

# Privacy Attitudes and Data Valuation Among Fitness Tracker Users

Jessica Vitak<sup>1</sup>, Yuting Liao<sup>1</sup>, Priya Kumar<sup>1</sup>, Michael Zimmer<sup>2</sup> and Katherine Kritikos<sup>2</sup>

<sup>1</sup> University of Maryland, College Park MD 20742, USA

<sup>2</sup> University of Wisconsin—Milwaukee, Milwaukee WI 53211, USA

{jvitak,yliao598,pkumar12}@umd.edu; {zimmerm,kritikos}@uwm.edu

**Abstract.** Fitness trackers are an increasingly popular tool for tracking one’s health and physical activity. While research has evaluated the potential benefits of these devices for health and well-being, few studies have empirically evaluated users’ behaviors when sharing personal fitness information (PFI) and the privacy concerns that stem from the collection, aggregation, and sharing of PFI. In this study, we present findings from a survey of Fitbit and Jawbone users (N=361) to understand how concerns about privacy in general and user-generated data in particular affect users’ mental models of PFI privacy, tracking, and sharing. Findings highlight the complex relationship between users’ demographics, sharing behaviors, privacy concerns, and internet skills with how valuable and sensitive they rate their PFI. We conclude with a discussion of opportunities to increase user awareness of privacy and PFI.

**Keywords:** Fitness tracking; Privacy; Fitbit; Jawbone; Quantified Self; Smartphones

## 1 Introduction

Fitness trackers are increasingly popular. A 2012 Pew Research Center survey found that 60 percent of Americans track their diet, weight, or exercise; of these, 21 percent used some form of technology, such as fitness trackers [13]. Demand appears to be increasing. Companies shipped 71.5 million fitness-tracking wristbands and watches in 2015; by 2020, that number is predicted to increase to 172.1 million [31].

These devices are part of a larger movement to capture and analyze metrics about one’s health and behaviors, the so-called “quantified self” [23]. Designed to be worn unobtrusively on the body, fitness trackers collect data in an ambient manner with little effort from the user. The miniaturization and ubiquity of sensors in smartphones and fitness trackers enable people to track several aspects of their bodies with one device [23]. These data points, known as “personal fitness information” (PFI), may seem innocuous, but when collected over time or combined with other data, they can reveal detailed insights about people’s health and habits [6, 28, 29].

This paper explores how people who use fitness trackers value the PFI they generate, how much they know about the data collection policies of fitness tracking companies, and how their sharing behavior compares to their overall privacy concerns and protection strategies. Our conceptualization of value encompasses several factors, including how sensitive people perceive their PFI, how concerned they would be if it were compromised, and how they compare PFI to other types of data (e.g., financial).

Our findings highlight how users' perceptions of PFI and their knowledge of fitness tracking companies' data collection policies are similar to and different from other types of information. We discuss the findings in light of the privacy paradox, or the idea that people express privacy concerns about certain activities but behave in ways that appear to undermine their privacy [33]. We conclude by discussing opportunities to increase user awareness of privacy and PFI.

## **2 Related Work**

### **2.1 Fitness Trackers and Ubiquitous Data Collection and Sharing**

Prior research has studied how people embed activity and fitness trackers into their personal and professional lives [14, 16, 30]—or why they do not [7]—with a recent focus on ubiquitous data collection and privacy [2, 6, 8, 28, 29]. The mobile and networked nature of fitness trackers means that they automatically and persistently collect data, which companies share or sell with third parties [12, 19, 20].

The intersection of fitness trackers and ubiquitous data collection poses three main privacy problems [7]. First, people who use fitness trackers often lack awareness about how PFI feeds into larger infrastructures of data collection. This hinders them from making informed decisions about sharing their PFI. Second, the dynamic nature of ubiquitous data collection means that data used for one purpose today may be used for another in the future. Analysis of PFI can be used to infer other characteristics that people have not directly shared [29]. Third, seemingly anonymous user data can be re-identified with increasing ease. Sensor data, for example, is granular enough “that each individual in a sensor-based data set is reasonably unique” [28, p. 38].

While studies reveal that people are broadly concerned with the collection of location data [21, 25, 27], data about mood or stress level [27, 29], conversational behavior [29], and detailed health information like glucose level or blood pressure [27], users of fitness trackers do not express specific privacy concerns about data collection on these devices [15, 21, 25]. Motti and Caine [25] surmise that users' lack of concern stems from a lack of awareness of how privacy can be compromised when companies collect granular data about users over a long time.

### **2.2 The Privacy Paradox and Mismatch in Users' Attitudes and Behaviors**

Prior work illustrates that while people express concerns about privacy, they continue to behave in ways that undermine it [33]. This concept, known as the privacy paradox, has been studied extensively in relation to social media use [1, 3, 5]. Such work attributes the paradox to users' lack of awareness of privacy issues associated with use of such platforms and lack of knowledge of ways to protect privacy. As mobile computing reaches greater ubiquity and internet-enabled devices such as fitness trackers gain popularity, privacy concerns are becoming more salient.

Further, Hargittai and Marwick [18] point out that behaviors often presented as a “privacy paradox” can be more accurately attributed to a sense of apathy or cynicism about online privacy. Even when they engage in privacy-protective behaviors, users recognize that these measures are likely insufficient in the face of online data mining,

widespread data aggregation, and confusing privacy settings. This leads to a belief that privacy violations are inevitable. Considering the privacy paradox as a response to online apathy may yield a more nuanced explanation of why people share PFI.

### 2.3 Current Study

We offer the following research questions to study users' knowledge of how fitness tracking companies use PFI and how much users value their PFI. First, we consider if the privacy paradox applies to PFI and empirically analyze Motti and Caine's [25] suggestion that users lack concern because they are not familiar with the companies' data use policies. If the paradox exists, we would expect that a person's general internet skills, privacy concerns, and knowledge of the fitness tracking company's privacy policies would be unrelated to their usage of the device. If no paradox exists, we would expect to see a positive correlation between people's knowledge and skills and their usage of their device and a negative correlation between privacy concerns and device usage.

*RQ1: What differences—if any—exist between users who have a high understanding of fitness tracking companies' data policies and those who have little to no understanding of these policies?*

Second, we empirically examine how much value users place on their PFI. Even though fitness trackers increasingly collect data that people perceive as sensitive, qualitative research suggests users do not have significant privacy concerns [15, 21, 25]. We believe one reason is because data collection happens largely in the background and the primary data point of most fitness trackers—steps taken—is innocuous on its own. To investigate this, we look at how users compare their PFI to other data types like financial information, and we ask users to compare their perceived value.

*RQ2: How do users view the value of PFI compared to other types of personal information?*

Finally, a goal of this paper is to understand how to help people consider privacy in their decisions about whether and how to use fitness trackers. To do this, we must parse the inter-relationships between various factors that influence a users' valuation of their PFI.

*RQ3: How are individual characteristics and privacy attitudes associated with users' perception of the sensitivity of PFI?*

## 3 Method

In January 2017, we invited two random samples of 3000 employees from two American public universities to participate if they were at least 18, owned a smartphone, and currently used a Fitbit or Jawbone device (which were most popular fitness trackers at the time). Participants completed an online survey and were invited to enter a raffle for one of five USD\$50 gift cards. We received 361 usable responses. Respondents were generally female (75%), age 38 (median=34,  $SD=13.1$ ), and highly educated (69% had an advanced degree). The vast majority (96%) used a Fitbit device, and most (71%) reported wearing it every day.

### 3.1 Measures

**Perceptions of personal fitness information.** Respondents were asked to think about the various types of data their fitness tracker generated and to respond to four original questions with a 0-100 slider scale they could move.

- **Data Sensitivity:** “How concerned would you be if your [Fitbit/Jawbone] data were compromised, such as through a security breach at the company?” (0=Not at All Concerned, 100=Very Concerned;  $M=54.44$ ,  $SD=29.26$ ).
- **Personal Data Value:** “Compared to other types of personal information about you—like financial information—how valuable is your [Fitbit/Jawbone] data to you?” (0=Not That Valuable, 100=Very Valuable;  $M=43.94$ ,  $SD=26.92$ ).
- **Advertisers’ Data Value:** “Compared to other types of personal information about you—like financial information—how valuable do you think that your [Fitbit/Jawbone] data is to third-party advertisers?” (0=Not That Valuable, 100=Very Valuable;  $M=52.60$ ,  $SD=27.13$ ).
- **Black Market Data Value:** “Compared to other types of personal information about you—like financial information—how valuable do you think that your [Fitbit/Jawbone] data is on the black market?” (0=Not That Valuable, 100=Very Valuable;  $M=35.66$ ,  $SD=27.85$ ).

**Privacy and mobile concerns.** Two measures were included to assess respondents’ general and mobile-specific concerns about the privacy of their data. General privacy concerns [34] is an 11-item scale ( $\alpha=.93$ ;  $M=3.72$ ;  $SD=0.98$ ) that asks respondents to “indicate your level of concern about the following scenarios that might happen when you use communication technologies” (scale: 1=Not at all concerned to 5=Very concerned). Mobile users’ information privacy concerns (MUIPC) [35] is an eight-item scale ( $\alpha=.93$ ;  $M=4.20$ ,  $SD=0.82$ ) measuring respondents’ concerns related to personal data sharing via mobile apps (scale: 1=Strongly Disagree, 5=Strong Agree).

**Perceived internet skills.** Internet skills are an often-used measure to gauge a person’s baseline knowledge about the internet. This measure is often used as a proxy to capture a broad understanding of a person’s technical skills. We used Hargittai and Hsieh’s [17] 10-item version of their internet skills scale ( $\alpha=.91$ ;  $M=3.72$ ;  $SD=0.98$ ).

**Knowledge of fitness tracking companies’ data collection policies.** To measure the extent to which people’s practices and concerns match their knowledge of company data policies, we asked respondents a series of questions about what data the Fitbit or Jawbone companies collect, who owns the data, how it is stored, and with whom companies share the data. A respondent’s knowledge score was calculated based on how his or her answers reflect the company’s stated privacy policies.

Respondents were first asked about nine pieces of information—IP address, full name, email address, home address, birthdate, height, weight, smartphone operating system, and GPS/location information—and whether that data is “Not Collected,” “Automatically Collected/Required,” “Optional Information Requested by Company,” or “I Don’t Know/Not Sure.” For example, because Fitbit requires users

to provide their email address, respondents who correctly selected “Automatically Collected or Required” for email address received five points toward their knowledge score. Those who said the email address is optional received one point, and those who said the email address is not collected or said they did not know received zero points. Eight open-ended questions were coded in a similar fashion. The knowledge score was derived by summing scores from each item ( $M=30.07$ ,  $SD=14.09$ ; range: 0-72).

**Fitness tracker sharing activities.** We asked three Yes/No questions about whether respondents had (1) shared fitness stats online, (2) joined a group or competed with other users, and (3) configured their device to automatically post stats online. These items were averaged based on the number of “Yes” responses to create an index of sharing activities; 62% of respondents engaged in at least one activity ( $M=.79$ ,  $SD=.74$ ; range: 0-3).

## 4 Findings

### 4.1 Factors Associated With Knowledge of Fitness Data Privacy Policies

Our first research question explored whether specific factors are associated with users’ knowledge of what the Fitbit and Jawbone companies do with their data (i.e., their “knowledge score”). Echoing other research on privacy policies, respondents had very limited knowledge of the policies of fitness tracking companies: 73% did not know whether Fitbit/Jawbone sold their data and 66% were not sure who owned the data. Regarding data retention, 85% of respondents did not know how long companies stored the data, and 89% were unsure where the data was stored beside the device.

To determine factors associated with a respondent’s knowledge of the privacy policies, we first ran an OLS regression with the knowledge score as the dependent variable (DV) and demographic variables, internet skills, and privacy concerns as independent variables (IVs). Although the overall model was significant, the adjusted R-square was very low, with IVs explaining just 2.3% of the variance. This lack of significant predictors provides support for the privacy paradox, since concerns and skills were similar across all levels of knowledge.

We also explored whether sex and perceived internet skills interacted in predicting respondents’ knowledge. Results showed a significant main effect of sex on respondents’ knowledge,  $F(1, 236)=4.22$ ,  $p<.05$ . Pair-wise comparisons indicated a significant difference in knowledge scores between females ( $M=50.80$ ,  $SD=.95$ ) and males ( $M=46.61$ ,  $SD=1.71$ ). There was no evidence of a main effect of perceived internet skills on respondents’ knowledge; however, there was a significant interaction between sex and perceived internet skills on knowledge,  $F(2, 237)=3.04$ ,  $p<0.05$ . Males scored higher on the knowledge test when they reported the highest level of perceived internet skills, while females scored higher when reporting lower levels of internet skills. After controlling for age and education, the main effect of sex and the interaction effect remained significant.

### 4.2 Users’ Attitudes Toward the Value of Their PFI

**Table 1.** OLS regressions predicting three measures of users' valuation of their PFI.

	<b>Personal Value</b>	<b>Third-Party Value</b>	<b>Black Market Value</b>
	<i>Standardized Betas Reported</i>		
Sex	-.06	.14	.02
Age	.14*	-.02*	-.01
Education	-.14*	.07	.06
Internet Skills	.01	-.03	.02
Privacy Concerns	.06	-.10	-.07
Mobile Data Concerns	-.04	.18*	.18**
Data Sensitivity	.51***	.43***	.50***
Sharing Activities	.02	.01	.01
<i>F</i> (8,180) =	11.87***	7.10***	10.59***
<b>R</b>	<b>.312</b>	<b>.213</b>	<b>.298</b>

\*  $p < .05$  \*\*  $p < .01$  \*\*\*  $p < .001$

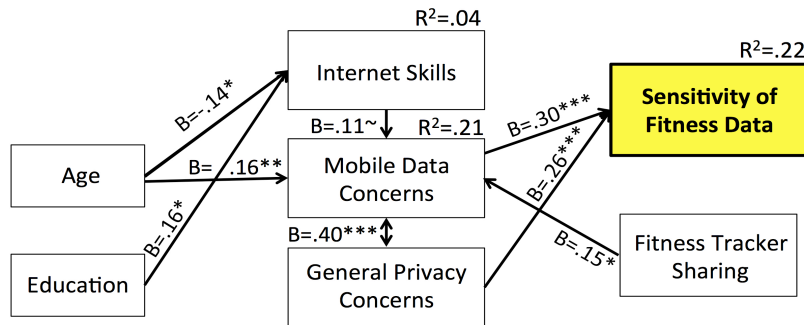
To address RQ2, we used Personal Data Value, Advertisers' Data Value, and Black Market Data Value as DVs in a series of OLS regressions to identify differences in respondents' perceptions of the personal and financial value of PFI (see Table 1).

Depending on the audience for the data, different factors emerged as significant predictors of respondents' data valuation. For example, age was positively correlated with how valuable PFI was to an individual ( $\beta = .14$ ,  $p < .05$ ), while education was negatively correlated with this assessment ( $\beta = -.14$ ,  $p < .05$ ). On the other hand, age was negatively correlated with the perceived value of PFI to third parties like advertisers ( $\beta = -.02$ ,  $p < .05$ ). For both third parties and on the black market, mobile data concerns positively correlated with how valuable respondents perceived their PFI was to other groups ( $\beta = .18$ ,  $p < .05$  in each model). This was not the case in determining the value of PFI to the individual. Finally, respondents' level of concern about their PFI being compromised was strongly positively correlated with all three valuations.

### 4.3 Predicting Users' Perceived Sensitivity of Their PFI

Our final RQ builds on prior analyses to consider the inter-relationships between demographic factors, privacy and skills factors, and tracker-specific factors in explaining respondents' overall valuation of their data. We used Data Sensitivity as the primary dependent variable, asking respondents to indicate their level of concern if their PFI were compromised, as in a data breach.

The proposed model was not a good fit to the data,  $X^2(14,201) = 28.04$ ,  $p = .01$ ; CFI = .79, RMSEA = .07. Therefore, we removed non-significant relationships between variables (including sex and knowledge of the company's privacy policies) and retested the model. The final model (see Figure 1), provided a strong fit to the data,  $X^2(13,201) = 15.77$ ,  $p = .28$ ; CFI = .97, RMSEA = .03. We found a positive correlation between respondents' privacy concerns and the value they place on their fitness data. These variables alone explain 22% of the variance in a person's PFI valuation.



**Figure 1.** Final path model addressing RQ3. All paths are significant.  
 $\sim p < .07$ ,  $* p < .05$ ,  $** p < .01$ ,  $*** p < .001$

## 5 Discussion

Fitness trackers are an increasingly popular tool. In this study, we moved beyond the health factors that drive people to use these devices and focused on how users conceptualize the privacy concerns that may arise from the creation and sharing of the data these devices generate. Through a survey of Fitbit and Jawbone users, we examined how users' attitudes and beliefs influence their use of fitness trackers, their concerns about PFI, and the value they place on this data when compared to other forms of personal information. Below, we discuss how our findings extend existing knowledge and theories about ubiquitous data collection and privacy.

### 5.1 New Platforms, Same User Practices

While researchers have not yet delved deeply into users' perceptions of PFI, this study's findings are largely consistent with how users think about sharing other types of information online. The general lack of knowledge about how fitness tracking companies collect, store, and share data is unsurprising in light of prior research that has found that users generally do not read company privacy policies [24] and, even if they do, they are not likely to understand or remember all the details [10, 22].

For example, Fitbit's privacy policy states, "We don't sell data that could identify you to anyone, anywhere, anytime. Ever. Period." It then states that it "may share or sell aggregated, de-identified data" but does not explain what data this includes or how the company de-identifies it [12]. This is important because PFI is particularly challenging to de-identify [28]. Jawbone's policy states, "We do not rent, sell or otherwise share your individual personal information with third parties, except as follows" and lists six cases in which it may share information [20]. These statements apply to identifiable data (Fitbit) and "individual personal information" (Jawbone), but it is not clear whether these terms encompass data that fitness trackers generate. This echoes the lack of definitional clarity found in other privacy policies [22]. Research confirms that fitness companies share the data their devices generate. A 2014 study by the U.S. Federal Trade Commission (FTC) found that 12 mobile health and fitness apps sent user data to 76 different third parties, which raises "significant privacy implications" [19, p. 35].

Users' lack of knowledge of company data collection practices also speaks to another trend in this dataset, as well as in prior research. While the privacy paradox [1, 3] has been a popular framework for thinking about conflicts between internet users' professed concerns about privacy and their online disclosures, more recent research suggests that internet users do care about their privacy but are generally apathetic toward the effort required to actively negotiate their self-presentation in online spaces [18]. Findings from the current study extend this argument to fitness trackers, as we found no significant relationships between users' PFI disclosure habits and all measures of privacy concerns. Future research should explore the underlying reasons for this seeming lack of concern to determine whether it stems from apathy, lack of knowledge of potential harms, or something else.

## **5.2 Opportunities for Increased User Awareness of Privacy and PFI**

Findings from our study identify opportunities for cross-sector partnerships, such as the one between Fitbit and the Center for Democracy & Technology [9], to approach this privacy challenge. First, our analyses revealed a strong positive correlation between users' general privacy concerns, their mobile data concerns, and how sensitive they rate their PFI. Likewise, users who publicly shared PFI expressed greater concerns about how their mobile data is used. Thus, the more users care about privacy in general—and the more they engage in sharing activities that might jeopardize their privacy—the more concern they have about PFI. Fitness tracking companies must find ways of easing anxiety over privacy if they wish to have users increasingly engage in information sharing activities on their platforms. Partnering with organizations that focus on privacy research is one way for them to do so.

Few regulations exist to constrain companies from sharing PFI with third parties. While the EU's General Data Protection Regulation explicitly protects health data [11], U.S. law does little to regulate or protect the collection and use of PFI [6, 27]. Companies see this data as valuable from a monetary and research perspective and use it accordingly. People who use fitness trackers and seek to protect their privacy may wrongly assume that the law protects it. Our analyses of users' (lack of) privacy policy knowledge suggests a need for greater education and outreach to users. This can include a more robust explanation of user-controlled privacy settings during onboarding, contextual explanations of how adjustments to device settings might affect data collection and flows, or regular communication to users reminding them of their current privacy settings.

## **6 Limitations and Conclusion**

We must note some limitations to this research. First, while recruitment methods (random sampling) were designed to minimize response bias, the sample is significantly more educated than the general population and likely more than the population of fitness tracker users. This could introduce bias related to data valuation and internet skills. The sample was also significantly skewed toward female users, and existing research has found that women both share more online than men and have greater privacy concerns. Finally, this data collection comes from a one-time



survey, meaning our analyses can only identify correlations between variables and not causation. That said, because of the lack of empirical research on the privacy and security issues around fitness trackers, we believe the findings presented here provide useful insights to guide future theoretically driven and design-based studies.

Emerging technologies provide new opportunities for users to learn about themselves, meet and interact with new and existing friends, and explore ways to enhance their well-being. However, these technologies—and the associated data generated from their use—also bring challenges to managing individual privacy. In this paper, we argue that more attention should be devoted to considering the privacy implications of fitness trackers and other wearable devices that collect large amounts of data about users’ movement and health. As boyd and Crawford [4] note in their work on the challenges of big data, PFI is neither objective nor a “fix” for health-related problems. We are entering a time when PFI will be used to evaluate healthcare incentives, court cases, and more. Users must recognize how this data can be used against them, and companies should take steps to teach users to protect themselves.

## 7 References

1. Acquisti A, Gross R (2006) Imagined communities: awareness, information sharing, and privacy on the Facebook. In: Danezis G, Golle P (eds) PET 2006. LCNS, vol. 4258. Springer, Heidelberg, pp 36–58. doi:10.1007/11957454\_3
2. Ball K, Di Domenico ML, Nunan, D (2016) Big data surveillance and the body-subject. *Body & Society* 22(2):58–81. doi: 10.1177/1357034X15624973
3. Barnes SD (2006) A privacy paradox: social networking in the United States. *First Mon* 11(9).
4. boyd d, Crawford K (2012) Critical questions for big data: provocations for a cultural, technological, and scholarly phenomenon. *Info, Comm & Society* 15(5): 662–679. doi:10.1080/1369118X.2012.678878
5. boyd d, Hargittai, E (2010) Facebook privacy settings: who cares? *First Mon* 15(8).
6. Christovich M (2016) Why should we care what Fitbit shares: a proposed statutory solution to protect sensitive personal fitness information. *Hastings Comm/Ent Law J* 38:91–116.
7. Clawson J et al. (2015) No longer wearing: investigating the abandonment of personal health-tracking technologies on Craigslist. In: *Proc of UbiComp ‘15*. ACM, New York, pp 647–658. doi:10.1145/2750858.2807554
8. Crawford K, Lingel J, Karppi T (2015) Our metrics, ourselves: a hundred years of self-tracking from the weight scale to the wrist wearable device. *Euro J Cultural Studies* 18(4–5):479–496. doi:10.1177/1367549415584857
9. De Mooy M, Yuen, S (2016) *Toward Privacy Aware Research and Development In Wearable Health*. Center for Democracy and Technology, Washington.
10. Earp JB, Anton AI, Aiman-Smith L, Stufflebeam WH (2005) Examining internet privacy policies within the context of user privacy values. *IEEE Trans on Eng Mgmt* 52(2):227–237. doi:10.1109/TEM.2005.844927
11. European Union (2016) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data. *Official J of Euro Union* 119:1–88.
12. Fitbit (2016) Fitbit Privacy Policy. <http://www.fitbit.com/legal/privacy-policy>
13. Fox S, Duggan M (2013) *Tracking for Health*. Pew Research Center, Washington.
14. Fritz T, Huang EM, Murphy GC, Zimmermann T (2014) *Persuasive technology in the real*

- world: a study of long-term use of activity sensing devices for fitness. In: Proc. CHI '14. ACM, New York, pp 487–496. doi:10.1145/2556288.2557383
15. Gorm N, Shklovski I (2016) Sharing steps in the workplace: changing privacy concerns over time. In: Proc. CHI '16. ACM, New York, pp 4315–4319. doi:10.1145/2858036.2858352
  16. Gorm N, Shklovski I (2016) Steps, choices and moral accounting: observations from a step-counting campaign in the workplace. In: Proc. CSCW '16. ACM, New York, pp 148–159. doi: 10.1145/2818048.2819944
  17. Hargittai E, Hsieh YP (2012) Succinct survey measures of web-use skills. *Soc Sci Comput Rev* 30(1): 95–107. doi:10.1177/0894439310397146
  18. Hargittai E, Marwick A (2016) “What can I really do?” explaining the privacy paradox with online apathy. *Int J Comm* 10: 3737-3757.
  19. Ho J-J, Novick S, Yeung C. (2014). A snapshot of data sharing by select health and fitness apps. Federal Trade Commission, Washington.
  20. Jawbone (2014) Jawbone UP Privacy Policy <https://jawbone.com/up/privacy>
  21. Klasnja P et al. (2009) Exploring privacy concerns about personal sensing. In: Tokuda H, et al. (eds) *Pervasive 2009*. Springer-Verlag, Berlin Heidelberg, pp. 176-183. doi:10.1007/978-3-642-01516-8\_13
  22. Kumar P. (2016) Privacy policies and their lack of clear disclosure regarding the life cycle of user information. FS-16-04. AAI, Palo Alto, pp. 249-256.
  23. Lupton D (2016) *The quantified self: a sociology of self-tracking*. Polity, Cambridge, UK.
  24. McDonald AM, Cranor LF (2008) The cost of reading privacy policies. *ISJLP* 4:543–568.
  25. Motti VG, Caine K (2015) Users’ privacy concerns about wearables: impact of form factor, sensors and type of data collected. In: Brenner M., Christin N., Johnson B., Rohloff K. (eds) *FC 2015*. LNCS, vol 8976. Springer, Berlin, Heidelberg, p 231-244. doi:10.1007/978-3-662-48051-9\_17
  26. Nissenbaum H (2011) A Contextual Approach to Privacy Online. *Daedalus* 140:32–48. doi:10.1162/DAED\_a\_00113
  27. Patterson H (2013) Contextual Expectations of Privacy in Self-Generated Health Information Flows. In: *TPRC* 41. SSRN, Rochester, pp. 1-48. doi:10.2139/ssrn.2242144
  28. Peppet SR (2014) Regulating the internet of things: first steps toward managing discrimination, privacy, security & consent. *Texas L Rev* 93:85–178.
  29. Raij A, Ghosh A, Kumar S, Srivastava M (2011) Privacy risks emerging from the adoption of innocuous wearable sensors in the mobile environment. In: Proc. CHI '11. ACM, New York, pp 11–20. doi:10.1145/1978942.1978945
  30. Rooksby J, Rost M, Morrison A, Chalmers M (2014) Personal Tracking As Lived Informatics. In: Proc. CHI '14, ACM, New York, pp 1163–1172. doi:10.1145/2556288.2557039
  31. Shirer M, Llamas R, Ubrani, J (2016) IDC Forecasts Wearables Shipments to Reach 213.6 Million Units Worldwide in 2020. IDC.
  32. Solove, DJ (2013) Privacy self-management and the consent dilemma. *Harvard L Rev* 126: 1880–1903.
  33. Taddicken M (2014) The “privacy paradox” in the social web. *J Comput-Med Comm* 19: 248–273. doi:10.1111/jcc4.12052
  34. Vitak J (2016) A digital path to happiness? In: Reinecke L, Oliver MB (eds) *Routledge Handbook of Media Use and Well-Being*. Routledge, New York, pp 274–287.
  35. Xu H, Gupta S, Rosson MB, Carroll JM. 2012. Measuring Mobile Users’ Concerns for Information Privacy. In: Proc ICIS 2012. AIS, Atlanta, pp. 1-16.