Issues in Information Systems
Volume 23, Issue 4, pp. 94-110, 2022

DOI: https://doi.org/10.48009/4_iis_2022_109

Internet of things: Measuring data privacy concerns of users

Adnan Chawdhry, *Pennsylvania Western University, chawdhry_a@pennwest.edu*
Karen Paullet, *Robert Morris University, paullet@rmu.edu*
Jamie Pinchot, *Robert Morris University, pinchot@rmu.edu*

Abstract

This study examined data privacy concerns related to the collection of data from Internet of Things (IoT) devices. There is a plethora of data generated from IoT devices which lends room for misuse of personal data gathered. This quantitative study attempts to understand users' privacy concerns as they relate to IoT enabled devices and their associated mobile apps. A total of 353 participants were surveyed for this study. The Mobile Users' Information Privacy Scale (MUIPC) was used to measure three core areas related to privacy that include perceived surveillance, perceived intrusion, and secondary use of personal information

Keywords: data privacy, privacy, mobile devices, Internet of Things, social media

Introduction

Data privacy is one of the most critical issues facing both individuals and organizations today. Belanger et al. (2011) suggest that privacy is "one's ability to control information about oneself" (p. 1018), and this definition also lends itself to the concept of data privacy in an increasingly digital world. Concern about data privacy has only increased due to the number of data breaches and privacy threats that continue to emerge (Hammouchi et al., 2019). The plethora of devices that can connect to the Internet, often referred to as "smart" devices and collectively known as the Internet of Things (IoT), exacerbates the problem by exponentially increasing the amount of personal data that is generated. IoT devices present a serious threat to personal data privacy (Foltz & Foltz, 2021; Zheng et al., 2018).

There are many different types of IoT devices and each type of device can incorporate a variety of sensors capable of automatically generating and collecting a vast amount of data including audio, video, GPS/location data, temperature, timestamps, and medical data (Zheng et al., 2018). There are devices that are used by individuals, including the ubiquitous smart phone (and all of the apps that come with it), smart watches, fitness and health trackers, wearables, and even smart cars. There are also IoT devices used within the living environment to create a smart home such as connected refrigerators, learning thermostats, video doorbells, energy tracking switches, smart baby monitors, and app- and voice-controlled lights, shades, speakers, and security cameras (Zheng et al., 2018). Lastly, there are devices that make up a smart city, which can include smart parking meters, smart traffic lights, and surveillance cameras.

The amount of data generated from these devices, often without the knowledge of the user, is staggering, and due to a lack of regulation as well as security challenges faced by IoT devices (Cirne et al., 2022; Saleem et al., 2018; Weber & Boban, 2016), there is great potential for misuse of personal data gathered from IoT devices. Despite the potential for misuse of personal data, the benefits provided can often outweigh the concern for data privacy, as evidenced by the rapidly growing use of IoT devices. This study will attempt to further understand the privacy concerns held by users of these devices.

Literature review

The use of IoT devices has become commonplace in the United States and around the world. As of June 2022, there were more than 10 billion active IoT devices. By 2025, there will be 152,200 IoT devices connecting to the Internet per minute. It is estimated that the number of IoT devices will surpass 25.4 billion by 2030. The amount of data generated by IoT devices is expected to reach 73.1 ZB (zettabytes) by 2025 (Jovanovic, 2022).

New Privacy Challenges for Internet of Things

New methods of data collection from IoT devices have led to new privacy challenges. Some of the challenges include obtaining consent for data collection, allowing users to control, customize and choose data they share, and ensuring that the use of collected data is limited to the stated purpose (Charith et al., 2015). The use of IoT devices has also brought about risks to personal privacy and safety. In order for IoT devices to be accepted by consumers, the developers of such devices must consider the privacy and security implications of their products (Emami-Naeini et al., 2017).

As people carry smart phones and share their lives on social network sites, we are witnessing an increasing penetration of people's private and public lives by technology that enables data collection, which in turn enables identification, tracking, and profiling (Radomirovic, 2010). Identification is the threat of associating a personal identifier such as a name, address, or pseudonym to information gathered about the user. Tracking is the threat of determining, recording, or following a person's location while their devices are turned on and in use. For instance, tracking can take place through GPS, app data, Internet traffic or cell phone triangulation. Lastly, profiling denotes the threat of compiling information about individuals in order to infer an individual's interests by gathering and correlating data from multiple profiles and sources. Profiling can lead to various privacy violations including discrimination, unsolicited advertisements, and social engineering (Ziegeldorf et al., 2014).

Personally Identifiable Information (PII) can be gathered from IoT devices without the user's consent. Chaudhuri (2015) designated that privacy can be classified into four categories: identity, location, search query, and digital footprint. As IoT devices are owned by individuals, the identity of these devices helps to identify the owners. An IoT device's location can be used to gather information about the owner's location. Search queries can disclose information about the person who initiated the search by tracking the IP address of the device to the source. Lastly, the digital footprint can be mapped out because IoT devices are always online, and therefore leave behind traceable data (Kanniappan et al., 2017).

Privacy is essential while communicating and connecting via IoT devices. In order to protect personal information, users must become aware of the risks associated with using IoT devices (Pinchot et al., 2014). As stated by Dotzer (2006), "Once privacy is lost, it is very hard to re-establish that state of personal rights" (p. 14).

IoT privacy policies are one area where the technology industry is attempting to improve. Privacy policies have historically been lengthy and confusing and therefore are often ignored by consumers. Kuznetsov et al. (2022) have worked to identify ways to write privacy policies in natural language to improve transparency for readers. Emami-Naeini et al. (2020) proposed an IoT privacy and security label for devices that will provide critical information for consumers in a standardized way; however, no label has currently been adopted by the industry.

Privacy Laws in the United States and Europe

Privacy, although not mentioned in the U.S. Constitution, is considered a fundamental human right. The first major piece of legislation on information privacy was the Privacy Act of 1974 which protects records about individuals retrieved by personal identifiers such as name, social security number, or other identifying numbers or symbols. This Act established a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies (U.S. DOJ, 2022).

A federal law that protects the privacy of children is the Children's Online Privacy Protection Act (COPPA). This law limits the collection and usage of privacy information about children for all operators of Internet services and websites. Prior to the law being passed, the Federal Trade Commission (FTC) surveyed 212 websites and found that approximately 90% of websites collected children's private information. COPPA imposes certain requirements on operators of websites or online services directed to children under 13 years of age, and on operators of other websites or online services that have actual knowledge that they are collecting personal information online from a child under the age of 13. For instance, when a person signs up for a social networking site, they are often required to confirm that they are over the age of 13. This option is in place due to COPPA (FTC, 2022).

There are several other U.S. laws that protect specific types of data only. The Health Insurance Portability and Accountability Act (HIPAA) covers communications between a patient and covered entities such as doctors and insurance companies. The Family Educational Rights and Privacy Act (FERPA) controls who can access student education records. The Electronic Communications Privacy Act (ECPA), passed in 1986, restricts government wiretaps on telephone calls and some electronic signals. However, it is outdated and does not protect against modern surveillance techniques or search of data in cloud-based storage. Another somewhat outdated law is the Video Privacy Protection Act (VPPA), which prevents the disclosure of VHS videotape rental records (Klosowski, 2021). The Gramm-Leach Biley Act (GBLA) requires financial institutions to explain their information-sharing practices to their customers and to safeguard sensitive data (Kranz, 2021).

The European Union (EU) created legislation in 1995 in regard to privacy with Directive 95/46/EC on the protection of individuals with regard to processing of personal data and on the free movement of such data (Lord, 2018). The data protection directive is binding within the member states of the EU and regulates how personal data is collected and processed in the European Union. The Directive is built on seven principles including: notice (individuals should be notified when their personal data is collected), purpose (user of personal data should be limited to the express purpose for which it was collected), consent (individual consent should be required before personal data is shared with other parties), security (collected data should be secured against abuse or compromise), disclosure (data collectors should inform individuals when their personal data is being collected), access (individuals should have the ability to access their personal data and correct any inaccuracies), and accountability (individuals should have a means to hold data collectors accountable to the previous six principles) (Lord, 2018).

The European Union's data protection laws have been viewed as the gold standard all over the world. In 2016, the EU adopted the General Data Protection Regulation (GDPR) which replaced the 1995 Data Protection Directive 95/46/EC (European Union, 2022). The GDPR is a legal framework that requires businesses to protect the personal data and privacy of the European Union (EU) citizens for transactions that occur within EU member states. It covers all compliances that deal with the data of EU citizens, specifically banks, insurance companies, and other financial companies. GDPR's provisions require that any personal data exported outside of the EU is protected and regulated. For instance, if a company in the United States is selling services to someone in the EU, the U.S. company is required to comply with the GDPR because of European data being involved. Companies in the U.S. and abroad must invest large amounts of money to ensure that they are in compliance (Rossow, 2018).

There are two major protective rights of the GDPR. The first is the right of erasure, or the right to be forgotten. If a person does not want their data out there, they can request to have it removed or erased. The second is the right of portability. Opt-in and opt-out clauses must be very clear in regard to the precise terms. GDPR requires clear consent and addresses the following types of data: personally identifiable information, web-based data, health and genetic data, biometric data, racial or ethnic data, political opinion, and sexual orientation (Rossow, 2018).

Although there are clearly challenges in regard to data privacy for users of IoT devices (Emami-Naeini et al., 2017; Kanniappan et al., 2017; Charith et al., 2015; Ziegeldorf et al., 2014; Radomirovic, 2010), laws in the U.S. have not kept pace with advancements in IoT technology and do not provide adequate privacy protection. Instead of a singular data privacy law, the U.S. has a variety of privacy laws that each cover only a specific kind of data (Klosowski, 2021). In contrast, the GDPR in the EU offers much more comprehensive data privacy protection for EU citizens (Rossow, 2018). This means that for U.S. citizens, the burden of protecting personal data privacy while using IoT devices falls to the user. This often requires a solid understanding of the data collection practices and policies of organizations that provide IoT devices, as well as the privacy features and settings available on those devices so that they can be set to match the user's privacy preferences.

Understanding Privacy Concerns

While many individuals are concerned with data privacy, these concerns do not always impact individual's behaviors in terms of continued use of IoT devices and data sharing activities. For example, Zheng et al. (2018) conducted a study of smart home owners in the U.S. about their long-term experiences with using IoT devices and found that convenience and connectedness were the most frequently cited reasons for disregarding concerns about personal privacy risks when using IoT devices. It is important to understand user privacy concerns as well as other factors that may mitigate or influence IoT device use and data sharing behavior despite privacy concerns.

Some studies of IoT devices have examined different factors that can impact individuals' willingness to share information, based on measures of comfort with data collection. Emami-Naeini et al. (2017) surveyed 1,007 participants to determine individuals' privacy preferences. The study revealed eight factors that can influence individuals' privacy preferences, including: the type of data collected, the location where the data is collected, who benefits from the data collection, the device that collects the data, the purpose of data collection, the retention time, whether the data is shared, and whether additional information could be inferred from the data collected. Bilogrevic et al. (2016) found that comfort levels associated with sharing data are highly dependent on specific types of data and the sharing context of that data (e.g. search engines, social networks, or online shopping sites). Lin et al. (2012) evaluated individuals' perceptions of requests to access privacy-sensitive resources on mobile devices. The researchers found that both individual expectations of what an app does and the purpose for which an app requests access to sensitive information impact their privacy decisions.

Ziegeldorf et al. (2014) developed a three-fold definition of privacy as it relates to IoT. First, users must be aware of privacy risks imposed by smart things and services. Second, individuals need to be able to have control over the collection process of personal information from IoT devices. Lastly, users must be aware that subsequent use and dissemination of personal information being collected from IoT devices is sometimes out of the user's control sphere. This definition of privacy for IoT would provide great guidance for future laws in the U.S. and worldwide. However, it is unclear at this point if users of IoT devices today meet any of these criteria. This study addresses this problem by exploring privacy concerns of IoT users and the impact of perceived benefits on willingness to allow personal data collection.

Purpose of the study

The purpose of this study was to measure the privacy concerns of users of Internet-connected devices including smartphones and other Internet of Things (IoT) devices. Additionally, the study examines whether perceived benefits to allowing data to be collected via devices impacts the user's willingness to sacrifice data privacy. Examples of perceived benefits include providing a better user experience for the app or service, providing customized content that is tailored to the user within the app or service, and notifying the user about potential health issues or security issues based on data collection that could help to prevent issues or catch them early. The following research questions were explored:

RQ1: What are the privacy concerns of users of Internet-connected devices?

RQ2: How willing are users to disregard their data privacy concerns in order to receive other benefits (provide a better user experience, receive customized content, prevent a major health issue, prevent a life-threatening security issue)?

RQ3: How do concerns about data privacy impact users' intentions to change behavior in regard to protecting privacy?

Methodology

This quantitative study was conducted using survey research (Fowler, 2013). For data collection, an electronic survey consisting of 42 questions was used. The majority of questions were closed-ended but there were four open-ended questions included as well. The sample (n=353) for the study includes adults 18 and older who own and have used at least one Internet enabled IoT device.

Participants were first asked some general demographic data including age group, gender, occupation, and whether they work in a technology-related field. Next, participants were asked a series of questions to determine the types and amount of personal data that they potentially share. They were asked whether they have accounts for several popular social media platforms and whether they actively use each. The social media platforms included were Facebook, YouTube, Instagram, Twitter, Snapchat, TikTok, Reddit, and LinkedIn. Another set of questions asked about the users' comfort level with apps and devices collecting data in different situations, both in general and if specific benefits were provided based on the data sharing. The benefits specifically addressed included providing a better user experience for the app or service, providing customized content that is tailored to the user within the app or service, and notifying the user about potential health issues or security issues. Participants were asked whether they plan to change any behavior to help further protect their privacy in regard to data collection on devices, and a series of questions asking about their prior experience with data privacy violations and their intention to disclose personal information via devices within the next year (adapted from Xu et al., 2012).

Measuring Privacy Concern

To measure the participants' privacy concerns regarding Internet-enabled devices and their associated mobile apps, we used the Mobile Users' Information Privacy Scale (MUIPC). MUIPC was developed by Xu et al. (2012) and was partially based on the Concern for Information Privacy (CFIP) scale developed by Smith et al. (1996) which measured concern about organizational privacy. MUIPC was also partially based on the Internet User's Information Privacy (IUIPC) scale, developed by Malhotra et al. (2004) to adapt CFIP for online data privacy concerns (Malhotra et al., 2004; Smith et al., 1996; Xu et al., 2012). MUIPC was specifically developed to address the concerns of mobile users in regard to information privacy in regard to both mobile apps and devices (Xu et al., 2012). However, MUIPC has been extended to address Internet-enabled devices, commonly referred to as the Internet of Things (Foltz & Foltz, 2020; Foltz & Foltz, 2021; Pinchot & Cellante, 2021), which makes it appropriate for this study.

MUIPC is a 9-item scale where each item is measured on a five-point Likert scale ranging from "Strongly Disagree" = 1 to "Strongly Agree" = 5. The scale measures three distinct dimensions of privacy concern through three subscales: perceived surveillance, perceived intrusion, and secondary use of personal information (Xu et al., 2012). Surveillance has been defined as any collection or processing of personal data in order to influence or manage the individuals from whom the data has been collected (Lyon, 2001) and can include watching, listening to, or recording conversations or activities of individuals (Solove, 2006). Perceived intrusion refers to the concept of having more personal information shared about oneself than an individual is comfortable with having shared (Xu et al., 2012) and has been defined as "invasive acts that disturb one's tranquility or solitude" (Solove, 2006, p. 491). Secondary use of information refers to an individual's concern that personal information will be used in an undisclosed or unexpected way, without getting authorization from the individual (Smith et al., 1996; Xu et al., 2012). The MUIPC scale has been tested for internal consistency, and scores highly with a Cronbach alpha coefficient above .7 reported for all three dimensions that make up the total scale (Xu et al., 2012; Degirmenci et al., 2013). Table 1 shows the items that were adapted from the MUIPC scale and used in this study.

Table 1: Survey Items from MUIPC Scale (adapted from Xu et al., 2012)

Perceived Surveillance (SURV)
(1) I believe that the location of my Internet-enabled device is monitored at least part of the time. (2) I am concerned that Internet-enabled devices are collecting too much information about me. (3) I am concerned that Internet-enabled devices may monitor my activities.
Perceived Intrusion (INTR)
(4) I feel that as a result of my using Internet-enabled devices, others know about me more than I am comfortable with. (5) I believe that as a result of my using Internet-enabled devices, information about me that I consider private is now more readily available to others than I would want. (6) I feel that as a result of my using Internet-enabled devices, information about me is out there that, if used, will invade my privacy.
Secondary Use of Personal Information (SUSE)
(7) I am concerned that Internet-enabled devices may use my personal information for other purposes without notifying me or getting my authorization. (8) When I give personal information to use Internet-enabled devices, I am concerned that the device may use my information for other purposes. (9) I am concerned that Internet-enabled devices may share my personal information with other entities without getting my authorization.

Sample

The sample for this research study was obtained through Amazon Mechanical Turk (MTurk). MTurk is a crowdsourcing tool that allows access to a pool of participants that meet specific inclusion criteria who are willing to participate in surveys for compensation. MTurk has been used extensively by academic researchers for survey research and has been found to be largely representative of the entire U.S. population (Lovett, 2018; Redmiles et al., 2019). The researcher chooses the compensation amount to offer for participation. For surveys that are short in length (approximately 5-9 minutes to take), the compensation amount offered is typically between $.10 and $.50 (Lovett, 2018). This survey had an average completion time of 6 minutes and provided compensation for respondents within the recommended range. The survey used in this study was created in Question Pro and posted on Amazon Mechanical Turk targeting 350 responses. Data was collected in May 2022 after receiving approval from the university's Institutional Review Board. A total of 384 people started the survey, but 353 (n=353) participants submitted complete surveys, which is a response rate of 92%.

Results

The survey asked a series of questions that would help understand the demographics, social media use, and device usage of the participants. Half of the participants were within the 25-34 age group with nearly a quarter of the respondents within the 35-44 age group. Table 2 provides the frequency distribution of all participants and their respective age groups. The gender breakdown of the participants was 40.06% female and 59.94% male. The majority of participants, 91.62%, indicated that they work in a technology-related field, while 8.38% do not.

Table 2: Age Distribution

Age Group	Percentage
18-24	4.00%
25-34	50.00%
35-44	24.29%
45-54	16.29%
55-64	5.14%
Above 64	0.29%

The survey continued by asking respondents about their membership and active usage of social media platforms as well as the IoT devices that they use. In these questions, participants were permitted to select more than one response for each question. Table 3 provides the breakdown of common social media platforms, the percentage of respondents who have a membership with those platforms, and a percentage of participants that are actively using them. As expected, most platforms have a reduced percentage of active users in comparison to their membership. An interesting point is that all the respondents who stated they had a membership to YouTube or Twitter also stated that they are actively using it. The remaining social media platforms showed a membership versus active usage reduction between .85% and 6.24%.

Table 3: Social Media Memberships vs Active Use

Social Media Platform	Memberships	Actively Used
Instagram	83.85%	79.89%
YouTube	72.24%	72.24%
Facebook	74.79%	70.54%
Twitter	52.97%	52.97%
Snapchat	33.99%	33.14%
TikTok	31.16%	30.31%
Reddit	20.96%	17.85%
LinkedIn	21.25%	15.01%
Other	0.00%	0.00%

Table 4 provides a breakdown of devices used by the participants. The most widely used device was the laptop computer with 71.10% of the respondents using it. More than 50% of the participants also indicated that they use devices such as smart phones, TVs, and desktop computers.

Table 4: Distribution of Devices Used

Devices Used	Percentage
Laptop computer	71.10%
Smart phone	66.86%
Desktop computer	60.62%
TV	54.39%
Digital tablet (e.g. iPad)	34.56%
Smart watch	32.01%
Personal digital assistant (PDA)	30.88%
Gaming console	22.10%
Health-related tracker or device	20.40%
Home assistant (e.g. Amazon Echo/Alexa, Google Home)	16.15%
Kitchen appliance	15.86%
Streaming device (e.g. Roku, AppleTV)	14.45%
Smart glasses	12.46%
Smart thermostat	12.18%
Smart doorbell	11.90%
Smart garage door	9.92%
Smart car	8.50%

Addressing RQ1

To understand the privacy concerns of users of Internet-enabled devices, a further analysis using the MUIPC scale was conducted by creating an index variable called PRIVACY_CONCERN, which added the values together for the questions on the subscales SURV, INTR, and SUSE. The PRIVACY_CONCERN score could range from a minimum of 3 to a maximum of 45, since each of the nine criteria is scored from "Strongly Agree" = 1 to "Strongly Disagree" = 5. Therefore, a lower PRIVACY_CONCERN score indicates high concern while a higher score indicates low concern. The scores were categorized as either High Privacy Concern (PRIVACY_CONCERN score of 24 or less) or Low Privacy Concern (PRIVACY_CONCERN score from 25 to 45). Scores ranged from 6 to 39 with 87.22% in the High Privacy Concern category and 12.78% in the Low Privacy Concern category. This shows that there was clearly a high level of concern in regard to privacy for this sample. The scale showed good internal consistency (Cronbach's a=.84).

PRIVACY_CONCERN was tested using Chi-square against a number of variables including age, gender, and actively using various social media platforms. A statistically significant relationship (chi square=0.068, *df*=1, p=.004) was found between PRIVACY_CONCERN and active use of Facebook. A second statistically significant relationship (chi square=15.69, *df*=1, p=.000) was found between PRIVACY_CONCERN and active use of Instagram. As the level of Facebook and Instagram increases, the level of privacy concern also increases. There was notably no significant relationship between privacy concern and age or gender. A full analysis of these variables is provided in Table 5.

Table 5: Statistical Significance with PRIVACY_CONCERN

Variable	Chi-Square Value	Degrees of Freedom	p-value (* indicates statistical significance)
Instagram	15.69	1	0.000*
Facebook	0.068	1	0.004*
Reddit	4.299	1	0.038*
Twitter	1.022	1	0.312
YouTube	0.798	1	0.372
Snapchat	0.5	1	0.48
Gender	0.414	1	0.52
LinkedIn	0.309	1	0.578
TikTok	0.223	1	0.637
Age	2.208	5	0.82

Addressing RQ2

The researchers wanted to understand how likely individuals are to disregard their data privacy concerns in order to receive other benefits. In order to answer this question, the survey asked if the participants were comfortable with Internet-enabled devices collecting information about them. Of the participants, 89.86% stated they were comfortable with letting these devices collect information while 10.14% were not. The survey continued to assess if participants would be comfortable allowing these devices to collect information from them if it could help prevent a health-related problem. In this case, 88.89% responded they were comfortable sharing their information while 10.12% were not. The participants were also asked if they were comfortable with Internet-enabled devices collecting information about them if it could help prevent a life-threatening security issue and 85.19% of the participants were okay with their data being collected while 14.81% were not comfortable. There was little variation in the responses to these three questions, indicating that the sample overall was very comfortable with allowing Internet-enabled devices to collect data about them, regardless of health or security-related benefits. In fact, the responses for the questions asking about these benefits were slightly lower than the responses for the sample's overall comfort level with data collection.

As a follow up, two additional questions asked participants to respond to the statement that they were comfortable with enabling apps to use technology to improve their user experience or to provide customized content. Examples of this technology included sharing facial identification and microphone audio from your Internet-enabled device. These questions were measured on a five-point Likert scale ranging from "Strongly Disagree" = 1 to "Strongly Agree" = 5. The majority of respondents, 75.66%, were comfortable allowing Internet-enabled devices to collect data in order to receive an improved user experience. Likewise, the majority of respondents, 74.79%, were comfortable allowing Internet-enabled devices to collect data in order to receive customized content. A full analysis of these variables is provided in Table 6.

Table 6: Level of Comfort with Data Collection When Receiving Benefits

Comfort Scenarios	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
Comfort When Improving User Experience	28.41%	47.25%	17.10%	4.64%	2.61%
Comfort When Receiving Customized Content	29.18%	45.61%	17.28%	4.82%	3.12%

To get a better sense of how participants' comfort level with personal data collection was impacted by privacy concern, the researchers tested each of these comfort variables against PRIVACY_CONCERN. The results can be found in Table 7. A statistically significant relationship (chi square=31.376, *df*=4, p=.000) was found between PRIVACY_CONCERN and Comfort When Improving User Experience. Another statistically significant relationship (chi square=30.057, df=4, p=.000) was found between PRIVACY_CONCERN and Comfort When Receiving Customized Content. Note that the PRIVACY_CONCERN variable is inverted as described above, so higher values indicate lower levels of concern. Therefore, these statistically significant relationships indicate that as privacy concern decreases, participants' comfort level in allowing personal data collection in order to improve the user experience or receive customized content increases.

Table 7: Impact of PRIVACY_CONCERN on Comfort Levels Regarding Data Collection

Variable	Chi-square Value	Degrees of Freedom	p-value (* indicates statistical significance)
Comfort When Receiving Customized Content	30.057	4	0.000*
Comfort When Improving User Experience	31.376	4	0.000*
Comfort When Preventing Threat	1.100	1	0.294
Comfort When Preventing Health Issue	.795	1	0.372

Addressing RQ3

The researchers wanted to understand how privacy concerns impact users' intentions to change behavior in regard to protecting privacy. One of the concluding survey questions asked if the participants planned to make any changes to their behavior in regard to data collection on their devices. Approximately 67% of the respondents stated they would make some minor or major changes to their behavior with how they use Internet-enabled devices to improve privacy, while 33% stated they would not anticipate making any changes. The full breakdown of these can be found below in Table 8.

Table 8: Intention to Change Behavior to Protect Privacy

Responses for Change Behavior to Protect Privacy	Percentage
No, I have the level of protection I need	17.09%
No, but I do not feel adequately protected	15.95%
Yes, I plan to make minor changes to how I use the device/technology in the future	49.57%
Yes, I plan to make significant changes to how I use the device/technology in the future	17.09%
Other	0.28%

A Chi-square test was conducted on PRIVACY_CONCERN with the Intention to Change Behavior, the analysis did not produce a statistically significant relationship with a resulting chi square=3.841, df=4, and p=.428.

Discussion

A primary focus of this study was to assess IoT device users' concerns about privacy. The researchers measured privacy concern via the MUIPC scale (Xu et al., 2012). The MUIPC scale is made up of three core areas related to privacy that include perceived surveillance, perceived intrusion, and secondary use of personal information which are summed up into a privacy concern index. In this sample, the majority of participants, 87.2%, showed a high degree of privacy concern.

The study did not find a statistical significance between the key descriptive variables like age and gender with the participants' overall privacy concern. Two social media platforms, Facebook and Instagram, were found to have statistically significant relationships with privacy concern. While it was somewhat surprising to find that these social media platforms were the only ones that were statistically significant, it can be explained as Facebook and Instagram are two of the top three actively used platforms for the sample. This is consistent with other findings in the literature, as Mobalaji (2021) found that although users of Facebook and Instagram are well aware of the privacy risks associated with the two platforms, users still continue to use and share personal information on them. Mobalajj (2021) concludes that the disregard to privacy risks can only be attributed to some gratification or benefit that is received as a trade-off to privacy risks associated with the platform.

The researchers sought to understand the willingness of participants to disregard their data privacy concerns in regard to IoT devices if they received potential benefits such as a better user experience, customized content, preventing a major health issue, and preventing a life-threatening security issue. When asked about comfort level when receiving the benefit of preventing a major health issue, 88.89% responded that they would be comfortable having IoT data collected. Similarly, when asked about comfort level when receiving the benefit of preventing a life-threatening security issue, 85.19% responded that they would be comfortable having IoT data collected. However, the resulting comfort level was lower for the benefit of improving user experience, 75.66%, and the benefit of receiving customized content, 74.79%. These results are in line with Mobolaji's (2021) view that some gratification or perceived benefit can result in individuals disregarding their privacy concerns. One example was presented by Veljanovski (2022) detailing how an Apple Watch saved a man's life as a bike rider became unconscious and fell from his bike. The Apple Watch notified emergency response not only of his "hard fall" but also of his location. When police arrived, they found the individual lying next to his bike and bleeding profusely from the head. The man was provided with help and lived. Other examples include smart watches calling emergency response teams or emergency contacts of potential heart attack victims. It is very understandable that individuals would disregard any privacy concerns in order to receive help in such dire situations.

The researchers were interested in the relationship between privacy concerns for data collection via IoT devices and intentions to change behavior in regard to protecting privacy in the future. While the study did not find a statistical significance between the participants' privacy concern and their intentions to change behavior, it is still important to note that 66.66% of the participants stated they would make a change in their behavior with 49.57% minor changes and 17.09% major changes. These results were important because the first step to any change is awareness and a willingness to change one's behavior. Future research can address not only the willingness to change but what specific changes have been implemented to protect one's privacy. A study by Bacchi (2019) of 10,000 participants illustrated that about half of the respondents had become more cautious about sharing personal information online and that 30% had incorporated digital tools to limit online tracking. Making these changes in behavior does not always mean abandoning social media platforms or devices, but instead, may change how people use them. An example is more carefully vetting a photo before it is posted online or double-checking privacy settings before posting content.

Conclusion

There are clear data privacy challenges for users of IoT devices (Emami-Naeini et al., 2017; Kanniappan et al., 2017; Charith et al., 2015; Ziegeldorf et al., 2014; Radomirovic, 2010), and though IoT privacy frameworks have been proposed by researchers (Ziegeldorf et al., 2014), laws in the U.S. do not currently provide adequate privacy protection for IoT users. Therefore, in the U.S., the burden of understanding laws, policies, and device settings related to IoT data privacy falls on the user. Because of this, it is important to understand the privacy concerns and behaviors of IoT users.

This study examined the privacy concerns of users of Internet-connected devices, such as IoT devices. The majority of participants, 87.22%, fell into the High Privacy Concern category, indicating that privacy is a concern for these IoT users. This finding was further illuminated by statistically significant relationships found between privacy concern and active use of Facebook and Instagram. As the level of Facebook and Instagram use increases, privacy concern also increases. This clearly shows that participants who use social media platforms understand that there is a risk in data sharing on those platforms.

Further, this study explored the willingness of IoT users to sacrifice data privacy if receiving another potential benefit such as a better user experience, customized content, or more serious benefits such as preventing a major health issue or preventing a life-threating security issue. Overall, 85.19% of participants responded that they were comfortable with Internet-enabled devices collecting information about them (such as sensor data, camera/video/facial identification, and audio). When asked whether they were comfortable with Internet-enabled devices collecting information about them in order to receive a specific benefit, responses were as follows: 88.89% were comfortable if data collection could help prevent a major health-related issue, 85.19% were comfortable if data collection could help prevent a life-threatening situation, 75.66% were comfortable if data collection could provide an improved user experience for the device, and 74.79% were comfortable if data collection could provide customized content for them. These results were all very consistent, with the majority of participants indicating high comfort levels with data collection for all of the reasons identified. While the comfort level percentages for health and safety-related benefits were higher than the user experience and personalization benefits, two statistically significant relationships were found with privacy concern: comfort level with data collection for an improved user experience (chi square=217.071, *df*=112, p=.000) and comfort level with data collection for customized content (chi square=213.458, df=116, p=.000). Note that privacy concern was coded inversely so a high score indicated low concern and a low score indicated high concern. This means that as the participants' privacy concern increases, their comfort level in allowing data collection in order to receive an improved user experience or receive customized content decreases. It is clear that IoT users do value perceived benefits provided as a tradeoff to offset their privacy concerns regarding data collection on these devices.

This is consistent with Mobolaji's (2021) finding that perceived benefits can result in individuals disregarding their privacy concerns.

Finally, this study looked at whether IoT users' privacy concern impact users' intentions to change behavior in regard to protecting data privacy. A majority of participants, 66.66%, indicated that they plan to change their device usage behavior in the future in order to better protect their data privacy while using IoT devices. Of the 66.66%, 17.09% indicated that they planned major changes to their device usage behavior and 49.57% indicated that they planned minor changes to their device usage behavior.

A potential limitation of this study was the use of Amazon Mechanical Turk to recruit participants. While MTurk has been shown to be largely representative of the entire U.S. population (Lovett, 2018; Redmiles et al., 2019), there is a possibility that the participants skew toward the more tech-savvy. In this sample, 91.62% of participants reported that they work in a technology-related field. This type of work could potentially mean that users in this sample are more aware of the data privacy risks of using IoT devices than other users.

Future studies should expand the participant base and focus on understanding more clearly the perceived benefits that IoT users value enough to risk their data privacy. The results of this study add to the body of knowledge in this regard but only begin to address the complex issue that users face in managing privacy concerns while still taking advantage of some of the key benefits of IoT devices such as connectedness and convenience.

References

Bacchi, U. (2019). *Privacy concerns pushing people to change online behavior, poll shows.* Reuters. https://www.reuters.com/article/us-global-tech-privacy/privacy-concerns-pushing-people-to-change-online-behavior-poll-shows-idUSKBN1Y803D

Belanger, F., & Crossler, R.E. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly, 35*(4), 1017-1041.

Charith, P., Ranjan, R., Wang, L., Khan, S., & Zomaya, A. (2015). Big data privacy in the internet of things era. *IT Professional, 17*(3), 32-39.

Cirne, A., Sousa, P.R., Resende, J.S., & Antunes, L. (2022). IoT security certifications: Challenges and potential approaches. *Computers & Security, 116*, 1-28.

Degirmenci, K., Guhr, N., & Breitner, M. (2013). Mobile applications and access to personal information: A discussion of user's privacy concerns. *Proceedings of the 34th International Conference on Information Systems*, 1-21.

Dotzer, F. (2006). Privacy issues in vehicular and ad hot networks. *Lecture Notes in Computer Science,* Vol. 3856, 197-209.

Emami-Naeini, P., Agarwal, Y., Cranor, L.F., & Hibshi, H. (2020). Ask the experts: What should be on an IoT privacy and security label? *2020 IEEE Symposium on Security and Privacy*, 447-464.

Emami-Naeini, P., Bhagavatula, S., Habib, H., Degeling, M., Bauer, L., Cranor, L, & Sadeh, N. (2017). Privacy expectations and preferences in an IoT world. *Symposium on Usable Privacy and Security (SOUPS) 2017*, Santa Clara, California.

European Union. (2022). *The history of the General Data Protection Regulation.* European Data Protection Supervisor. https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en

Foltz, C.B., & Foltz, L. (2020). Mobile user's information privacy concerns instrument and IoT. *Information & Computer Security, 28*(3), 359-371.

Foltz, C.B., & Foltz, L. (2021). MUIPC and intent to change IoT privacy settings. *The Journal of Computing Sciences in Colleges, 36*(7), 27-38.

Fowler, F.J. (2013). *Survey research methods (5th edition).* Sage.

FTC (2022). *Children's online privacy protection rule (COPPA).* Federal Trade Commission. https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa

Hammouchi, H., Cherqi, O., Mezzour, G., Ghogho, M., & El Koutbi, M. (2019). Digging deeper into data breaches: An exploratory data analysis of hacking breaches over time. *International Symposium on Machine Learning and Big Data Analytics for Cybersecurity and Privacy*, 1004-1009.

Jovanovic, B. (2022). *Internet of things statistics for 2022 – Taking things apart.* DataProt. https://dataprot.net/statistics/iot-statistics/

Kanniappan, J., & Rajendiran, B. (2017). Privacy in the internet of things. *The Internet of Things in the Modern Business Environment.* Western Illinois University.

Klosowski, T. (2021). *The state of consumer data privacy laws in the US (and why it matters).* New York Times. https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/

Kranz, G. (2021). *Gramm-Leach-Biley Act (GLBA).* Tech Target. https://www.techtarget.com/searchcio/definition/Gramm-Leach-Bliley-Act

Kuznetsov, M., Novikova, E., Kotenko, I., & Doynikova, E. (2022). Privacy policies of IoT devices: Collection and analysis. *Sensors, 22*(1838), 1-23.

Lin, J., Amini, Sh., Hong, J., Sadeh., N., Lindqvist, J., & Zhang, J. (2012). Expectation and purpose: understanding users' mental models of mobile app privacy through crowdsourcing. *Proceeding of the 2012 ACM Conference on Ubiquitous Computing*. ACM, 501-510.

Lord, N. (2018). *What is the data protection directive? The predecessor to the GDPR.* Digital Guardian. https://digitalguardian.com/blog/what-data-protection-directive-predecessor-gdpr

Lovett, M., Bajaba, S., Lovett, M., & Simmering, M. (2018). Data quality from crowdsourced surveys: A mixed method inquiry into perceptions of Amazon's Mechanical Turk Masters. *Applied Psychology, 67*(2), 339-366.

Lyon, D. (2001). *Surveillance society: Monitoring everyday life.* Open University Press.

Malhotra, N.K., Kim, S.S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research, 15*(4), 336-355.

Mobolaji, A. (2021). Privacy concerns, self-disclosure and social media users' online behaviour. 10.13140/RG.2.2.20891.39202.

Pinchot, J., & Cellante, D. (2021). Privacy concerns and data sharing habits of personal fitness information collected via activity trackers. *Journal of Information Systems Applied Research, 14*(2), 4-13.

Pinchot, J., & Paullet, K. (2014). Use of preventative measures to protect data privacy and mobile devices. *Journal of Information Systems Applied Research*, 8(2), 44-50.

U.S. DOJ. (2022). *United States Department of Justice, Privacy Act of 1974*. https://www.justice.gov/opcl/privacy-act-1974

Patel, M., Shangkuan, J., Thomas, C. (2017). *What's new with the internet of things?* McKinsey & Company. Retrieved from https://www.mckinsey.com/industries/semiconductors/our-insights/whats-new-with-the-internet-of-things

Radomirovic. S. (2010). Towards a model for security and privacy in the Internet of Things. *1st International Workshop on the Security of the Internet of Things*, Tokyo, Japan.

Redmiles, E.M., Kross, S., & Mazurek, M.L. (2019). How well do my results generalize? Comparing security and privacy survey results from MTurk, web, and telephone samples. *2019 IEEE Symposium on Security and Privacy*, 1326-1343.

Rossow, A. (2018). *The birth of DGPR: What is it and what you need to know.* Forbes Magazine.

Saleem, J., Hammoudeh, M., Raza, U., Adebisi, B., & Ande, R. (2018). IoT standardization: Challenges, perspectives, and solution. *Proceedings of the 2nd International Conference on Future Networks and Distributed Systems*, 1-9.

Smith, H.J., Milberg, J.S., & Burke, J.S. (1996). Information privacy: Measuring individual's concerns about organizational practices. *MIS Quarterly, 20*(2), 167-196.

Solove, D.J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review, 154*(3), 477-560.

Veljanovski, L. (2022). *Apple Watch saves man's life after he falls from electric bike.* Newsweek. https://www.newsweek.com/apple-watch-saves-mans-life-falls-electric-bike-california-tech-1675335

Weber, M., & Boban, M. (2016). Security challenges of the Internet of Things. *39th International Convention on Information and Communication Technology, Electronics, and Microelectronics*, 638-643.

Xu, H., Rossen, M.B., Gupta, S., & Carroll, J.M. (2012). Measuring mobile user's concerns for information privacy. *Thirty Third International Conference on Information Systems*, 1-16.

Zheng, S., Apthorpe, N., Chetty, M., & Feamster, N. (2018). User perceptions of smart home IoT privacy. *Proceedings of the ACM on Human-Computer Interaction, 2*, 1-20.

Ziegeldorf, J.H., Morchon, O, G., & Wehrle, K. (2014). Privacy in the internet of things: Threats and challenges. *Security and Communications Networks, 7*(12), 2728-2742.