll, S.: Ubiquitous intelligent cameras—between legal nightmare and social empowerment. IEEE MultiMedia **26**(2), 76–86 (April 2019). https://doi.org/10.1109/MMUL.2019.2902922
31. Koelle, M., Kranz, M., Möller, A.: Don't look at me that way! understanding user attitudes towards data glasses usage. In: Proceedings of the 17th international conference on human-computer interaction with mobile devices and services. pp. 362–372 (2015)
32. Koops, B.J., Newell, B.C., Timan, T., Skorvanek, I., Chokrevski, T., Galic, M.: A typology of privacy. U. Pa. J. Int'l L. **38**, 483 (2016)
33. Larson, E., Cohn, G., Gupta, S., Ren, X., Harrison, B., Fox, D., Patel, S.: Heatwave: Thermal imaging for surface user interaction. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. pp. 2565–2574. CHI '11, ACM, New York, NY, USA (2011). https://doi.org/10.1145/1978942.1979317, http://doi.acm.org/10.1145/1978942.1979317
34. Li, Y., Kobsa, A., Knijnenburg, B.P., Nguyen, M.C.: Cross-cultural privacy prediction. Proceedings on Privacy Enhancing Technologies **2017**(2), 113–132 (2017)
35. McReynolds, E., Hubbard, S., Lau, T., Saraf, A., Cakmak, M., Roesner, F.: Toys that listen: A study of parents, children, and internet-connected toys. In: Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems. pp. 5197–5207 (2017)
36. Mekovec, R., Vrček, N.: Factors that influence internet users' privacy perception. In: Proceedings of the ITI 2011, 33rd International Conference on Information Technology Interfaces. pp. 227–232. IEEE (2011)
37. Mekovec, R., Vrček, N.: Factors that influence internet users' privacy perception. In: Proceedings of the ITI 2011, 33rd International Conference on Information Technology Interfaces. pp. 227–232 (2011)
38. Park, S., Kim, J., Mizouni, R., Lee, U.: Motives and concerns of dashcam video sharing. In: Proceedings of the 2016 CHI. pp. 4758–4769 (2016)

39. Sahami Shirazi, A., Abdelrahman, Y., Henze, N., Schneegass, S., Khalilbeigi, M., Schmidt, A.: Exploiting thermal reflection for interactive systems. In: Proceedings of the 32Nd Annual ACM Conference on Human Factors in Computing Systems. pp. 3483–3492. CHI '14, ACM, New York, NY, USA (2014). https://doi.org/10.1145/2556288.2557208, http://doi.acm.org/10.1145/2556288.2557208
40. Saleh, M., Khamis, M., Sturm, C.: What about my privacy, habibi? understanding privacy concerns and perceptions of users from different socioeconomic groups in the arab world (April 2019), http://eprints.gla.ac.uk/186430/
41. Udoh, E.S., Alkharashi, A.: Privacy risk awareness and the behavior of smartwatch users: A case study of indiana university students. In: 2016 Future Technologies Conference (FTC). pp. 926–931. IEEE (2016)
42. Wadhwani, P., Gankar, S.: Thermal imaging market report 2024 - global industry share forecast (Jun 2018), https://www.gminsights.com/industry-analysis/thermal-imaging-market. Accessed on 02/21/2020
43. Wang, H., Lee, M.K., Wang, C.: Consumer privacy concerns about internet marketing. Communications of the ACM **41**(3), 63–70 (1998)
44. Wang, P., Petrison, L.A.: Direct marketing activities and personal privacy: A consumer survey. Journal of Direct Marketing **7**(1), 7–19 (1993)
45. Widen, W.H.: Smart cameras and the right to privacy. Proceedings of the IEEE **96**(10), 1688–1697 (2008)
46. Wilkowska, W., Ziefle, M.: Perception of privacy and security for acceptance of e-health technologies: Exploratory analysis for diverse user groups. In: 2011 5th International Conference on Pervasive Computing Technologies for Healthcare (PervasiveHealth) and Workshops. pp. 593–600 (2011). https://doi.org/10.4108/icst.pervasivehealth.2011.246027
47. Wilson, C., Hargreaves, T., Hauxwell-Baldwin, R.: Smart homes and their users: a systematic analysis and key challenges. Personal and Ubiquitous Computing **19**(2), 463–476 (2015)
48. Wisniewski, P.J., Knijnenburg, B.P., Lipford, H.R.: Making privacy personal: Profiling social network users to inform privacy education and nudging. International Journal of Human-Computer Studies **98**, 95–108 (2017). https://doi.org/https://doi.org/10.1016/j.ijhcs.2016.09.006, https://www.sciencedirect.com/science/article/pii/S1071581916301185
49. Wolf, K., Schmidt, A., Bexheti, A., Langheinrich, M.: Lifelogging: You're wearing a camera? IEEE Pervasive Computing **13**(3), 8–12 (2014)
50. Yao, Y., Xia, H., Huang, Y., Wang, Y.: Free to fly in public spaces: Drone controllers' privacy perceptions and practices. In: Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems. pp. 6789–6793 (2017)
51. Youn, S.: Teenagers' perceptions of online privacy and coping behaviors: a risk–benefit appraisal approach. Journal of Broadcasting & Electronic Media **49**(1), 86–110 (2005)
52. Youn, S., Hall, K.: Gender and online privacy among teens: Risk perception, privacy concerns, and protection behaviors. Cyberpsychology & behavior **11**(6), 763–765 (2008)
53. Zeng, E., Mare, S., Roesner, F.: End user security & privacy concerns with smart homes. In: Proceedings of the Thirteenth USENIX Conference on Usable Privacy and Security. p. 65–80. SOUPS '17, USENIX Association, USA (2017)
54. Zeng, E., Roesner, F.: Understanding and improving security and privacy in multi-user smart homes: A design exploration and in-home user study. In: 28th USENIX Security Symposium (USENIX Security 19). pp. 159–176. USENIX Association, Santa Clara, CA (Aug 2019), https://www.usenix.org/conference/usenixsecurity19/presentation/zeng
55. Zheng, S., Apthorpe, N., Chetty, M., Feamster, N.: User perceptions of smart home iot privacy. Proc. ACM Hum.-Comput. Interact. **2**(CSCW) (Nov 2018). https://doi.org/10.1145/3274469, https://doi.org/10.1145/3274469