JOURNAL OF INFORMATION SYSTEMS APPLIED RESEARCH

Volume 14, Issue. 2
June 2021
ISSN: 1946-1836

In this issue:

iscap
Information Systems & Computing Academic Professionals

The **Journal of Information Systems Applied Research** (JISAR) is a double-blind peer reviewed academic journal published by ISCAP, Information Systems and Computing Academic Professionals. Publishing frequency is three issues a year. The first date of publication was December 1, 2008.

JISAR is published online (https://jisar.org) in connection with CONISAR, the Conference on Information Systems Applied Research, which is also double-blind peer reviewed. Our sister publication, the Proceedings of CONISAR, features all papers, panels, workshops, and presentations from the conference. (https://conisar.org)

The journal acceptance review process involves a minimum of three double-blind peer reviews, where both the reviewer is not aware of the identities of the authors and the authors are not aware of the identities of the reviewers. The initial reviews happen before the conference. At that point papers are divided into award papers (top 15%), other journal papers (top 30%), unsettled papers, and non-journal papers. The unsettled papers are subjected to a second round of blind peer review to establish whether they will be accepted to the journal or not. Those papers that are deemed of sufficient quality are accepted for publication in the JISAR journal. Currently the target acceptance rate for the journal is about 40%.

Questions should be addressed to the editor at editor@jisar.org or the publisher at publisher@jisar.org. Special thanks to members of ISCAP/EDSIG who perform the editorial and review processes for JISAR.

2021 ISCAP Board of Directors

Eric Breimer Siena College President	James Pomykalski Susquehanna College Vice President	Jeffry Babb West Texas A&M Past President/ Curriculum Chair
Jeffrey Cummings Univ of NC Wilmington Director	Melinda Korzaan Middle Tennessee State Univ Director	Niki Kunene Eastern CT St Univ Director/Treasurer
Michelle Louch Carlow University Director	Michael Smith Georgia Institute of Technology Director/Secretary	Lee Freeman Univ. of Michigan - Dearborn Director/JISE Editor
Tom Janicki Univ of NC Wilmington Director/Meeting Facilitator	Anthony Serapiglia St. Vincent College Director/2021 Conf Chair	

Copyright © 2021 by Information Systems and Computing Academic Professionals (ISCAP). Permission to make digital or hard copies of all or part of this journal for personal or classroom use is granted without fee provided that the copies are not made or distributed for profit or commercial use. All copies must bear this notice and full citation. Permission from the Editor is required to post to servers, redistribute to lists, or utilize in a for-profit or commercial use. Permission requests should be sent to Scott Hunsinger, Editor, editor@jisar.org.

JOURNAL OF INFORMATION SYSTEMS APPLIED RESEARCH

Editors

Scott Hunsinger
Senior Editor
Appalachian State University

Thomas Janicki
Publisher
University of North Carolina Wilmington

2021 JISAR Editorial Board

Ulku Clark
University of North Carolina Wilmington

Ed Hassler
Appalachian State University

Muhammed Miah
Tennessee State University

James Pomykalski
Susquehanna University

Christopher Taylor
Appalachian State University

Karthikeyan Umapathy
University of North Florida

Jason Xiong
Appalachian State University

Privacy Concerns and Data Sharing Habits of Personal Fitness Information Collected via Activity Trackers

Jamie Pinchot
pinchot@rmu.edu

Donna Cellante
cellante@rmu.edu

Computer and Information Systems Department
Robert Morris University
Moon Township, PA 15108 USA

Abstract

Activity trackers such as FitBit and Apple Watch have become popular for collecting fitness and health data. Few studies have examined privacy concerns and risks regarding the use of activity trackers and the sharing of personal fitness information (PFI). This study presents findings from a survey of activity tracker users (n = 325) to explore the privacy concerns, perceptions, and habits of users. Findings indicate that several factors impact the PFI data sharing habits of users, including understanding privacy policies, understanding device privacy settings, and the level of value placed on PFI. Further, knowledge of privacy policies and settings had a clear impact on perceptions of the sensitivity and value of PFI.

Keywords: privacy, Internet of Things, personal fitness information, health information, activity trackers, fitness trackers

1. INTRODUCTION

Devices that are able to connect to a network and interact with other apps and devices are referred to as the Internet of Things (IoT). Typical examples of IoT devices are smart phones, tablets, smart watches, activity trackers, home appliances, home assistants, smart cars, and smart parking meters. The number of global IoT devices connected to the Internet has been increasing at a rapid pace, from 18.4 billion networked devices in 2018 to an estimated 29.3 billion devices in 2023. This includes multiple devices per person, with a global average of 2.4 devices per individual in 2018 and an estimated increase to 3.6 devices per individual in 2023 (Cisco, 2020).

The Pew Research Center estimates that 60 percent of all Americans engage in some sort of fitness tracking (Boran, 2017). Many people own a wearable activity tracker such as a Fitbit, Apple Watch, Garmin, or Samsung Gear, and use associated mobile apps to track fitness and activity data. If worn continuously, these trackers can monitor the user 24/7, and collect a large amount of data. Among IoT devices, activity trackers are among those that have the greatest number of sensors, which are capable of collecting sensitive information, such as step count, location, heart rate, exercise activities, distance travelled, calories burned, weight, and even sleep habits (Torre, Sanchez, Koceva, & Adorni 2018). This can be a serious privacy concern. Collectively, the health-related data

captured by activity trackers is referred to as personal fitness information (PFI).
Activity trackers fall into the category of IoT devices called wearables. The term "wearable technology" refers to an electronic device or product which can be worn by a person to integrate computing into daily activity or work and use technology to avail advanced features and characteristics (PR Newswire, 2013). While wearables can conveniently provide access to an overabundance of PFI for individuals, there are potential privacy risks to consider. Scholars have been spreading the word about the risk of possible data loss, leakage, or compromise with self-tracing wearable technologies (Ajana 2017; Fotopoulou & O'Riordan 2016; and Lanzing 2016).

2. RELATED WORK

Security risk is defined as a "circumstance, condition, or event with the potential to cause economic hardship to data or networked resources in the form of destruction, disclosure, modification of data, denial of service, and/or fraud, waste and abuse" (Balta-Ozkan et al., 2013). In the U.S., citizens' Constitutional right to privacy is implied in the language of the 4th Amendment, where it states: "The right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated" (Legal Information Institute, n.d.). While some studies have found that users of wearable devices are concerned with privacy (Fuller et al., 2017; Seguar Anaya et al., 2018; Vitak et al., 2018), others suggest that individuals have low levels of concern when it comes to disclosing information collected with wearable devices (Lehto & Lehto, 2017; Motti & Caine, 2015; Truong, 2019).

Vitak et al. (2018) studied 361 activity tracker users to understand how concerns about privacy affected users' mental models of personal fitness information (PFI) privacy. The study found that the majority of users were lacking general knowledge about how fitness companies collect, store, and share activity data. Vitak et al. (2018) found no significant relationships between user's disclosure of activity data and privacy concerns. They note that this finding echoes another study that found that the privacy paradox does exist and attributes it largely to the apathy of Internet users who do value privacy, but feel that once information is shared, it is out of their control (Hargittai & Marwick, 2016).

Lehto and Lehto (2017) conducted a qualitative study focused on user experiences of using a wearable device and associated privacy concerns. The study found that information collected with wearable devices was not perceived by participants as sensitive or private, although health information stored in medical records was considered to be very sensitive and private. This disconnect is of increasing concern as more health information that was only stored in medical records is now being stored in a variety of places including activity trackers, mobile apps, and cloud services.

Torre et al. (2018) conducted a study on FitBit wearables and associated mobile apps, including FitBit's own app and the Lose It! app. They found that during installation of the FitBit app, which is required in order to use the device, users are prompted to allow a number of permissions on their smart phone including: identity, contacts, location, SMS, photos/media, camera, Bluetooth, and device ID/call information. Installation requires name, gender, height, weight, and birthday as mandatory inputs. The study's findings illustrate the privacy risks for FitBit data due to the possibility of using shared data to correlate to third party app data or infer undisclosed personal information.

One privacy risk with wearable devices and the associated services is that individuals may not understand how their information is stored and handled (Patterson, 2013). Further, it is possible that risk awareness regarding the uses of health information data, even in aggregate form, is not well understood by users. In fact, device manufacturers of activity trackers have claimed that health and fitness data of users is de-identified and aggregated, and therefore does not pose a privacy risk (FitBit, n.d.). FitBit's privacy policy, for example, states "We may share non-personal information that is aggregated or de-identified so that it cannot reasonably be used to identify an individual" (FitBit, n.d., para. 21). However, this can be misleading to users who may not know that there are often ways to re-identify this data if it was only partially aggregated or aggregated in ways that might be possible to reverse engineer. Any partial demographic data that can be associated with the anonymized data could allow for reidentification (Na et al., 2018).

Machine learning can also be used for reidentification of de-identified and aggregated health information collected from activity trackers (Na et al., 2018). Na et al. (2018)

conducted a cross-sectional study of national physical activity data collected for 14,451 individuals between 2003 and 2006. The data sets included fitness data such as step count that was collected from activity trackers. Though this data was de-identified and partially aggregated, the authors were able to use machine learning to re-identify individuals by learning their daily footstep patterns via 20-minute-level physical activity data and connecting those patterns to demographic data. Approximately 95% of adults and 80% of children in the study were successfully identified (Na et al., 2018).

Another privacy risk is that increasing quantities of health data are being created outside of the protection of the Health Insurance Portability and Accountability Act (HIPAA). This includes data generated via activity trackers and mobile health apps as well as other social media (Glenn & Monteith, 2014). The companies that collect this health data include data brokers and Internet companies, often combining this data with other known information about users and then sell it for advertising or other purposes (Pinchot et al., 2018). In some cases, employers have begun to collect heath data on employees and treat it in similar fashion (Brown, 2016).

A final privacy risk of activity trackers is that location information can be used to track an individual or locate sites that an individual frequently visits. For example, location information from activity trackers published as a heat map by Strava.com, an exercise-focused social network, has been used to identify the location of military sites (Perez-Pena & Rosenberg, 2018).

3. CURRENT STUDY

While it is clear that there are risks to data privacy for users of activity trackers, these devices continue to grow in popularity and use. The global market for activity trackers was valued at $17.9 million in 2016 and is forecasted to grow 19.6% by 2023 (Loomba & Khairnar, 2018). Even for users who express concern for privacy, there is often a mismatch between attitude and behavior. This is known as the privacy paradox, and has been studied extensively in relation to the use of social media (Acquisti & Gross, 2006; Barnes, 2006; Kokolakis, 2017; Taddicken, 2014).

The purpose of this study is to explore data privacy concerns, perceptions, and habits among users of activity trackers. The first research question will explore a number of factors related to PFI privacy:

RQ1: What are activity tracker users' PFI privacy concerns, perceptions about PFI sensitivity, perceptions about PFI value, understanding of privacy settings, understanding of privacy policies, and PFI data sharing habits?

The second research question probes further by examining the relationship between these concerns, perceptions, and habits:
RQ2: What is the relationship between activity tracker users' PFI privacy concerns, perceptions about PFI sensitivity, perceptions about PFI value, understanding of privacy settings, understanding of privacy policies, and their PFI data sharing habits?

4. RESEARCH METHODOLOGY

This study used an electronic survey consisting of 20 quantitative questions. The sample (n=325) for the study includes adults 18 and older who have used an activity tracker such as a FitBit, Apple Watch, etc. Participants were first asked about their frequency of use for their activity tracker, specifically asking for the average number of days (on a scale from 0 to 30) they wear their tracker in a typical month. Participants were then asked a set of questions focusing on their privacy concerns, a set of questions focusing on their PFI data sharing habits, a set of questions focused on their understanding of privacy settings for their activity tracker, and questions regarding their understanding of the privacy policy and data sharing activities of the company that makes their activity tracker, their perception of the sensitivity of PFI data, and their perception of the value of PFI data.

Mobile User's Information Privacy Scale (MUIPC)

To measure the participants' privacy concerns regarding activity trackers and their associated mobile apps, we used the Mobile Users' Information Privacy Scale (MUIPC) that was developed by Xu et al. (2012). MUIPC was developed as an evolution of two prior scales focused on privacy: the Concern for Information Privacy (CFIP) scale developed by Smith et al. (1996) to measure individuals' concern about organizational privacy and the Internet User's Information Privacy (IUIPC) scale, developed by Malhotra et al. (2004) to adapt CFIP to an online environment for Internet users concerned about information privacy (Malhotra et al., 2004;

Smith et al., 1996; Xu et al., 2012). MUIPC is a 9-item scale that was developed "to reflect mobile users' concerns about information privacy" (Xu et al., 2012, p. 13). Items were measured on a five-point Likert scale anchored with "Strongly disagree" = 1 and "Strongly agree" = 5. The scale includes three dimensions: perceived surveillance, perceived intrusion, and secondary use of personal information (Xu et al., 2012).

Perceived Surveillance (SURV)
(1) I believe that the location of my activity tracker is monitored at least part of the time.
(2) I am concerned that the mobile app associated with my activity tracker is collecting too much information about me.
(3) I am concerned that mobile apps may monitor my activities on my activity tracker.
Perceived Intrusion (INTR)
(4) I feel that as a result of my using an activity tracker, others know about me more than I am comfortable with.
(5) I believe that as a result of my using an activity tracker, 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 an activity tracker, information about me is out there that, if used, will invade my privacy.
Secondary Use of Personal Information (SUSE)
(7) I am concerned that mobile apps with access to my activity data may use my personal information for other purposes without notifying me or getting my authorization.
(8) When I give personal information to use mobile apps, I am concerned that apps with access to my activity data may use my information for other purposes.
(9) I am concerned that mobile apps with access to my activity data may share my personal information with other entities without getting my authorization.

Table 1: Adapted Mobile Users' Information Privacy Scale (MUIPC)
Note: Adapted from Xu et al. (2012)

Perceived surveillance has been defined as, "the watching, listening to, or recording of an individual's activities" (Solove, 2006, p. 490). Perceived intrusion is defined as, "invasive acts that disturb one's tranquility or solitude" (Solove, 2006, p. 491). Table 1 shows the items used for the MUIPC scale.

The MUIPC scale has good internal consistency, with a Cronbach alpha coefficient above .7 reported for all three subscales (Xu et al., 2012; Degirmenci et al., 2013).

PFI Data Sharing Habits (SHARE)
As personal fitness information (PFI) can often include sensitive data that users may not want shared in certain contexts, it was important to understand how respondents disclose PFI in an online environment. We adapted three yes/no questions from Vitak et al. (2018) that focused on activity tracker data sharing habits. Respondents were asked whether they had (1) shared fitness data online, (2) configured their tracker to automatically post fitness data online, and (3) shared fitness data with other users. These three items were reported individually and averaged to create an index of PFI data sharing habits.

Understanding of Privacy Settings (SET)
Users of activity trackers may not always know how to review and configure privacy settings on their devices. Or, users may be aware of how to configure privacy settings but do not make an effort to do so. Two items were used to measure understanding of the privacy settings of their activity tracker. Respondents were asked (1) how confident they are that they understand how to use the privacy settings of their activity tracker (measured on a scale from 0 = not at all confident to 100 = very confident) and (2) how much effort they have put into reviewing and configuring privacy settings of their activity tracker (measured on a scale from 0 = no effort to 100 = much effort). These two items were averaged to create an index of understanding of privacy settings.

Understanding of Privacy Policies (POL)
Many companies have data sharing policies and practices that allow users' personal data to be shared, individually or in aggregate, with third parties. To address this important concept, we adapted one question from Vitak et al. (2018) that asked respondents how confident they are that they understand the privacy policy and data sharing practices of the company that makes their activity tracker. This question was measured on a scale from 0 = not at all confident to 100 = very confident.

Perception of PFI Sensitivity (SENS)
It is important to understand how respondents feel about PFI in relation to other types of personally identifiable information (PII). To address data sensitivity, we asked respondents how concerned they would be if their activity tracker data were compromised (such as via a security breach). Responses were measured on a scale from 0 = not at all concerned to 100 = very concerned.

Perception of PFI Value (VAL)
To address data value, respondents were asked how valuable their activity tracker data is to them, in comparison to other types of PII, such as financial data. Responses were measured on a scale from 0 = not at all valuable to 100 = very valuable. Both questions were adapted from Vitak et al. (2018).

Sample
The sample for this study was obtained via Amazon Mechanical Turk (MTurk), a crowdsourcing tool that has been used extensively by academic researchers for survey research and allows access to a pool of participants that meet inclusion criteria (Lovett, 2018; Redmiles et al., 2017). This tool allows a survey to be posted with a specified compensation amount. For short surveys, the compensation amount per survey completion is typically between $.10 and $.50 (Lovett, 2018). This study provided compensation within the recommended range. Redmiles et al. (2017) found that samples from MTurk studies are largely representative of the entire U.S. population and are comparable to census web-panel and telephone survey respondents. However, they also note that respondents on MTurk differ from their demographic peers in their online skill and experience level (Redmiles et al., 2017). This higher level of online skill and experience should be taken into account for a study focused on mobile device and Internet privacy issues.

The survey used in this study was created in Question Pro and posted on Amazon Mechanical Turk targeting between 300-350 responses. Data was collected in April 2020. A total of 386 people started the survey, but 325 (84%) participants completed usable surveys.

4. FINDINGS

Of the participants who completed the survey (n=325), the majority of the participants were in the 25-34 year old range. We did, however, have four participants above 64 years old. Table 2 is details the breakdown of the ages.

Age Range	No. of Participants	Percentage
18-24	52	16%
25-34	172	52.9%
35-44	55	16.9%
45-54	34	10.5%
55-64	8	2.5%
Above 64	4	1.2%

Table 2: Participants by Age

The participants came from a variety of countries, with the majority of participants, 56.9%, from the United States and significant numbers of participants from India, 18.5%; Brazil, 7.7%; and Canada, 3.4%, as shown in Table 3. The remainder of participants, 13.5%, came from a variety of other countries including France, Spain, Columbia, and Venezuela.

Country	Frequency	Percentage
United States	185	56.9%
India	60	18.5%
Brazil	25	7.7%
Canada	11	3.4%
Other (17 countries)	44	13.5%

Table 3: Participants by Country

The average days per month that the participants used their activity tracker was between 21-30 days. This indicates that the sample included users who actively used their activity trackers. Table 4 shows the breakdown of usage:

Days Per Month	No. of Respondents	Percentage
0-10 days	41	12.6%
11-20 days	112	34.5%
21-30 days	172	52.9%

Table 4: Activity Tracker Usage by Days per Month

Addressing RQ1
RQ1 asked "What are activity tracker users' PFI privacy concerns, perceptions about PFI sensitivity, perceptions about PFI value, understanding of privacy settings, understanding of privacy policies, and PFI data sharing habits?" PFI privacy concern (MUIPC) was measured using the MUIPC scale. Of the 325 respondents, 296 had completed all questions used in the scale and were included in the index. The scale

showed good internal consistency (Cronbach's a=.89). The median value of the index score was used to divide the users into high and low privacy concern categories. As shown in Figure 1, the high and low concern categories were nearly equally split, with low concern having a slight edge (50.9%) over high concern (49.1%). This result clearly showed that there was not a strong level of opinion regarding privacy concern, in either direction, for this sample. The majority of the respondents had an average score that fell into the Neutral response category (mean = 3.52, median = 3.67).

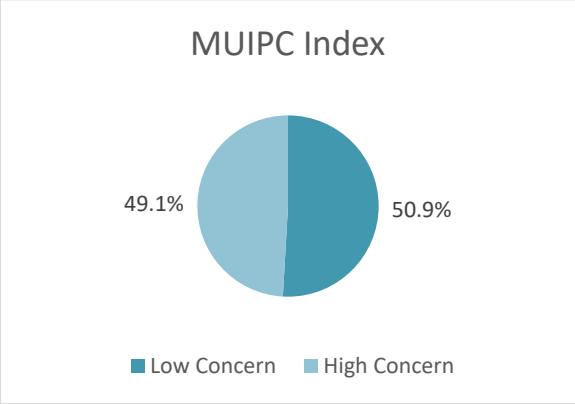

Figure 1: MUIPC Index Showing High and Low Privacy Concern Categories

PFI sensitivity (SENS), PFI value (VAL), understanding of privacy policies (POL), and understanding of privacy settings (SET) were each measured on a sliding scale of 0 to 100. Table 5 shows the breakdown of responses for each of these variables.

Response	SENS	VAL	POL	SET
0 to 20	34	55	59	38
21 to 40	42	67	58	62
41 to 60	75	86	68	83
61 to 80	86	63	83	75
81 to 100	78	52	55	33
Mean	59.8	50.9	52.6	50.7
Median	61	50	52	50.5

Table 5: Breakdown of Responses for SENS, VAL, POL, and SET

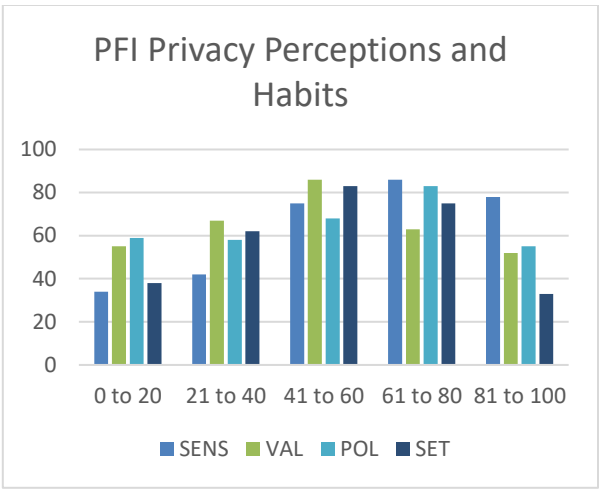

Figure 2: PFI Privacy Perceptions and Habits

Figure 2 visually depicts the breakdown of responses. The mean is near the midpoint of the scale for all four variables, though PFI sensitivity is skewed very slightly more toward the higher end of the scale.

Three questions on the survey addressed the PFI data sharing habits of respondents. Of the 325 participants, 112 never shared any information at all. Forty-three participants shared at least one aspect. Fifty-nine respondents shared at least two aspects, and 94 participants shared everything. Seventeen respondents did not answer the questions.

Table 6 shows the breakdown of the data sharing habits:

Amount of Sharing	Frequency	Percent
0% (nothing)	112	34.5%
33% (1 part)	43	13.2%
66% (2 parts)	59	18.2%
100% (3 parts)	94	28.9%
No answer	17	5.2%

Table 6: PFI Data Sharing Habits

An interesting point about this table is that there are about the same number of participants who share nothing (112) as those that share everything (94). An inverted bell curve as shown in Figure 3 visually demonstrates the breakdown.

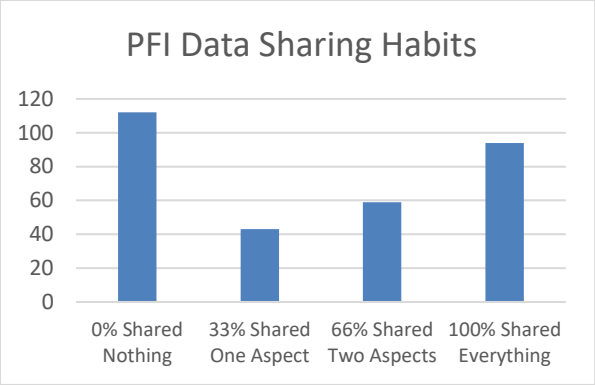

Figure 3: PFI Data Sharing Habits of Participants

Addressing RQ2

RQ2 asked, "What is the relationship between activity tracker users' PFI privacy concerns (MUIPC), perceptions about PFI sensitivity (SENS), perceptions about PFI value (VAL), understanding of privacy settings (SET), understanding of privacy policies (POL), and their PFI data sharing habits (SHARE)?" Relationships between the privacy factors were investigated using the Pearson's product-moment correlation coefficient.

Impacts on PFI Data Sharing Habits (SHARE)

There was a statistically significant, negative correlation between understanding of privacy policies (POL) and PFI data sharing habits (SHARE), $r = -.139$, $n = 307$, $p < .05$. This indicates that high levels of understanding of privacy policies were associated with low levels of PFI data sharing habits. Additionally, there was a statistically significant, negative correlation between understanding of privacy settings (SET) and PFI data sharing habits (SHARE), $r = -.251$, $n = 284$, $p < .001$. This indicates that high levels of understanding of privacy settings were associated with low levels of PFI data sharing habits. This clearly shows that the more understanding a user has of the privacy policies in place for the company that makes their activity tracker, and the more knowledgeable a user is of the device's privacy settings, the less likely they will be to share PFI data online.

A statistically significant, negative correlation was also found between perceptions of PFI value and PFI data sharing habits, $r = -.284$, $n = 306$, $p < .001$. This indicates that high perceptions of PFI value were associated with low levels of PFI data sharing habits. So, the more value that a user placed on PFI, the less likely they were to share PFI data online.

Notably, there was no correlation found between the respondents' PFI privacy concern (as measured by MUIPC) or PFI sensitivity and PFI data sharing habits.

Impacts of Understanding Privacy Policies (POL) and Device Privacy Settings (SET)

There was a statistically significant correlation between understanding of privacy policies (POL) and PFI sensitivity (SENS), $r = .191$, $n = 313$, $p < .005$. This indicates that high levels of understanding of privacy policies were associated with high perceptions of PFI sensitivity. There was also a statistically significant correlation between POL and PFI value (VAL), $r = .383$, $n = 321$, $p < .001$. This indicates that high levels of understanding of privacy policies were associated with high perceptions of PFI value. There was a statistically significant correlation between understanding of privacy settings (SET) and PFI sensitivity (SENS), $r = .334$, $n = 292$, $p < .001$. This indicates that high levels of understanding of privacy settings were associated with high perceptions of PFI sensitivity. Additionally, there was a statistically significant correlation between SET and PFI value (VAL), $r = .542$, $n = 296$, $p < .001$. This indicates that high levels of understanding of privacy settings were associated with high perceptions of PFI value. Lastly, there was a strong, statistically significant correlation between POL and SET, $r = .702$, $n = 296$, $p < .001$. This indicates that high levels of understanding of privacy policies were associated with high levels of understanding of privacy settings.

The more knowledgeable a user was on privacy policies, the higher they valued PFI and the higher they found PFI's sensitivity in comparison to other types of data. Additionally, the more knowledgeable a user was on privacy policies, the more likely they were to be knowledgeable on privacy settings on their device. The inverse was also true; the more knowledgeable a user was on the privacy settings of their device, the more knowledgeable they would be of privacy policies and the higher they valued PFI and the higher they found PFI's sensitivity.

Another interesting significant finding was related to POL. There was a statistically significant, negative correlation between POL and privacy concerns (MUIPC), $r = -.132$, $n = 296$, $p < .05$. This indicates that high levels of privacy concern were associated with low levels of understanding of privacy policies.

Impacts on Privacy Concerns (MUIPC)

There was a statistically significant correlation between PFI data sensitivity (SENS) and MUIPC ($r = .366$, $n = 286$, $p < .001$) and PFI value (VAL) and MUIPC ($r = .166$, $n = 294$, $p < .005$). This indicates that high perceptions of PFI data sensitivity and data value were associated with high levels of privacy concern.

5. CONCLUSIONS

First, the authors acknowledge some possible limitations to this research. The use of Amazon Mechanical Turk (MTurk) for data collection may have introduced a limitation in that users of MTurk often skew toward the online-savvy, which could impact the generalizability of results if participants had more online experience and perhaps used this experience to more readily find and learn about privacy policies and settings for their activity trackers (Redmiles et al., 2017). Future studies could minimize this potential bias by utilizing a sample that is not skewed in terms of online experience and may better represent a general audience of activity tracker users. Additionally, volunteer response bias is always a possibility when conducting an online survey, and this could be exacerbated by paying participants via MTurk. This bias could result in overrepresentation of participants with strong opinions on the survey topic.

The participants surveyed showed an interesting mix of privacy factors related to the use of wearable activity trackers. Participants were active users of activity trackers, with the majority using a tracker between 21 and 30 days in an average month. They showed a neutral stance in terms of overall privacy concern for PFI, with the majority of participants averaging a neutral score on the MUIPC scale. Their PFI data sharing habits were somewhat dichotomous, with the majority of participants either sharing no PFI online (35%) or sharing all aspects of PFI data online (29%).

Findings indicated that the factors that significantly impacted activity tracker users' personal fitness information (PFI) data sharing habits (SHARE) included understanding privacy policies (POL), understanding privacy settings on the device (SET), and the level of value they placed on PFI data (VAL). Each of these factors had an inverse relationship with data sharing habits, meaning that the more a user understood privacy policies and settings, and the more they valued PFI, the less likely they were to share PFI online. Their level of privacy concern (as measured by MUIPC) and the level of sensitivity they placed on PFI in comparison to other types of data (SENS) did not have any impact on data sharing habits (SHARE). As privacy concern did not have an impact on data sharing habits, there is no support from these results for the concept of a privacy paradox for IoT wearables such as activity trackers.

Additionally, knowledge of privacy policies (POL) and device privacy settings (SET) for activity trackers had a significant impact on both perceptions of PFI sensitivity (SENS) and PFI value (VAL). There was a clear connection between this knowledge and how sensitive or valuable a user found PFI. This could indicate that a user gains a clearer understanding of the types of risks associated with disclosure of PFI via the knowledge gained by learning more about the company's privacy policies and settings that are available to secure PFI data on an activity tracker device. There was also a significant inverse relationship between knowledge of privacy policies (POL) and level of privacy concern (MUIPC) such that as knowledge of privacy policies increased, the level of privacy concern decreased. This could be interpreted that privacy policies were found to be reassuring to users and thus decreased their concerns about PFI privacy.

Higher perceptions of the sensitivity and value of PFI had a significant impact on privacy concern. This logically shows that the higher the importance a user placed on PFI, the more concerned they were about PFI privacy. However, as PFI privacy concern was not shown to have impacted data sharing habits, the results of this study did not support the idea of a privacy paradox for PFI shared via activity trackers.

While this study has shed some insights on PFI privacy concerns, perceptions, and data sharing habits, additional work is warranted. We are moving into an era where personal fitness information (PFI) can be auto-generated by a variety of IoT wearables and other devices and used, individually or in aggregate, in ways that users may not anticipate. This kind of data can potentially be used to evaluate healthcare and insurance applications and claims, as well as other employer-sponsored programs. Other applications for this type of data may not have been discovered yet, but could prove to be a privacy risk for individuals. It is imperative that users of IoT wearables, such as activity trackers, are empowered with knowledge about the PFI privacy risks, and also the policies and settings that can be used to mitigate those risks.

6. REFERENCES

Acquisiti, A., & Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on Facebook. PET 2006: International Workshop on Privacy Enhancing Technologies. Springer, 36-58. https://doi.org/10.1007/11957454_3

Ajana, B. (2017). Digital health and the biopolitics of the quantified self. *Digital Health, 3,* 2. Doi: 10.1177/2055207616689509

Balta-Ozkan, N., Davidson, R., Bicket, M., and Whitmarsh, L. (2013). Social barriers to the adoption of smart homes. *Energy Policy, 63,* 363-374.

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday, 11*(9). https://doi.org/10.5210/fm.v11i9.1394

Boran, M. (2017, June 15). *Fitness trackers run into data security concerns: Self-tracking boom has prompted consumer worries about keeping personal data safe. The Irish Times.* https://www.irishtimes.com/business/technology/fitness-trackers-run-into-resistance-over-data-security-concerns-1.3119483

Brown, E. (2016). The FitBit fault line: Two proposals to protect health and fitness data at work. *Yale Journal of Health Policy, Law, and Ethics, 16*(1), 1-50.

Cisco (2020, March 9). *Cisco annual Internet report 2018-2023.* White paper. https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html

Fotopoulou, A., & O'Riordan, K. (2016). Training to self-care: Fitness tracking, biopedagogy and the healthy consumer. *Health Sociology Review, 25(*3*)*. http://sro.sussex.ac.uk/60044/

Fuller, D., Shareck, M., & Stanley, K. (2017). Ethical implications of location and accelerometer measurement in health research studies with mobile sensing devices. *Social Science & Medicine, 191*, 84-88.

Glenn, T., & Monteith, S. (2014). Privacy in the digital world: Medical and health data outside of HIPAA protections. *Current Psychiatry Reports, 16*(494), 3-11.

Hargittai, E., & Marwick, A. (2016). 'What can I really do?' Explaining the privacy paradox with online apathy. *International Journal of Communication, 10*, 3737-3757.

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

Legal Information Institute. (n.d.). *Fourth amendment*. Cornell Law School. https://www.law.cornell.edu/constitution/fourth_amendment

Lehto, M., & Lehto, M. (2017). Health information privacy of activity trackers. Proceedings of the 16th European Conference on Cyber Warfare and Security. University College Dublin. Dublin, Ireland, 243-251.

Loomba, S., & Khairnar, A. (2018, March). *Fitness trackers market overview.* Allied Market Research. https://www.alliedmarketresearch.com/fitness-tracker-market

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. doi: 10.1111/apps.12124

Motti, V., & Caine, K. (2015). Users' privacy concerns about wearables: Impact of form factor, sensors and type of data collected. *FC 2015: Financial Cryptography and Data Security, 8976*, 231-244. Doi: 10.1007/978-3-662-48051-9_17

Na, L., Yang, C., Lo, C., Zhao, F., Fukuoka, Y., & Aswani, A. (2018). Feasibility of reidentifying individuals in large national physical activity data sets from which protected health information has been removed with use of machine learning. *JAMA Network Open, 1*(8), 1-13. doi:10.1001/jamanetworkopen.2018.6040

Patterson, H. (2013). Contextual expectations of privacy in self-generated health information flows. *41st Research Conference on Communication, Information, and Internet*

Policy. http://dx.doi.org/10.2139/ssrn.2242144

Perez-Pena, R., & Rosenberg, R. (2018, January 29). Strava fitness app can reveal military sites, analysts say. *New York Times.* https://www.nytimes.com/2018/01/29/world/middleeast/strava-heat-map.html

Pinchot, J., Chawdhry, A., & Paullet, K. (2018). Data privacy issues in the age of data brokerage: An exploratory literature review. *Issues in Information Systems, 19*(3), 92-100.

Privacy policy. (n.d.). FitBit. https://www.fitbit.com/us/legal/privacy

PR Newswire. (August 19, 2013). Wearable electronics market and technology analysis (2013-2018): By components (sensors, battery, display, networking); Applications. *PR Newswire*.

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

Taddicken, M. (2014). The 'privacy paradox' in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure. *Journal of Computer-Mediated Communication, 19*(2), 248-273.

Torre, I., Sanchez, O.R., Koceva, F., & Adorni, G. (2018). Supporting users to take informed decisions on privacy settings of personal devices. Springer. doi 10.1007/s00779-017-1068-3

Truong, K. (2019). *How private health info can be identified through fitness tracker data.* MedCityNews. https://medcitynews.com/2019/01/how-private-health-info-can-be-identified-through-fitness-tracker-data/

Vitak, J., Liao, Y., Kumar, P., Zimmer, M., & Kritikos, K. (2018). Privacy attitudes and data valuation among fitness tracker users. *International Conference on Information, iConference 2018: Transforming Digital Worlds*, 229-239. Springer.

Zimmer, M., Kumar, P., Vitak, J., Liao, Y., & Kritikos, K. (2018). 'There's nothing really they can do with this information': Unpacking how users manage privacy boundaries for personal fitness information. *Information, Communication, & Society.* doi: 10.1080/1369118X.2018.154344

Editor's Note:

This paper was selected for inclusion in the journal as an CONISAR 2020 Distinguished Paper. The acceptance rate is typically 7% for this category of paper based on blind reviews from six or more peers including three or more former best papers authors who did not submit a paper in 2020.

©2021 ISCAP (Information Systems and Computing Academic Professionals)