Are Companies Responsible for Internet of Things (IoT) Data Privacy? A Survey of IoT User Perceptions

Karen Paullet
Robert Morris University
paullet@rmu.edu

Adnan A. Chawdhry
Pennsylvania Western University
Chawdhry_a@pennwest.edu

Jamie Pinchot
Robert Morris University
pinchot@rmu.edu

Abstract

This study addressed privacy concerns of Internet of Things (IoT) users, in relation to concerns about personal data collection. Data breaches continue to impact people who use online services such as web sites, mobile apps, and IoT devices. IoT devices, in particular, can often collect data via sensors without the user even being aware of all of the varied types of data being collected. Therefore, this study examined IoT users' data privacy concerns perceptions regarding the responsibilities of companies providing IoT devices and data collection services. A survey of 353 IoT users was conducted and found that participants had a high level of concern for data privacy and a high level of concern about ethical violations at companies that provide and collect data from IoT devices. The survey focused on the users experience across all IoT devices but did have one question to identify IoT devices they have used. The majority of participants had experienced a prior data privacy violation, and prior experience did impact their privacy concerns. However, prior experience did not impact participant's comfort level with allowing data collection, and participants also indicated that the benefits of sharing IoT data could outweigh the data privacy risks.

Keywords: data privacy, privacy, Internet of Things, mobile devices, ethics

1. INTRODUCTION

The Internet of Things (IoT) refers collectively to the many and varied types of devices that can connect to the Internet. These devices are often referred to as "smart" devices and can range from personal devices to smart home appliances and smart city devices. Personal IoT devices can include smart phones, smart watches, health and fitness trackers, and other wearables. Examples of home IoT devices include toasters, refrigerators, thermostats, light switches, video monitors, and doorbell cameras that can all be controlled via mobile apps or web sites because they are connected to the Internet. At the largest scale, smart city IoT devices can include smart traffic lights that sense and adjust to traffic patterns, surveillance cameras, and trackable bicycles and scooters (Haney et al., 2021; Rice & Bogdanov, 2019; Zheng et al., 2018).

While these smart devices can provide many conveniences for people, they also introduce some new threats in regard to data privacy. While most Internet users are aware of the data they are sharing online via web sites, mobile apps, and social media platforms, the data shared via IoT devices can be less obvious, and many users are not even aware that certain data is being collected. Non-technical users in particular may not understand a device's privacy and security implications (Rice & Bogdanov, 2019). Some examples of data collected by sensors on IoT devices that may impact personal privacy and safety include current location, past locations, and even most frequented locations. When traveling, sensors can determine changes in direction, speed, and acceleration. Health and fitness devices may include sensor data that tracks sensitive health information (Zheng et al., 2018).

Any personal data that is collected and stored can potentially be breached. IoT devices exacerbate the problem of data privacy by generating an exponentially increased amount of personal data, often without the knowledge of the user. Further, IoT devices currently face a number of security challenges and lack of regulation. Due to these issues, IoT devices present a serious threat to data privacy (Cirne et al., 2022; Foltz & Foltz, 2021; Rice & Bogdanov, 2019).

Because of the lack of regulation on IoT devices, and the continual development of new types of devices, it is important for users to be aware of the ways in which IoT data is collected and shared (Rice & Bogdanov, 2019). It is currently unclear where perceived responsibility for IoT data privacy lies.

Haney et al. (2021) conducted a study of smart home users and found that users assume some personal responsibility for data privacy but also assign responsibilities to manufacturers and government. Users may mistakenly believe that IoT manufacturers have taken precautions for data privacy. However, not all companies see online privacy as a corporate social responsibility. Pollach (2011) found that only a small proportion of information technology companies have implemented comprehensive privacy programs. Allen and Peloza (2015) found that despite its importance in a world of digital technologies, the concept of privacy is rarely addressed in research on corporate social responsibility. Further, Rice and Bogdanov (2019) found that methods companies typically use to describe their privacy practices, such as the privacy statement available on product websites, are largely ineffective in conveying information to users.

Because of this potential threat to data privacy that IoT devices present, it is important to understand IoT users' perceptions of data privacy, and their perceptions of the responsibilities of companies that provide IoT devices and collect data from them.

2. LITERATURE REVIEW

Personally Identifiable Information (PII), as defined by NIST (2017) is "information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth or mother's maiden name." PII is often the target of a data breach. For IoT users, PII could also include sensor data that could impact privacy, such as personal health information. It could also include sensor data that could impact personal safety, such as current location or location history. Because so much data is generated by IoT devices, a data breach could be a serious privacy threat for users.

Recent Data Breaches

Data breaches of sensitive information are on the rise. According to the Identity Theft Resource Centers 2021 Annual Data Breach Report, the overall number of data compromises is up more than 68% compared to 2020. The new record number of data compromises is 23% over the previous all-time high set in 2017. Additionally, the number of data events that involved sensitive information such as social security numbers increased to 83% from 80% in 2020 (ITRC, 2022). Other key findings in the report include:

- Ransomware-related data breaches have doubled in each of the past two years (2020, 2021). At the current rate, ransomware attacks will surpass phishing as the number one root cause of data compromises in 2022.
- There were more cyberattack-related data compromises (1,608) in 2021 than all data compromises in 2020 (1,108).
- Compromises increased from 2020 to 2021 in every primary sector but one, the military, where there were zero public breaches.
- The number of data breach notices that do not reveal the root cause of a compromise has grown by more than 190% since 2020.

Cyberattacks and security breaches continue to happen daily around the world. In the United States in 2022 below are a partial list of breaches:

- Crypto.com (Jan 17): targeted nearly 500 cryptocurrency wallets
- Red Cross (Jan): An attack on a third-party contractor had more than a half a million records compromised
- GiveSendGo (Feb): A political hacker stole then published the information of 90,000 people who donated money to protestors
- Flagstar Bank (June): The Michigan-based bank notified 1.5 million customers that hackers stole their social security numbers
- Marriott: Marriott International confirmed that hackers stole 202 gigabytes of sensitive data

It is important to mention that cyber-attacks worldwide are growing rapidly. Approximately 95% of cybersecurity breaches are caused by human error (World Economic Forum, 2020). The U.S. was the target of 46% of cyberattacks in 2020, more than double any other country (Lambert, 2021). Fifty-four percent of companies say their IT departments are not sophisticated enough to handle advanced cyberattacks (Sophos, 2021). Data breaches exposed 22 billion records in 2021 (Risk Based Security, 2022).

There has been a surge of interconnected devices known as IoT (Internet of Things). With this rapid growth of IoT enabled devices breaches are on the rise. The number of connected IoT devices as of September 2022 is 14.3 billion globally (Hasan, 2022). This is expected to grow to 75 billion by 2025. Approximately 84% of surveyed companies have reported an IoT security breach (Conosco, 2021). Ring, owned by Amazon had two separate incidents where user data was exposed to a third party. One where trackers were embedded into their Android application and the second due to an IoT security breach where cybercriminals hacked into the home monitoring systems of several families

According to Gartner, 40% of smart home appliances globally are being used for botnet attacks (Gartner, 2021). Research given to the FDA found that St. Jude Medical's implantable devices have vulnerabilities. If hackers were able to gain access they could deplete the battery or administer incorrect pacing shocks.

Consumer Privacy Concerns

SAS (2018) found that although consumers acknowledge their own responsibility for their personal data, 73% or participants believe that organizations are collecting their personal information without their knowledge. Fifty-eight percent of respondents said they do not trust organizations to keep their personal information secure while believing that 57% of companies do not try their best to protect consumers data. When it comes to industries that people trust most to protect their data, 46.5% of participants believe that health care and banking are the most secure. Social media was the least trusted, with only 14% of participants expressing the same confidence, followed by retail at 18%, energy companies at 21%, and government agencies at 29%.

Consumers' stated privacy preferences, as measured in surveys, can often differ from their actual behavior, as measured by consumers' online activity. This is referred to as the "privacy paradox". Research on the privacy paradox explains that consumers may judge privacy as important in surveys but continue to engage with websites and disclose information (Martin, 2019; Kokolakis, 2017; Strahilevitz et al., 2016; Norberg et al., 2007). The privacy paradox is important for businesses because the narrative defines the scope for corporate responsibility as quite narrow. Companies have little to no responsibility to identify or respect privacy expectations of consumers while online (Martin, 2019). So, in practice, consumers essentially must give up their right to privacy when they go online, use social media, or use a mobile app.

The privacy paradox suggests that consumers demonstrate their willingness to 'trade' the risk of privacy for the benefits of sharing information online. Consumers regularly exchange their privacy preferences for the benefits of discounts, better service, or social affiliation (Martin, 2019; Schumann et al., 2014; Xu et al., 2009; Hui et al., 2007). This exchange approach to privacy shows consumers as taking the risks and benefits of disclosing information into consideration when assessing privacy concerns. Consumers are willing to disclose for personalization and free services (Martin, 2019; Xu et al., 2009; Banerjee et al., 2008).

Consumer concerns about the security of their data continues to solidify as cyber-attacks continue to grow. Companies' information security practices are increasingly the subject of government scrutiny through the Federal Trade Commission (FTC), the Financial Industry Regulatory Authority (FINRA) and the Health Insurance Portability and Accountability Act (HIPPA). Additionally, the Securities and

Exchanges commission (SEC) has elevated the issue of cybersecurity to the level of the board of directors of public companies (Aguilar, 2014).

Consumer Attitudes Toward Data Breaches

Mayer et al. (2021) conducted a study on individuals' awareness, perceptions and responses to data breaches. The study found that 73% of participants experienced at least one breach and 5.36 breaches on average. An email address's likelihood of being exposed in a breach significantly correlated with the email account's age and utilization. Only 14% of participants attributed the cause of being affected by a breach to external factors such as hacking. Most participants rated their concern regarding breaches as low (56% slightly/somewhat concerned, 19% no concern). Breaches such as the release of their physical address or passwords raised more concern. Lastly, participants reported having already changed or being very likely to change their passwords and review their credit report and financial statements in response to over 50% of breaches.

A 2019 study conducted by the Pew Research Center in regard to privacy and personal data revealed that seven out of 10 Americans feel as if their data is less secure than it was five years prior to the study date. Roughly three out of 10 Americans have experienced some kind of data breach in the previous 12-month period and eight out of 10 believe they have control over their personal data. Lastly, only 6% of adults say they understand what companies do with the data collected (Pew Research Center, 2019).

3. PURPOSE

The purpose of this study was to explore the perceptions of users of Internet-connected devices in regard to data privacy responsibilities of the companies that collect data from these devices. Further, the study examines whether prior experience with a data privacy issue, such as involvement in a data breach, impacts those perceptions. The following research questions were addressed in the study:

RQ1: What are users' perceptions about the responsibilities of companies collecting user data from Internet-connected devices in regard to data privacy?

RQ2: How does prior experience with a data privacy issue impact users' data privacy concerns?

4. METHOD

This study used a survey research method (Fowler, 2013) and collected data via an electronic survey. The population for the study consisted of adults aged 18 and older who own and have used at least one Internet-connected device. There were 353 responses collected (n=353). The study was approved by the university's Institutional Review board (IRB).

The survey included questions addressing general demographic data: age group, gender, and whether the participant works in a technology-related field. The next set of questions addressed users' comfort level with companies collecting personal data from Internet-connected devices. Another set of questions addressed user concerns about whether allowing devices to collect personal data could lead to ethical violations at the company that collects the data. Questions specifically addressed whether users believe it is the responsibility of the company to protect the privacy of data collected from personal devices, and further asked about what specific responsibilities should be upheld, if any, on the part of the company collecting data. Participants were asked if they think that the safeguards put in place by companies to protect personal data privacy are adequate. Finally, participants were asked whether they had experienced any prior issues with data privacy related to Internet-connected devices (adapted from Xu et al., 2012), about the personal impact, if any, of allowing devices to collect their personal data, and whether they planned to change any behavior in regard to sharing data from devices in the future.

Measuring Privacy Concern

The Mobile Users' Information Privacy Scale (MUIPC) was used to measure the participants' privacy concerns regarding Internet-connected devices. MUIPC was developed by Xu et al. (2012) and was partially based on both the Concern for Information Privacy (CFIP) scale (Smith et al., 1996) and the Internet User's Information Privacy (IUIPC) scale (Malhotra et al., 2004). Malhotra et al. (2004) adapted CFIP for the online environment in developing IUIPC (Malhotra et al., 2004; Smith et al., 1996; Xu et al., 2012). MUIPC further developed the questions to apply to mobile device and app users in regard to data privacy (Xu et al., 2012). MUIPC has been used to address Internet-connected devices, commonly referred to as the Internet of Things, as they fall into the category of mobile devices (Foltz & Foltz, 2020; Foltz & Foltz, 2021;

Pinchot & Cellante, 2021). This makes the use of MUIPC appropriate for this study.

MUIPC is a scale consisting of 9-items, each of which is measured on a five-point Likert scale ranging from "Strongly Disagree" = 1 to "Strongly Agree" = 5. The scale measures three dimensions of mobile data privacy concern: perceived surveillance, perceived intrusion, and secondary use of personal information (Xu et al., 2012). Surveillance includes any collection or processing of personal data in order to influence the individuals from whom the data has been collected (Lyon, 2001). Methods of data collection can include watching, listening to, or recording individuals' actions or conversations (Solove, 2006). Perceived intrusion is having more personal information shared about oneself than an individual is comfortable with having shared (Xu et al., 2012). Finally, secondary use of information refers to the concern that personal data will be used without permission in an undisclosed or unexpected way (Smith et al., 1996; Xu et al., 2012). The MUIPC scale has been tested for internal consistency, with a Cronbach alpha coefficient above .7 (Xu et al., 2012; Degirmenci et al., 2013), which is a high score.

Sample

This study utilized Amazon Mechanical Turk (MTurk) for sample selection and distribution of the electronic survey. MTurk is a crowdsourcing tool that allows access to participants that meet specific inclusion criteria who are willing to participate in surveys for compensation. MTurk has been found to be largely representative of the entire U.S. population, and is used widely in academic research (Lovett, 2018; Redmiles et al., 2019). In MTurk, compensation is offered to all participants; the researcher chooses the amount of compensation to offer, and the number of respondents desired. For short surveys (approximately 5-9 minutes), the compensation amount offered is typically between $.10 and $.50 (Lovett, 2018). This survey had an average completion time of 6 minutes. Compensation was provided within the recommended range.

Question Pro was used to create the electronic survey and record responses. The electronic survey was posted on MTurk in May 2022 targeting 350 responses. A total of 384 people began the survey, and 353 people submitted complete surveys (n=353). The high response rate, 92%, is typical of using the MTurk platform.

5. RESULTS

The survey began with questions to evaluate background demographics. Of the participants, half were within the 25-34 age group while nearly a quarter of the respondents were within the 35-44 age group. Table 1 provides the frequency distribution of participants' ages. Additionally, the gender breakdown of the participants was 40.06% female and 59.94% male. The majority of the participants, 91.2%, stated they work in a technology-related field while 8.38% stated they do not.

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%

Table 1: Age Distribution

Addressing RQ1

The first research question focused on the users' perceptions on a company's responsibility when collecting user data. Of the participants, 91.6% stated they have a concern that companies collecting data from devices can lead to an ethical violation. A breakdown of their responses can be found in Table 2. Additionally, 95.3% of the participants felt that it is the company's responsibility to protect the data it collects, while 4.7% did not. Subsequent to this question, participants were asked if the safeguards put in place by organizations were adequate and only 85.5% stated yes while 14.5% stated no, they are not adequate.

Concern for Company Ethical Violations	Response
Yes - I have already experienced an ethical violation related to collection of my data	68.1%
Yes - I am concerned that I will experience an ethical violation related to collection of my data	23.5%
No	8.4%
Total	100%

Table 2: Ethical Violations

Participants were asked an open-ended question about the ethical responsibilities of companies when collecting user data. A few notable

statements written by participants are:

- *Now more than ever, you should know how big data is collected and understand some of the impacts of big data in your personal life.*
- *Big data helps us save money on what we eat too with loyalty card schemes, cashback sites and money-off coupons all designed to reduce the weekly food bill. . A staggering 90% of the world's data has been created in the past two years.*
- *Improving health care and generating scientific knowledge create an ethical imperative for the sharing of data. Sharing data, if done appropriately, can help to address health inequalities, and therefore creates an obligation to participants who have consented to use the data well and efficiently.*
- *Smart business leaders and key stakeholders are making it a priority to implement corporate responsibility programs (CSR). A CSR program can support worthy causes, improve employee morale, and create a company culture of integrity.*
- *The ethical responsibilities that companies have to customers revolve around collecting only necessary data from customers properly protecting customer data.*

Addressing RQ2

The second research question evaluates users' prior experiences with data privacy issues and whether those experiences impact their data privacy concerns.

To measure user's privacy concerns, the MUIPC scale was used to create an index PRIVACY CONCERN variable. The score for PRIVACY CONCERN could range from a minimum of 3 to a maximum of 45. Since the scale questions used a 5-point Likert scale scored from "Strongly Agree" = 1 to "Strongly Disagree" = 5, the scale was inverted, with a low score indicating a high level of concern, and a high score indicating a low level of concern. The scores were then categorized as either High Privacy Concern (24 or less) or Low Privacy Concern (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 data privacy for this sample. The scale showed good internal consistency (Cronbach's a=.84).

The participants were asked about their overall impact if they allowed devices to collect data about them. Of the participants, 83.4% stated it had some impact (positive or negative) while 13.1% stated it had no impact on their lives. The breakdown of responses is available in Table 3.

Collecting Data Impact	Percent
It had a positive impact on my life	53.80%
It had a negative impact on my life	29.60%
It had no impact on my life	13.10%
I do not allow data collection on my devices.	3.40%
Total	100%

Table 3: Impact of Prior Data Collection

To get a better sense of the participants privacy concerns, the researchers tested two variables (PRIOR EXPERIENCE and ETHICAL VIOLATIONS CONCERN) against both PRIVACY CONCERN and COMFORT WITH DATA COLLECTION. Statistical significance (p-value of less than or equal to 0.05) was found in all cases. The results of this analysis can be found in Tables 5 and 6.

Variable	Chi-square Value	df	p-value (* indicates statistical significance)
Prior Privacy Violations	405.21	6	.000*
Ethical Violations Concern	13.421	2	.001*

Table 4: Privacy Concern Chi-Square

Table 4 shows that there is a strong statistically significant relationship (p<.000) between PRIOR PRIVACY VIOLATIONS and PRIVACY CONCERN. This indicates that the more prior experiences a participant had with privacy violations such as data breaches or ethical violations, the higher their level of privacy concern.

Additionally, there is a strong statistically significant relationship (p<.001) between ETHICAL VIOLATIONS CONCERN and PRIVACY CONCERN. This indicates that the more concern a participant has that companies will allow ethical violations with their data, the higher their level of privacy concern.

Table 5 shows that there is a statistically significant relationship (p<.029) between PRIOR PRIVACY VIOLATIONS and COMFORT WITH DATA COLLECTION. This indicates that the more prior experiences a participant had with privacy violations such as data breaches or ethical violations, the higher their level of comfort with

data collection. This result is counter-intuitive, but may indicate that users who have already experienced data privacy violations are no longer as concerned about them**.**

Variable	Chi-square Value	df	p-value (* indicates statistical significance)
Prior Privacy Violations	7.093	2	.029*
Ethical Violations Concern	35.516	2	.000*

Table 5: Comfort with Data Collection Chi-Square

Additionally, there is a strong statistically significant relationship (p<.000) between ETHICAL VIOLATIONS CONCERN and COMFORT WITH DATA COLLECTION. This indicates that the more concern a participant has that companies will allow ethical violations with their data, the higher their level of comfort with data collection. This result is also counter-intuitive, but may indicate that while participants are concerned with potential ethical violations, they find that the benefits outweigh the risks.

6. DISCUSSION

The primary focus of this study was to explore the perceptions of users of Internet-connected devices in regard to data privacy responsibilities of the companies that collect data from these devices. User perceptions were assessed by questions related to concerns about companies having an ethical violation with data collected, the company's responsibility to protect user privacy, and the adequacy of a company's safeguards. It was interesting to note that 91.6% of the participants had some level of concern and 68.1% of the participants actually had experienced some kind of ethical violation. Of the participants, 95.3% responded that a company is responsible for protecting data collected on their devices, which seems in line with the expectations. Of the participants, 85.3% stated that the companies had put in proper safeguards to protect their privacy. Considering these responses, one theory is that users feel that companies are safeguarding their data but are nevertheless still concerned about potential ethical violations.

After reviewing the open-ended question about the users' perceptions on a company's ethical responsibilities, it was clear that users felt strongly that a company needs to go above and beyond to protect data privacy if the need should arise to collect data. Several responses noted that the benefits that could be obtained with collecting this data could outweigh the impact of an ethical violations. This is a valuable finding because it shows that some users find the benefits providing by data collection to outweigh the risks. Most important was to see that users appreciate when companies' setup internal departments to help ensure that consumer data is protected to avoid an ethical violation. Lastly, the researchers found it interesting that a few participants mentioned that in the time of internet-connected devices, it is also our responsibility to understand what data is collected, how it is used, and how big data can be impactful in our lives. This comment was important because it showed that not only is the responsibility on the company, but some responsibility should be shared with the individual using these devices.

The second research question focused on the participants' prior experiences with data collection from devices and the impact it has had on their life. A very low percentage stated they either had no impact in their lives or do not allow companies to collect data. Most interesting was that 53.8% of the participants had a positive impact from the data being collected while 29.6% did not. The split between these two impacts seems proportionate to the open-ended comments as some participants stated a strong desire for additional protection and others were accepting of data collection but with a beneficial trade-off like improved healthcare or user experience.

The research also found that participants had a higher comfort level with data collection when they had less prior experience with a privacy issue such as a data breach or ethical violation. An indirect relationship was found between comfort collecting data and the impact of allowing data to be collected. Therefore, the higher comfort level was linked with a positive impact while a lower comfort level was highest with a negative impact. While these two relationships were indirect, they do add to the findings of the study that comfort allowing data collection does have a statistically significant relationship with their prior experience of a privacy issue such as a data breach or ethical violation.

7. CONCLUSIONS

It is clear that there are serious data privacy concerns for users of IoT devices (Cirne et al., 2022; Foltz & Foltz, 2021; Rice & Bogdanov,

2019) and for companies that provide these devices (Martin, 2019; Acquisti et al., 2006).

This study explored the perceptions of users of Internet-connected (IoT) devices in regard to data privacy responsibilities of the companies that that provide the devices and collect data from them. A clear majority of participants, 95.3%, responded that a company is responsible for protecting data collected on their devices. Further, 85.3% felt that companies did provide adequate safeguards but 91.6% stated that they were concerned about potential ethical violations by companies collecting their data. Collectively, these findings indicate that there is a high level of concern for data privacy, but participants also felt that companies are implementing adequate safeguards and the benefits could outweigh the risks when it comes to allowing IoT data collection.

Additionally, the study examined whether prior experiences with a data privacy violation such as a data breach or ethical violation impacted an IoT user's level of privacy concern. In the sample, a majority, 68.1% had experienced a prior privacy violation. Privacy concern was measured using the MUIPC scale (Xu et al., 2012). The majority of participants, 87.22%, fell into the High Privacy Concern category, indicating that privacy is a concern for the participants. Statistically significant relationships were found between privacy concern and prior privacy violations, and between privacy concern and ethical violations concern. These findings clearly show that high levels of privacy concern are related to past experience with data breaches or ethical violations and specific concern for how companies handle personal data.

More surprising were the statistically significant relationships found between comfort level in allowing data collection and both prior privacy violations and ethical violations concern. These findings seem counter-intuitive and were unexpected. They indicate that as the IoT users' prior experiences with data breaches or other privacy violations increases, their comfort level with data collection increases. Similarly, as the IoT users' concern for ethical violations by companies increases, their comfort level with data collection increases.

A potential limitation of this study was the use of Amazon Mechanical Turk to recruit participants.

MTurk has been known to skew toward tech-savvy participants even though it has been shown to be representative of the overall U.S. population (Lovett, 2018; Redmiles et al., 2019. For this sample in particular, 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 potential risks to data privacy when using IoT devices that other non-technical users.

This exploratory study included some contradictory findings and future studies could further examine the complex perceptions of IoT users about data privacy. Future studies could also focus on corporate responsibilities and address a population of IoT companies to explore the corporate perspective on this issue.

8. REFERENCES

Ablon, L., Heaton, P., Lavery, D.C., & Romanosky, S. (2016). Consumer attitudes toward data breach notifications and loss of personal information. Technical report. Rand Corp.

Aguilar, L. (2014). *Boards of directors, corporate governance and cyber-risks: Sharpening the focus.*http://www.sec.gov/News/Speech/Detail/Speech/1370542057946

Allen, A.M., & Peloza, J. (2015). Someone to watch over me: The integration of privacy and corporate social responsibility. *Business Horizons, 58*, 635-642.

Banerjee, S. S. & Dholakia, R.R. (2008). Mobile advertising: Does location based advertising work? *International Journal of Mobile Marketing, 2*(2), 68-74.

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

Conosco. (2021). IoT security breaches: 4 Real-world examples. Retrieved from https://www.conosco.com/blog/iot-security-breaches-4-real-world-examples/

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.

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.

Haney, J., Acar, Y., & Furman, S. (2021). It's the company, the government, you, and I: User perceptions of responsibility for smart home privacy and security. *Proceedings of the 30th USENIX Security Symposium*, 411-428.

Hassan, M. (2022). State of IoT 2022: Number of connected IoT devices growing 18% to 14.4. billion globally. IOT Analytics.

Hui, K., Hock, H.T., Sang-Yong, T.L. (2007). The value of privacy assurance: An exploratory field experiment. *MIS Quarterly, 31*(1), 19-33.

Identity Theft Resource Center (2022). *Identity Theft Resource Center's 2021 annual data breach report sets new record for number of compromises.* https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises/

Karunakaran, S., Thomas, K., Bursztein, E., & Comanescu, O. (2018). Data breaches: User comprehension, expectations, and concerns with handling exposed data. *Symp. On Usable Privacy and Security*, 217-234.

Kokolakis, S. (2017). Privacy attitudes and privacy behavior: A review of current research on the privacy paradox phenomenon. *Computers & Security, 64*, 122-134.

Lambert, J. (2021). *Microsoft digital defense report shares new insights on nation-state attacks.* Microsoft Security. https://www.microsoft.com/security/blog/2021/10/25/microsoft-digital-defense-report-shares-new-insights-on-nation-state-attacks/

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.

Marti, K. (2019). Breaking the privacy paradox: The value of privacy and associated duty of firms. *Business Ethics Quarterly, 1052*, 150.

Mayer, P., Zou, Y., Schaub, F., & Aviv, A. (2021). Now I'm a bit angry: Individuals' awareness, perception, and responses, to data breaches that affected them. *USENIX Security Symposium 2021.*

Mikhed, V., & Vogan, M. (2018). How data breaches affect consumer credit. *Journal of Banking and Finance*, *88*, 192-207.

Norberg, P.A., Horne, D.R., & Horne, D.A. (2007). The privacy paradox? Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs, 41*(1), 100-126.

NIST. (2017). Information technology laboratory: Computer resource center. https://csrc.nist.gov/glossary/term/personally_identifiable_information

Pew Research Center (2019, November). *Americans and Privacy: Concerned, confused and feeling lack of control over their personal information.* https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

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.

Pollach, I. (2011). Online privacy as a corporate social responsibility: An empirical study. *Business Ethics: A European Review, 20*(1), 88-102.

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.

Rice, M.D., & Bogdanov, E. (2019). Privacy in doubt: An empirical investigation of Canadians' knowledge of corporate data collection and usage practices. *Canadian Journal of Administrative Sciences, 36*, 163-176.

Risk Based Security (2022, February). *Data breach report: 2021 year end.* https://www.riskbasedsecurity.com/2022/02/04/data-breach-report-2021-year-end/

SAS. (2018). *Data Privacy: Are you concerned?*

Insights from a survey of US consumers. https://www.sas.com/content/dam/SAS/documents/marketing-whitepapers-ebooks/sas-whitepapers/en/data-privacy-110027.pdf

Schumann, J.H., Von Wagenheim, F., & Groen, N. (2014). Targeted online advertising: Using reciprocity appeals to increase acceptance among users of free web services. *Journal of Marketing, 78*(1), 59-75.

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.

Sophos. (2021). *Ransomware recovery cost reaches nearly $2 million, more than doubling in a year: Sophos survey shows.* https://www.sophos.com/en-us/press-office/press-releases/2021/04/ransomware-recovery-cost-reaches-nearly-dollar-2-million-more-than-doubling-in-a-year

Strahilevitz, L.J., & Kugler, M.B. (2016). Is privacy policy language irrelevant to consumers? *The Journal of Legal Studies, 45*(S2), S69-95.

The Federal Trade Commission. (2020). *When information is lost or exposed 2020.* https://www.identitytheft.gov/databreach

Wagenseil, P. (2019). *What to do after a data breach.* https://www.tomsguide.com/us/data-breach-to-dos,news-18007.html

World Economic Forum (2020, December). *After reading, writing and arithmetic, the 4th 'r' of literacy is cyber-risk.* https://www.weforum.org/agenda/2020/12/cyber-risk-cyber-security-education

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.

Xu, H., Zhang, C., Shi, P., & Song, P. (2009). Exploring the role of overt vs. covert personalization strategy in privacy calculus. *Academy of Management Annual Meeting Proceedings*, *2009*(1), 1-6.

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.

Zou, Y., Roundy, K., Tamersoy, A., Shintre, S., Roturier. J., & Schaub, F. (2020). Examining the adoption and abandonment of security, privacy, and identity theft protection practices. *ACM CHI Conference on Human Factors in Computing Systems.*