COGITATIO

Media and Communication (ISSN: 2183–2439)
2021, Volume 9, Issue 4, Pages 145–157
https://doi.org/10.17645/mac.v9i4.4162

Article

Algorithmic Self-Tracking for Health: User Perspectives on Risk Awareness and Coping Strategies

Noemi Festic [1,*], Michael Latzer [1] and Svetlana Smirnova [2]

[1] Department of Communication and Media Research, University of Zurich, Switzerland;
E-Mails: n.festic@ikmz.uzh.ch (N.F.), m.latzer@ikmz.uzh.ch (M.L.)
[2] Department of Media and Communications, London School of Economics and Political Science, UK;
E-Mail: s.smirnova@lse.ac.uk

* Corresponding author

Submitted: 7 February 2021 | Accepted: 21 September 2021 | Published: 18 November 2021

Abstract
Self-tracking with wearable devices and mobile applications is a popular practice that relies on automated data collection and algorithm-driven analytics. Initially designed as a tool for personal use, a variety of public and corporate actors such as commercial organizations and insurance companies now make use of self-tracking data. Associated social risks such as privacy violations or measurement inaccuracies have been theoretically derived, although empirical evidence remains sparse. This article conceptualizes self-tracking as algorithmic-selection applications and empirically examines users' risk awareness related to self-tracking applications as well as coping strategies as an option to deal with these risks. It draws on representative survey data collected in Switzerland. The results reveal that Swiss self-trackers' awareness of risks related to the applications they use is generally low and only a small number of those who self-track apply coping strategies. We further find only a weak association between risk awareness and the application of coping strategies. This points to a cost-benefit calculation when deciding how to respond to perceived risks, a behavior explained as a privacy calculus in extant literature. The widespread willingness to pass on personal data to insurance companies despite associated risks provides further evidence for this interpretation. The conclusions—made even more pertinent by the potential of wearables' track-and-trace systems and state-level health provision—raise questions about technical safeguarding, data and health literacies, and governance mechanisms that might be necessary considering the further popularization of self-tracking for health.

Keywords
algorithmic selection; coping strategies; mHealth; risk awareness; self-tracking apps; self-quantification; societal risks; user perception; wearables

Issue
This article is part of the issue "Algorithmic Systems in the Digital Society" edited by Sanne Kruikemeier (University of Amsterdam, The Netherlands), Sophie Boerman (University of Amsterdam, The Netherlands) and Nadine Bol (Tilburg University, The Netherlands).

1. Introduction

Algorithms are shaping many domains of our datafied lives, from the curation of news content to recommendations for what to buy. Self-tracking for health is no exception: this digital variant of self-surveillance is performed with the help of wearable devices (e.g., sports bracelets, smart jewelry) and mobile applications. It typically involves continuous data collection, storage, and analysis, which results in algorithmically-derived health recommendations, quasi-human motivational communication, and competitive benchmarking against peers. While self-trackers measure various aspects of their lives, the central focus of this article is on health, fitness, and

wellness tracking, which revolves around measuring and analyzing aspects of physical and mental well-being (e.g., sleep, diet, stress) and athletic performance.

In the last decade, self-tracking has grown exponentially in popularity and reach. In 2020, close to half a billion wearables were in use worldwide. The market of related mobile applications is highly concentrated: From more than 300,000 healthcare apps available, 36 account for more than half of all downloads (estimates by IMS Institute for Healthcare Informatics, 2015). Similarly, the market for wearables is split between five dominant players—Apple, Xiaomi, Fitbit, Samsung, and Huawei—accounting for nearly two-thirds of devices sold (Statista, 2020).

Self-tracking applications have in common that they rely on *algorithmic selection*, defined as a special kind of selection that builds on the automated assignment of relevance to certain pieces of information (Latzer et al., 2016). Risks that can be associated with the employment of algorithmic selection in widespread online services are receiving much public and academic attention. Personalized algorithmic selection shapes the practice of self-trackers in multiple and unknown ways. The self-tracking industry has developed a persuasive narrative that values self-optimization, personalization, prediction, and self-management of health. Not least owing to the opacity of these applications and the sensitive, health-related data they use, self-tracking applications have come under public scrutiny. A glance at the historical evolution of the adoption of self-tracking applications reveals that the need for a debate on their risks and benefits has amplified: While such applications were initially designed for personal use only and data was maybe shared with peers on social networks for comparison and motivation, the stakes for users have dramatically increased. A rapidly growing number of public and corporate actors are promoting the use of these services, using the data and linking financial benefits to achieving certain objectives, thereby exacerbating the potential for a variety of social risks: Self-tracking applications have not only been shown to be of dubious scientific quality (Mercurio et al., 2020), but the industry is also poorly regulated, especially when it comes to handling personal data. The European General Data Protection Regulation (GDPR) has, for instance, been assessed as ineffective in adequately accounting for the fast-paced evolution of self-tracking practices (Marelli et al., 2020). Consequently, different governance options such as self-help protection behaviors by users are likely to play an important role in coping with the risks associated with algorithmic-selection applications for health self-tracking (Ireland, 2020). Coping strategies allow users to exert agency against the "panoptic practices" that companies apply (De Certeau, 1984): By monitoring, measuring, and controlling internet user data, they transform their users into measurable types and classify them based on their habitus that mirrors different aspects of their social disposition. Thereby, these internet platforms and services co-construct users' realities by "mirroring their social dispositions in the form of scorings, recommendations, search results or advertisements" (Latzer & Festic, 2019, p. 10). In the context of self-tracking applications, this specifically involves health-related recommendations or scorings, which have an influence on the users' perceptions of themselves and the world. This article defines coping strategies as internet users' counterparts to the companies' data collection and analysis strategies that induce certain risks for users. This understanding is related to Kitchin and Fraser's (2020) notion of "slow computing," which captures a way for users to regain autonomy over their digital lives in the face of ever-accelerating and increasingly encompassing data grabbing infrastructures on the internet. In the context of self-tracking applications, one exemplary risk, induced by their algorithmic nature, is the inaccurate measurements and resulting fitness recommendations that are scientifically unfounded and inapt for the respective user (Depper & Howe, 2017). Double-checking measurements with the aid of different tools is one possible coping strategy for users to regain autonomy (Kitchin & Fraser, 2020) and mitigate risks.

Extant research has not sufficiently studied self-tracking for health in the wider context of the social power of algorithms—although personalized algorithmic selection lies at the core of these applications and provides a helpful framework to investigate associated risks. The call for more representative empirical research from a user perspective (see Albrecht, 2016) has so far not been sufficiently answered. Against the conceptual backdrop of algorithmic selection, this article first contributes to filling these gaps by empirically investigating how aware self-trackers are of the risks associated with health applications and how they cope with them. Second, this article contributes to the understanding of the coping behavior observed. While we know little about risk awareness and coping strategies by individual users in the realm of self-tracking for health, scholarship on online privacy lends a helpful concept to consider: the privacy calculus, which describes cost-benefit calculations that internet users perform when negotiating their online behavior in response to perceived risks to their privacy (see Baruh et al., 2017). As we described above, social risks associated with self-tracking applications for health have been linked to the growing interest of corporate actors in this data. Using the example of sharing personal self-tracking data with insurance companies as a case study, this article empirically explores self-trackers' behaviors in response to risks and in light of benefits attached to sharing personal data. In combination with the first aim introduced above, this article contributes to our (empirical) understanding of the relationship between risk awareness and coping strategies, which could help to shed light on how self-trackers evaluate risks and deal with them.

To fulfil these tasks, this article draws on representative survey data from Switzerland, a highly digitized

country where 95% of the population use the internet and self-tracking applications for health are gaining popularity: while 29% of internet users reported using them in 2017, this share has risen to 41% in 2021 (Latzer et al., 2021).

This article begins by conceptualizing self-tracking applications for health as algorithmic-selection applications. We then present a review of the existing literature on associated risks and coping strategies and introduce the concept of the privacy calculus. After the methodological approach is explained, the results section outlines our empirical insights. Lastly, the findings are interpreted and we conclude by identifying further research directions.

2. Theoretical Background and Review of Relevant Literature

2.1. Self-Tracking as an Algorithmic-Selection Application

While research on self-tracking applications and their implications is emerging, engagement with literature on algorithms often remains superficial. Bol et al. (2019, p. 2) are some of the few who explicitly address the personalized nature of self-tracking applications by referring to "customization," which captures users' "ability to *self*-tailor…mobile health app content and features." While this user-driven self-tailoring as an affordance of self-tracking applications is included in our understanding of algorithmic selection as introduced below, it goes beyond user-initiated personalization and also includes the automated selection of contents that is outside of what users are aware of and can influence.

In general, algorithmic selection describes the process that transforms *input* with the help of automated computational procedures (*throughput*) into *output* (Cormen et al., 2009; Latzer et al., 2016). Figure 1 illustrates how this model aids to understand the functionality of self-tracking applications for health.

The starting point for this algorithmic-selection process embedded in widely used self-tracking applications for health is a user request (e.g., for a training plan) paired with available user characteristics such as personal demographic factors (e.g., gender, age), user behaviors (e.g., levels of physical activity, diet), and personal goals. These user requests and characteristics combined with a basic data set are used as input by these applications to derive output that ranges from graphs of daily step counts and motivational reminders to be physically active, to an alarm being triggered automatically during a specific stage of sleep to ease waking or a prompt to meditate in response to rising stress levels. The inner functioning of algorithmic-selection applications (throughput) remains largely obscure to users, can form the basis for different biases, and relies on computational operations (Latzer et al., 2016). This process of algorithmic selection functions as follows in the context of a specific type of self-tracking for health: Based on data about fitness levels, past running experience, and age (input), a health application and its designated algorithms (throughput) can identify the ideal training strategy and make personalized recommendations to prepare someone for a marathon (output).

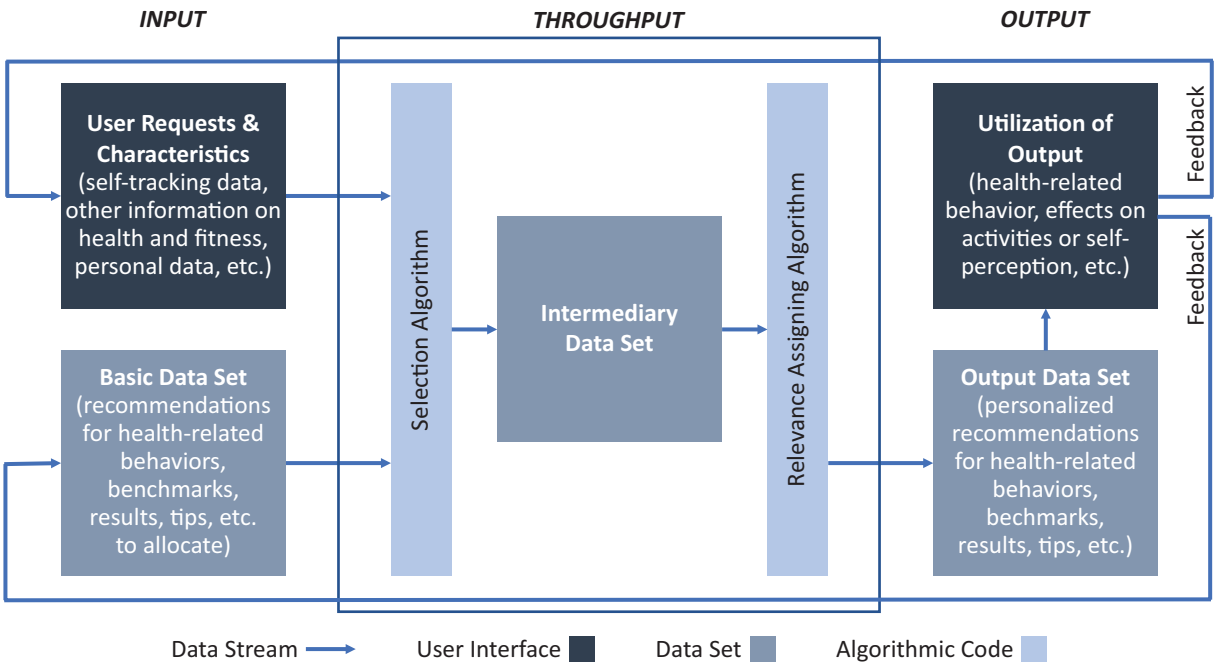

Figure 1. Input–throughput–output model of algorithmic selection applied to self-tracking applications for health and fitness. Source: Adapted from Latzer et al. (2016).

This conceptual understanding of self-tracking applications for health will guide and structure the following considerations on related risks and coping strategies.

2.2. Algorithmic Self-Tracking: Risks and Coping Strategies From a User Perspective

The central arguments of critical scholarship regarding users' risk awareness and coping strategies can be summarized as follows.

While there has been much discussion identifying the *risks* of the spread of algorithmic-selection applications in all domains of life, empirical evidence is only just emerging. Most of the critique directed at algorithmic-selection applications for self-tracking is derived from theoretical reasoning and does not rely on empirical data from a user perspective (for a critique of visualization and analytics, see Fawcett, 2015; and Hepworth, 2017; for a critique of Western-centered, ableist assumptions embedded in tracking systems, see Elias & Gill, 2018; Elman, 2018; Mills & Hilberg, 2020). Risks such as the spread of misinformation (Albrecht, 2016) or use-errors and resulting wrong treatments (Israelski & Muto, 2012) have also only been theoretically derived so far. In their SWOT (strengths, weaknesses, opportunities, and threats) analysis, Li and Hopfgartner (2016) recognize over-tracking and erosion of privacy as weaknesses and negative societal consequences in terms of privacy as a threat of self-tracking applications.

Lack of transparency, particularly in relation to medical evidence, is of special concern given the health-focused nature of the practice. There is robust empirical evidence revealing that expert involvement and adherence to medical evidence is low for various health applications (Chen et al., 2015; Subhi et al., 2015) and longitudinal comparisons reveal that smartphone health apps are not improving in terms of safety or quality (Mercurio et al., 2020). Empirical evaluations of self-tracking applications for weight loss (Mercer et al., 2016) concluded that goals were not adequately backed up by science, sponsorships were not disclosed, sources of information were not cited, and major behavior change techniques were missing.

Qualitative, user-centered research has revealed a variety of self-trackers' concerns, especially considering the output of self-tracking devices: accuracy of data and analysis, inability to edit erroneous entries, weak analytics, and unusable feedback. To exemplify, the accuracy of measurements, the universality of benchmarks (e.g., 10,000 steps or eight hours' sleep at night) and embedded heteronormative assumptions have been sources of concern (Barassi, 2017; Depper & Howe, 2017; Matthews et al., 2017).

Furthermore, privacy remains a significant issue that has been explored in relation to the practice. The risks related to privacy include data trading and access by third parties, lack of legal protection merited by the sensitive nature of data, extensive collection of data irrelevant to the functioning of the application, and users' inability to foresee the extent of data collected on them (Cyr et al., 2014; Daly, 2015; Katuska, 2019). In regard to privacy-related risks, earlier studies showed that self-trackers underestimated the amount of data they shared with companies and lacked knowledge of the conditions of data storage, sharing, and retention, as well as privacy policies, and what they could do to minimize unwanted privacy invasions (Goodyear et al., 2019; Lupton & Michael, 2017; Spiller et al., 2017; Vitak et al., 2018). Recent studies have also suggested that while self-trackers might know about their data being used and believe that harm may come from that (e.g., ovulation data used by an employer for human resources planning), they also think that such scenarios are unlikely to affect them personally (Alqhatani & Lipford, 2019; Gabriele & Chiasson, 2020), which is why they might not engage in mitigation strategies.

As one of the few studies with large-scale survey data in the field, Grzymek and Puntschuh (2019) found across all EU member states that people have little awareness of the potential of algorithms to assist in diagnosing diseases and there was significant concern about medical decisions made by algorithms.

In the realm of coping strategies, existing scholarship suggests that self-trackers use a range of techniques to deal with concerns related to their self-tracking. For example, ethnographic studies have explored how intermediation and reflection are employed by users to cope with problems of inaccuracy, data incompletion, and device breakage (Pink & Fors, 2017a, 2017b; Pink et al., 2017). Alternatively, multiple qualitative studies have illustrated how self-trackers engage in reframing their data, paying selective attention to some data points, or resisting the use of devices as designed (Gorm & Shklovski, 2019; Mopas & Huybregts, 2020; Sjöklint et al., 2015). Other than general research on privacy protection behavior, there is, to the best of our knowledge, no quantitative empirical evidence on how users cope with potential risks in the context of self-tracking applications.

Overall, there is a lack of representative, nation-level data that addresses how aware self-trackers are of various risks and how they cope with them. The discussion of related risks has so far lacked conceptual clarity and not sufficiently taken into account the algorithmic nature of self-tracking applications. When assessing the current state of research with the input-throughput-output model of algorithmic selection in mind, it becomes apparent that most research on risks and coping strategies is limited to the output dimension. We derive the following two research questions from the extant literature for this article:

> RQ1: How aware are Swiss self-trackers of the risks associated with the applications they use and how do they cope with them?

RQ2: How is risk awareness related to the employment of coping strategies among Swiss internet users?

Since the process of personalized algorithmic selection, which underlies the commonly used self-tracking applications, relies heavily on personal data, this topic is intertwined with critical scholarship on online privacy, which has been concerned with questions about how worried internet users are about their data online and how they attempt to protect it. From an (empirical) communication science perspective, privacy-related risks are among those studied most extensively in terms of internet users' awareness and their behavioral and cognitive reactions to it. While early research in the field revealed a seemingly paradoxical relationship between privacy concerns and behavior (e.g., Barnes, 2006; Norberg et al., 2007), more recent studies have replaced this image of ignorant internet users who do not protect their personal data online despite being concerned about their privacy with one where they constantly perform cost-benefit calculations: People engage in online behaviors if the benefit of disclosing personal data or not engaging in protective behaviors, respectively, outweighs the cost (Baruh et al., 2017). Bol et al. (2018) provided experimental empirical evidence for such a "cost-benefit trade-off" in the context of health websites, indicating that both privacy risk perception and perceived benefits were associated with the participants' willingness to self-disclose personal data. When it comes to protection behavior, extant research has shown that—based, for instance, on protection motivation theory—low levels in protective behaviors may be explained by a low perceived self-efficacy despite of high perceived severity of related threats (Boerman et al., 2018). For a convenience sample, Kordzadeh et al. (2016) found empirical proof of a privacy calculus effect on self-disclosure in virtual health communities. Dienlin and Metzger (2016) expanded the privacy calculus framework to include not only self-disclosure, but also self-withdrawal (e.g., deleting posts)—accounting for internet users' co-existing desires for disclosing and withholding information predicted by communication privacy management theory (see Petronio, 2012)—and found empirical evidence for this extended model for a representative sample of adult Facebook users in the US.

Applying this calculus logic to the research interest at hand provides indications for engaging in self-tracking and not applying coping strategies despite being aware of potential risks because the benefits outweigh the cost. A specific, real-world example for these cost-benefit calculations is provided by the rising interest of insurance companies in self-tracking data, offering financial benefits in exchange for personal tracking data. Sharing highly sensitive data on one's health with a third party through an opaque algorithmic-selection application despite a multitude of risks that can arise from this behavior in the short and long run can arguably only be explained if the perceived benefits of this behavior (i.e., a financial compensation) exceed the perceived cost (i.e., any harms from the risks). We use insurance settings as a case study to explore if user behavior is consistent with a calculus logic in the context of self-tracking applications by answering the following question:

RQ3: To what extent are Swiss self-trackers willing to share their data with insurance companies for financial benefit?

An extensive body of research has repeatedly shown that traditional societal fault lines are replicated in the digital space: Male, younger, more affluent members of a society tend to reap more benefits from their internet use and are able to deal with associated risks better (see van Dijk, 2020). Therefore, this article analyzes risk awareness and coping strategies in the realm of self-tracking for health against this backdrop of sociodemographic differences, too.

3. Method

3.1. Data Collection

The empirical section of this article relies on a representative survey of Swiss internet users conducted between October 2018 and February 2019. The survey covered the significance of algorithmic selection for everyday life (Latzer et al., 2020) and included questions on the frequency and purpose of tracking device use, attitudes, risk awareness, and coping strategies, as well as on the willingness to share personal data with insurance companies for financial benefit.

The survey was conducted as part of a larger project in which we also collected internet use tracking data: All participants, who were actively recruited from an existing mobile tracking panel by the LINK Institute, received installation instructions for a passive metering software for their desktop or laptop device (provided by Wakoopa) at the beginning of the field phase. We collected tracking data on private mobile and desktop or laptop devices. The following variables were collected: URL of visited webpages or name of visited app, duration and time of the visit, device, and operating system. On completion of the tracking, the participants received an invitation to complete the online survey questionnaire. While the research questions of this article will be empirically answered with the survey data, the sample description below includes relevant results from the tracking data on the use of self-tracking applications to provide context for the interpretation of the survey results.

3.2. Sample

The original survey sample consisted of $N_{participants}$ = 1,715. As part of the aforementioned questionnaire, the

participants were asked to evaluate the relevance they assign to various online and offline services and activities (e.g., self-tracking applications, offline contacts, search engines) for obtaining information on their personal health. They rated how relevant they believed each of these sources to be for their health information on a scale from 1 = *not at all relevant* to 5 = *very relevant*. For this study, we used a subsample of those participants who assigned some relevance (>1) to an application or device that automatically monitors their fitness or health (N = 716).

The tracking sample consisted of $N_{\text{tracked events}}$ = 13,486,101. We compiled a list of 675 websites and applications which allow their users to automatically track their fitness and health or connect to a wearable device (e.g., a watch) by systematically searching the Apple App Store, Google PlayStore, and Microsoft Store, and by conducting an extensive Google search. By searching the tracking data for occurrences of these app and website names and extracting these cases from the data set, we filtered all uses of self-tracking applications for health from the tracking data set to get descriptive results on the use of these applications in the sample.

Before addressing the guiding research questions, descriptive statistics on self-trackers in Switzerland are presented. Based on the survey data, one in 10 users of tracking applications (11%) reported using such services several times a day and a quarter (25%) reported using them daily. The majority used them either at least weekly (32%) or less than monthly (29%). There were no major differences in the frequency of use of these applications with regard to gender, age, or education. The most common purposes that the respondents reported using their devices for (multiple responses were possible) were fitness and sports (79%), sleep (28%), nutrition (16%), and documenting symptoms associated with a disease (11%).

Of all tracked events, .5% (N = 65,753) were uses of self-tracking applications. We identified 24 unique services used. Table 1 reveals the 10 most used self-tracking applications in descending order (as a share of all tracked use events of self-tracking applications for health). As becomes apparent from the most widespread services, Swiss internet users who engage in self-tracking through mobile applications almost exclusively track their physical activity (e.g., steps, training) and potentially related vital data (e.g., heart rate).

Table 1. Most used self-tracking applications in Switzerland (based on tracking data).

Name	% of self-tracking events
Fitbit	93.14% (N = 61,243)
Google Fit	3.14% (N = 2,062)
TomTom Sports	<.01% (N = 562)
Mi Fit	<.01% (N = 550)
Beurer HealthManager	<.01% (N = 357)
VeryFitPro	<.01% (N = 283)
Huawei Health	<.01% (N = 197)
Sports Tracker	<.01% (N = 136)
Visana-App	<.01% (N = 81)
FunDo Pro	<.01% (N = 57)

These descriptive characteristics of the self-tracking population are important to be kept in mind when interpreting the subsequent empirical answers to this article's guiding research questions.

3.3. Survey Measures

Based on existing literature introduced in Section 2.2, risk awareness was measured for four key risks: The respondents answered on a five-point Likert scale (1 = *do not agree at all*, 5 = *totally agree*) how strongly they agreed that they used their tracking device too much (overuse), were uncertain about the accuracy of their device's measurements (measurement inaccuracy), did not know how their device calculated the results it provides (lack of transparency), and were concerned about what happens with their data (loss of control over data).

To measure coping strategies, the respondents answered how often (1 = *never*, 2 = *rarely*, 3 = *sometimes*, 4 = *frequently*) they checked the accuracy of the measurements by comparing them to other results (checking measurements), how often they did not blindly trust their tracking device's results but actively thought about their meaning (reflecting on results) and how often they consciously refrained from using their tracking device (conscious non-use). Some of these risk awareness and coping strategy items can be clearly situated at one level in the input-throughput-output model of algorithmic selection (e.g., lack of transparency at the throughput level; checking measurements at the output level), others transcend this categorization and concern multiple levels. The goal of this empirical approach was to cover all levels in the measurement of both risk awareness and coping strategies.

The respondents indicated their willingness to share personal data with their insurance company by stating their agreement on a five-point Likert scale (1 = *strongly disagree*, 5 = *strongly agree*) to the following statement: "I would be willing to give my insurance access to my data if I received financial advantages for doing so." While potential risks (i.e., the cost) of using self-tracking applications were not explicitly part of the question, they were made salient to the respondents through multiple questions on risk awareness placed prior in the questionnaire.

The respondents were further asked to report their gender (female, male) as well as their age in years, which was recoded into four groups (16–29, 30–49, 50–69, 70–85) for certain analyses below. They also reported their completed levels of educational attainment, which were recoded into three levels: individuals whose highest completed education level was compulsory schooling were assigned the value *low* and those with tertiary qualifications were assigned the value *high*.

3.4. Data Analysis

Data analysis for RQ1 and RQ3 relied on descriptive statistics. To test the relationship between risk awareness and coping strategies (RQ2), we estimated a path model with the lavaan package in *R* (Rosseel, 2012). For the path model, we used all items separately with the raw scales introduced in Section 3.3. This allowed a detailed analysis of the relationship between different risks and coping strategies. A positive relationship between a risk awareness and a coping strategy item in the model can therefore be interpreted as follows: "stronger agreement with a risk is associated with applying coping strategies more frequently." We freely estimated the covariances between the items for risk awareness and coping strategies, respectively (the script for the analysis and further results are available in the Supplementary Material).

4. Results

The following sections detail our empirical results for the three research questions based on the survey data.

To answer RQ1, we address how widespread the awareness of risks associated with self-tracking applications and the employment of coping strategies is. Figure 2 shows the distribution of responses to the survey questions about risk awareness (*N* = 716).

Overall, awareness of the surveyed risks was low: About four out of ten (39%) to seven out of ten (69%) self-tracking users were not concerned about the risks associated with their self-tracking practice. For overuse and lack of transparency, "do not agree at all" was the modal category: About half of the internet users did not agree at all that they use their tracking device too much (48%) and disagreed or fully disagreed that they do not know how their application calculates health results (54%). Loss of control over data and measurement inaccuracy were different in that the responses were roughly equally distributed: 27% and 30%, respectively, agreed (4) or fully agreed (5) with the statements. Users of self-tracking applications felt more at risk of losing control over their data or being presented with inaccurate measurements than they feared overusing their device or not knowing how their results are calculated.

The application of coping strategies, which can counteract these risks, was distributed as shown in Figure 3 (*N* = 716).

Figure 3 shows that the practice of cross-checking tracking measurements was uncommon: almost half of users (46%) never do this and only a quarter (24%) engage in the practice at least sometimes. One third (33% and 34%, respectively) of self-trackers never consciously decide to not use their tracking device or engage in this practice at least sometimes. Reflecting on one's

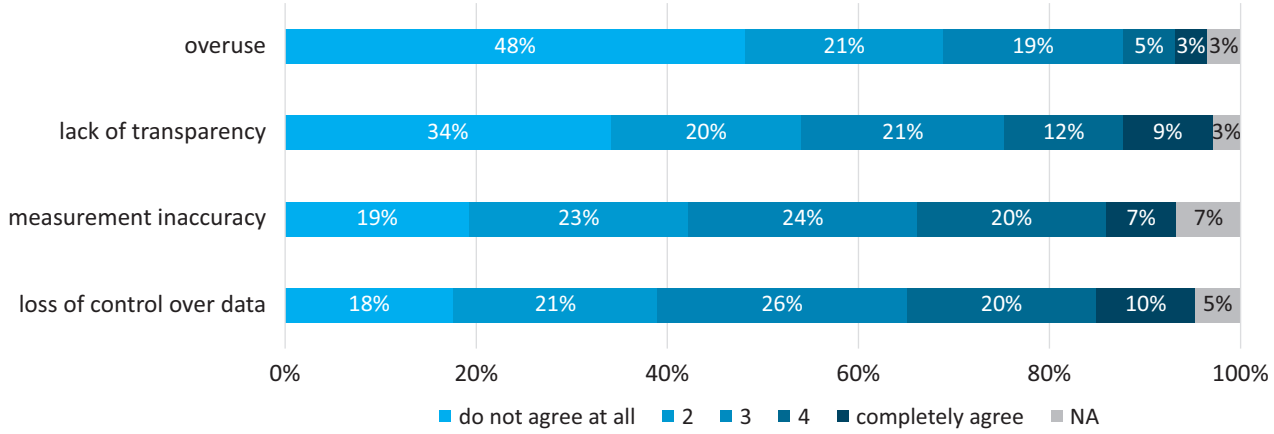

Figure 2. Distribution of indicators of risk awareness.

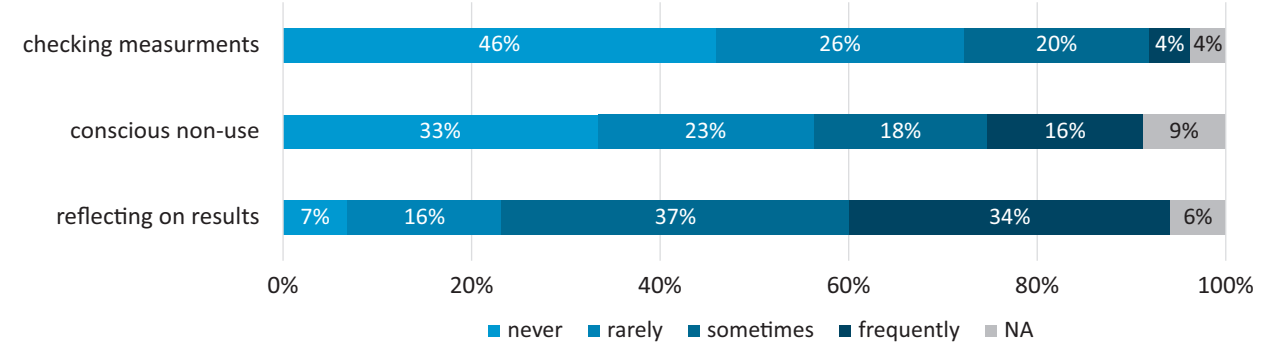

Figure 3. Distribution of indicators of coping strategies.

results was the most widespread coping strategy: only 7% never do this, while 71% of users engage in this practice at least sometimes.

To answer RQ2, we assessed the relationship between risk awareness and coping strategies. The awareness of specific risks and the frequency with which self-tracking users employed coping strategies was only weakly correlated both for the single items and for the two respective mean score indices (for further results see the Supplementary Material).

Figure 4 depicts a path model for the relationship between risk awareness and coping strategies. While gender and education were not significantly related to the two variables of interest, age was added as a control variable.

The model fit the data well: $\chi^2(3, N = 716) = 3{,}433$ ($p = .330$), $\chi^2/df = 1{,}144$, CFI = .999, TLI = .991, RMSEA = .014, SRMR = .012. Overall, the awareness of risks related to self-tracking devices explained only very small proportions of the variance in coping strategies. While there were some indications for a positive association between risk awareness and coping strategies—i.e., awareness of the risk to overuse self-tracking was positively associated with double-checking measurements and awareness of the risk of losing control over one's data was positively associated with consciously not using self-trackers—these effects were weak. Age was only significantly (and negatively) associated with the awareness of the risk of measurement inaccuracy.

While the application of coping strategies as a protection behavior does not appear to be meaningfully explained by risk awareness, this article also investigates whether Swiss self-trackers are willing to self-disclose their self-tracking data to insurance companies despite having been made aware of associated risks. RQ3 can be empirically answered as follows: 43% of tracking-device users in Switzerland agreed (4) or completely agreed (5) that they would generally be willing to share their data with their insurance company if they received financial advantages for doing so. This willingness was relatively uniformly distributed across all societal groups (see Figure 5). There was a weak tendency for older people and females to be less willing to share their data. Female self-trackers aged 70 and over reported the lowest willingness to share their data with an insurance company. There were no differences regarding education.

The following section discusses our empirical findings and details how they contribute to answering our research questions.

5. Discussion

Overall, our results reveal that awareness of risks associated with algorithmic self-tracking applications is relatively low and coping strategies are not regularly used. In the realm of risks, the results highlight that users perceive some risks—inaccuracy of measurements and losing control over their data—as more pertinent than others. However, even for those risks, less than a third of Swiss self-trackers reported awareness (RQ1). It is not necessarily the case that those who are more aware of risks engage in coping strategies more often (RQ2). This seemingly paradoxical result could be explained by a "calculus'' logic: Although Swiss self-trackers are somewhat aware of the risks they face, they still engage in the practice and do not apply many coping strategies because they rate the benefits higher than potential risks. Their willingness to share their self-tracked data with insurance companies (when there are direct financial benefits attached) further reiterates the plausibility of this explanation (RQ3). This result extends the extant literature on the privacy calculus (see e.g., Masur, 2019), from which this calculus logic was derived, to other types of risks associated with a specific type of everyday internet use that is dominated by algorithmic selection: self-tracking for health. In accordance with Dienlin

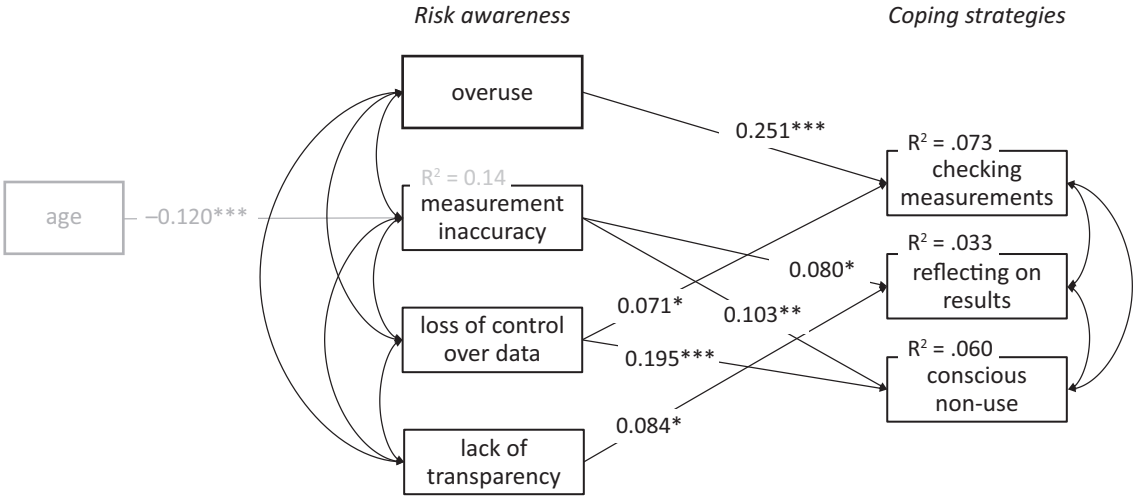

Figure 4. Path model: Risk awareness and coping strategies. Notes: Standardized estimates are shown; only significant paths are shown; ***$p < .001$, **$p < .05$, *$p < .1$

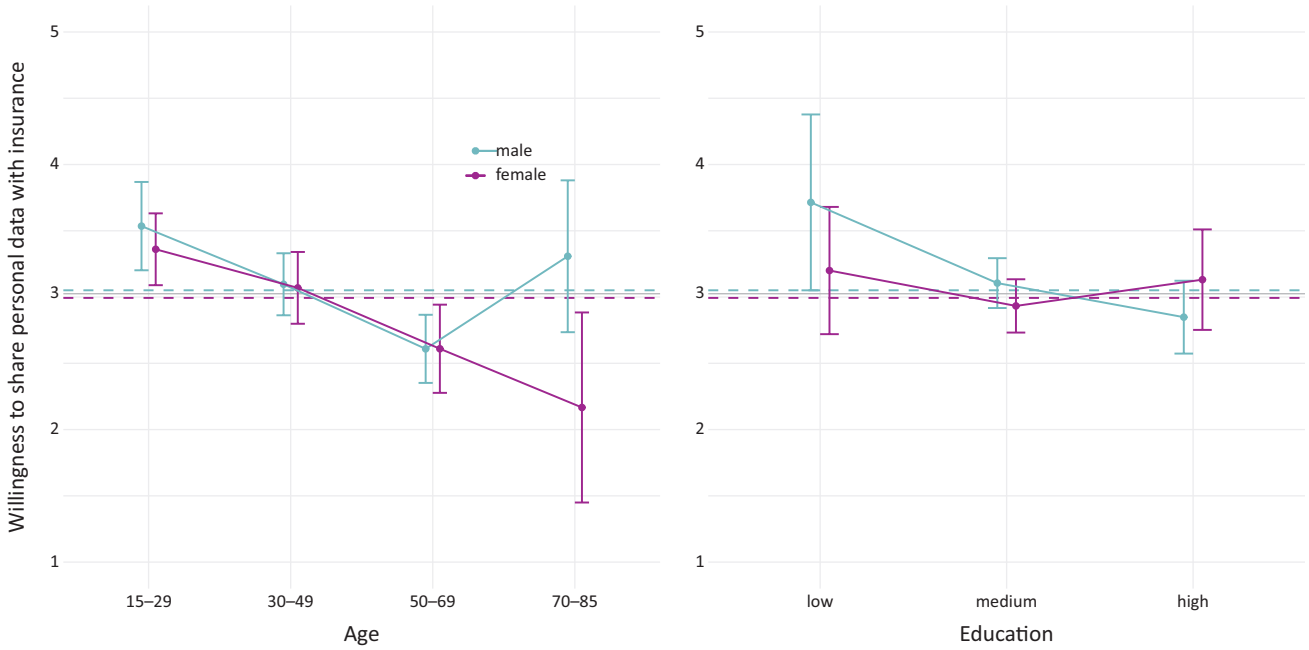

Figure 5. Willingness to share personal data with insurance company: Mean scores by gender, age, and education. Notes: Vertical bars represent 95% confidence intervals; horizontal lines represent overall (solid) and group means (dashed); Y-axis indicates means on a continuous scale (1 = *do not agree at all* to 5 = *completely agree*); *N* = 692.

and Metzger's (2016) empirical results, this effect was also likely present for coping strategies that reflect self-withdrawal behavior (i.e., conscious non-use).

From a public-policy perspective, these are important results to keep in mind when assessing the need for regulatory interventions to mitigate the possibility of certain risks occurring: While users may be familiar with some aspects of algorithmic selection and associated risks, this understanding does not deter them from engaging in the practice of self-tracking in their everyday lives. Alternative interpretations of this weak relationship could include skepticism about the efficacy of coping strategies (Boerman et al., 2018) or mediating effects of personality traits, internet skills, or more general concerns about being online. Our path model for the relationship between risk awareness and coping strategies (see Figure 4) also showed that coping strategies that are arguably effective in light of certain risks (e.g., conscious non-use as a coping strategy in response to awareness about the risk of overuse) were empirically not those most strongly associated with the respective risks. This provides further indications for the aforementioned interpretations and substantiates the need for further research on this relationship.

There are limitations to acknowledge when considering the results and implications of this study. Both survey and tracking data can be subject to biases such as effects of social desirability in surveys or the self-selection of people with certain personal characteristics into tracking samples. Another limitation concerns the list of risks included in this article. We examined a limited number of risks that we perceived as key, but future research should also consider emerging risks that have been associated with self-tracking, such as distorted self-perceptions (Strübing, 2021).

We found that existing research conceives self-tracking applications as a homogenous group. However, such applications and devices vary in the services they offer, the volume, type, and sensitivity of data they collect, the algorithms they employ, and the outputs they provide. Accordingly, the social risks we addressed in this article carry a different weight depending on the context of the self-tracking practice: While the potential risks of incorrect recommendations or data leaks for a chronically ill person relying on a self-tracking device for reminders of their medicine intake may be detrimental for their life chances, the effects of the same events in the context of a healthy person using a step counter are much less significant. This could be an additional, different explanation for the weak association between risk awareness and the application of coping strategies we found in our representative data set, which was almost exclusively composed of individuals who track arguably non-sensitive data (e.g., step counts) and where the potential for harm is therefore comparatively low. With this in mind, our data offer some specific indications that those who are chronically ill or require medical assistance are a group that future research should specifically focus on: Those in the sample who reported engaging in self-tracking to monitor symptoms in connection with a disease were more concerned about losing control over their data (38%, vs. 30% in the entire sample) and less willing to share their data with an insurance company for financial benefit (36%, vs. 43% in the

entire sample)—arguably because the potential harms are much more detrimental for them, even if their occurrence is unlikely. Future research should account for this diversity in self-tracking applications when investigating their uses, implications, and the need for governance interventions. In any circumstance, throwing all self-tracking applications into one basket and proposing generalized, one-size-fits-all explanations or solutions is unpromising for a realistic assessment of their harms and benefits. The identified tensions raise further research, normative, and regulation questions. For instance, it remains an open question if users would be more concerned about the implications of their self-tracking practice if their life chances were more transparently linked to its outcomes (e.g., by tracked data having an impact on premiums).

Examining users' understanding of algorithmic selection embedded in self-tracking applications and associated risks is becoming more pressing as the practice permeates deeper into formal medical settings and drives up the costs of opting out (Lupton, 2015). Today, dominant corporate quantification players are expanding their reach into organizational settings: For example, Fitbit, has developed a dedicated product that is marketed to employers, and a health insurance provider has integrated the use of Apple watches into their wellness plans (United Healthcare, 2021). Organizations (e.g., Target, Barclays, BP, Emory University) and nation-states alike (e.g., Singapore, the UK National Health Service) have initiated the integration of self-quantification into their health delivery operations. Results from more fine-grained studies will be particularly relevant in light of the fast-paced evolution of the adoption of self-tracking applications: from being mere tools for measuring health-related indicators for personal use only, they have more recently attracted the interest of powerful, profit-maximizing institutions that are looking to capitalize on individuals' self-tracking practices and are increasingly pervading private domains such as sleep, mental health, and family planning.

In terms of governance conclusions, we can derive from our results that self-help by individual internet users in the form of coping strategies alone is not a promising path forward when it comes to mitigating the risks associated with algorithmic self-tracking applications that apply panoptic practices. Is there a need for self-, co-, or state regulation and if so, how might the transnational nature of dataflows hinder such efforts? Should the functioning of algorithmic selection (throughput) be made more transparent? While there are attempts such as the mHealth App Trustworthiness checklist (van Haasteren et al., 2019) to systematically assess and improve the quality of self-tracking applications, these studies should take into account that algorithms are at the core of these applications and consider scholarship in the field of critical algorithm studies to advance these endeavors.

6. Conclusion

This article makes two central contributions: On the conceptual level, we have elaborated on the functionality of self-tracking as algorithmic-selection applications and discussed related risks and coping strategies. On the empirical level, we have provided hitherto missing representative evidence of the relationship between risk awareness and coping strategies. Based on tracking data, we also found evidence of a highly concentrated usage of self-tracking applications in Switzerland.

The findings highlight that users recognize some risks associated with algorithmic selection for shaping their practice; however, this awareness is sparse and mostly limited to the applications' input and output levels. The findings also suggest that users employ a limited range of coping strategies to mitigate these risks. Based on these conclusions, we argue that limited awareness of algorithmic functioning and the associated risks does not deter users from adopting self-tracking practices in their everyday lives. In that vein, this article also provides empirical indication for a cost-benefit calculus derived from the weak relationship between risk awareness and coping strategies as well as from the high willingness to share personal data with insurance companies. The blind spots in risk awareness and the toothless nature of coping strategies, however, call for further consideration as the practice continues to permeate medical, corporate, educational, legal, and nation-state settings. Our results substantiate the need for a more differentiated analysis of self-tracking applications, taking into account different types of applications, user groups, and data with different degrees of sensitivity.

Acknowledgments

This project received funding from the Swiss National Science Foundation.

Conflict of Interests

The authors declare no conflict of interests.

Supplementary Material

Supplementary material for this article is available at https://osf.io/ekjx9/?view_only=a513ba966d204966ac388079dfe84d62

References

Albrecht, U.-V. (Ed.). (2016). *Chances and risks of mobile health apps*. Hannover Medical School. https://doi.org/10.24355/dbbs.084-201210110913-73

Alqhatani, A., & Lipford, H. (2019). "There is nothing that I need to keep secret": Sharing practices and concerns of wearable fitness data. In H. R. Lipford (Ed.), *Proceedings of the fifteenth sympo-*

sium on usable privacy and security (pp. 421–434). USENIX. https://www.usenix.org/sites/default/files/soups2019_full_proceedings_interior.pdf

Barassi, V. (2017). BabyVeillance? Expecting parents, online surveillance and the cultural specificity of pregnancy apps. *Social Media + Society*, *3*(2), 1–10. https://doi.org/10.1177/2056305117707188

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday*, *11*(9). http://journals.uic.edu/ojs/index.php/fm/article/view/1394/1312

Baruh, L., Secinti, E., & Cemalcilar, Z. (2017). Online privacy concerns and privacy management: A meta-analytical review. *Journal of Communication*, *67*(1), 26–53. https://doi.org/10.1111/jcom.12276

Boerman, S. C., Kruikemeier, S., & Zuiderveen Borgesius, F. J. (2018). Exploring motivations for online privacy protection behavior: Insights from panel data. *Communication Research*, *48*(7), 953–977. https://doi.org/10.1177/0093650218800915

Bol, N., Dienlin, T., Kruikemeier, S., Sax, M., Boerman, S. C., Strycharz, J., Helberger, N., & de Vreese, C. H. (2018). Understanding the effects of personalization as a privacy calculus: Analyzing self-disclosure across health, news, and commerce contexts. *Journal of Computer-Mediated Communication*, *23*(6), 370–388. https://doi.org/10.1093/jcmc/zmy020

Bol, N., Høie, N. M., Nguyen, M. H., & Smit, E. S. (2019). Customization in mobile health apps: Explaining effects on physical activity intentions by the need for autonomy. *Digital Health*, *5*, 1–12. https://doi.org/10.1177/2055207619888074

Chen, J., Cade, J. E., & Allman-Farinelli, M. (2015). The most popular smartphone apps for weight loss: A quality assessment. *JMIR mHealth and uHealth*, *3*(4), Article e104. https://doi.org/10.2196/mhealth.4334

Cormen, T. H., Leiserson, C. E., Rivest, R. L., & Stein, C. (2009). *Introduction to algorithms* (3rd ed.). MIT Press.

Cyr, B., Horn, W., Miao, D., & Specter, M. (2014). *Security analysis of wearable fitness devices (Fitbit)*. MIT. https://pdfs.semanticscholar.org/f4ab/ebef4e39791f358618294cd8d040d7024399.pdf

Daly, A. (2015). The law and ethics of "self-quantified" health information: An Australian perspective. *International Data Privacy Law*, *5*(2), 144–155. https://doi.org/10.1093/idpl/ipv001

De Certeau, M. (1984). *The practice of everyday life*. University of California Press.

Depper, A., & Howe, P. D. (2017). Are we fit yet? English adolescent girls' experiences of health and fitness apps. *Health Sociology Review*, *26*(1), 98–112. https://doi.org/10.1080/14461242.2016.1196599

Dienlin, T., & Metzger, M. J. (2016). An extended privacy calculus model for SNSs: Analyzing self-disclosure and self-withdrawal in a representative U.S. sample. *Journal of Computer-Mediated Communication*, *21*(5), 368–383. https://doi.org/10.1111/jcc4.12163

Elias, A. S., & Gill, R. (2018). Beauty surveillance: The digital self-monitoring cultures of neoliberalism. *European Journal of Cultural Studies*, *21*(1), 59–77. https://doi.org/10.1177/1367549417705604

Elman, J. P. (2018). "Find your fit": Wearable technology and the cultural politics of disability. *New Media & Society*, *20*(10), 3760–3777. https://doi.org/10.1177/1461444818760312

Fawcett, T. (2015). Mining the quantified self: Personal knowledge discovery as a challenge for data science. *Big Data*, *3*(4). https://doi.org/10.1089/big.2015.0049

Gabriele, S., & Chiasson, S. (2020, April 25–30). *Understanding fitness tracker users' security and privacy knowledge, attitudes and behaviors* [Paper presentation]. CHI Conference on Human Factors in Computing Systems, Honolulu, HI, US. https://dl.acm.org/doi/proceedings/10.1145/3313831

Goodyear, V. A., Kerner, C., & Quennerstedt, M. (2019). Young people's uses of wearable healthy lifestyle technologies: Surveillance, self-surveillance and resistance. *Sport, Education and Society*, *24*(3), 212–225. https://doi.org/10.1080/13573322.2017.1375907

Gorm, N., & Shklovski, I. (2019). Episodic use: Practices of care in self-tracking. *New Media & Society*, *21*(11/12), 2505–2521. https://doi.org/10.1177/1461444819851239

Grzymek, V., & Puntschuh, M. (2019). *What Europe knows and thinks about algorithms* (Discussion Paper Ethics of Algorithms #10). Bertelsmann Stiftung. https://doi.org/10.11586/2019008

Hepworth, K. (2017). Big data visualization: Promises & pitfalls. *Communication Design Quarterly Review*, *4*(4), 7–19. https://doi.org/10.1145/3071088.3071090

IMS Institute for Healthcare Informatics. (2015). *Patient adoption of mhealth: Use, evidence, and remaining barriers to the mainstream acceptance*. https://www.iqvia.com/-/media/iqvia/pdfs/institute-reports/patient-adoption-of-mhealth.pdf

Ireland, L. (2020). Predicting online target hardening behaviors: An extension of routine activity theory for privacy-enhancing technologies and techniques. *Deviant Behavior*. Advance online publication. https://doi.org/10.1080/01639625.2020.1760418

Israelski, E., & Muto, W. (2012). Human factors risk management for medical products. In P. Carayon (Ed.), *Handbook of human factors and ergonomics in health care and patient safety* (2nd ed., pp. 475–506). CRC Press.

Katuska, J. (2019). Wearing down HIPAA: How wearable technologies erode privacy protections. *Journal of Corporation Law*, *44*(2), 385–401.

Kitchin, R., & Fraser, A. (2020). *Slow computing: Why we need balanced digital lives*. Bristol University Press.

Kordzadeh, N., Warren, J., & Seifi, A. (2016). Antecedents

of privacy calculus components in virtual health communities. *International Journal of Information Management*, *36*(5), 724–734. https://doi.org/10.1016/j.ijinfomgt.2016.04.015

Latzer, M., Büchi, M., Kappeler, K., & Festic, N. (2021). *Internetverbreitung und digitale Bruchlinien in der Schweiz 2021* [Internet diffusion and digital fault lines in Switzerland 2021]. University of Zurich. http://mediachange.ch/research/wip-ch-2021

Latzer, M., & Festic, N. (2019). A guideline for understanding and measuring algorithmic governance in everyday life. *Internet Policy Review*, *8*(2), 1–19. https://doi.org/10.14763/2019.2.1415

Latzer, M., Festic, N., & Kappeler, K. (2020). *Use and assigned relevance of algorithmic-selection applications in Switzerland*. University of Zurich. https://mediachange.ch/research/algosig

Latzer, M., Hollnbuchner, K., Just, N., & Saurwein, F. (2016). The economics of algorithmic selection on the internet. In J. Bauer & M. Latzer (Eds.), *Handbook on the economics of the internet* (pp. 395–425). Edward Elgar. https://doi.org/10.4337/9780857939852

Li, N., & Hopfgartner, F. (2016). To log or not to log? SWOT analysis of self-tracking. In S. Selke (Ed.), *Lifelogging* (pp. 305–325). Springer. https://doi.org/10.1007/978-3-658-13137-1_17

Lupton, D. (2015). Quantified sex: A critical analysis of sexual and reproductive self-tracking using apps. *Culture, Health and Sexuality*, *17*(4), 440–453. https://doi.org/10.1080/13691058.2014.920528

Lupton, D., & Michael, M. (2017). "Depends on who's got the data": Public understandings of personal digital dataveillance. *Surveillance & Society*, *15*(2), 254–268. https://doi.org/10.24908/ss.v15i2.6332

Marelli, L., Lievevrouw, E., & Hoyweghen, I. V. (2020). Fit for purpose? The GDPR and the governance of European digital health. *Policy Studies*, *41*(5), 447–467. https://doi.org/10.1080/01442872.2020.1724929

Masur, P. K. (2019). *Situational privacy and self-disclosure*. Springer. https://doi.org/10.1007/978-3-319-78884-5

Matthews, M., Murnane, E., & Snyder, J. (2017). Quantifying the changeable self: The role of self-tracking in coming to terms with and managing bipolar disorder. *Human-Computer Interaction*, *32*(5/6), 413–446. https://doi.org/10.1080/07370024.2017.1294983

Mercer, K., Li, M., Giangregorio, L., Burns, C., & Grindrod, K. (2016). Behavior change techniques present in wearable activity trackers: A critical analysis. *JMIR mHealth and uHealth*, *4*(2). https://doi.org/10.2196/mhealth.4461

Mercurio, M., Larsen, M., Wisniewski, H., Henson, P., Lagan, S., & Torous, J. (2020). Longitudinal trends in the quality, effectiveness and attributes of highly rated smartphone health apps. *Evidence Based Mental Health*, *23*(3), 107–111. https://doi.org/10.1136/ebmental-2019-300137

Mills, C., & Hilberg, E. (2020). The construction of mental health as a technological problem in India. *Critical Public Health*, *30*(1), 41–52. https://doi.org/10.1080/09581596.2018.1508823

Mopas, M. S., & Huybregts, E. (2020). Training by feel: Wearable fitness-trackers, endurance athletes, and the sensing of data. *The Senses and Society*, *15*(1), 25–40. https://doi.org/10.1080/17458927.2020.1722421

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. https://doi.org/10.1111/j.1745—6606.2006.00070.x

Petronio, S. (2012). *Boundaries of privacy: Dialectics of disclosure*. SUNY Press.

Pink, S., & Fors, V. (2017a). Being in a mediated world: Self-tracking and the mind-body-environment. *Cultural Geographies*, *24*(3), 375–388. https://doi.org/10.1177/1474474016684127

Pink, S., & Fors, V. (2017b). Self-tracking and mobile media: New digital materialities. *Mobile Media & Communication*, *5*(3), 219–238. https://doi.org/10.1177/2050157917695578

Pink, S., Sumartojo, S., Lupton, D., & Heyes La Bond, C. (2017). Mundane data: The routines, contingencies and accomplishments of digital living. *Big Data & Society*, *4*(1), 1–12. https://doi.org/10.1177/2053951717700924

Rosseel, Y. (2012). Lavaan: An R package for structural equation modeling. *Journal of Statistical Software*, *48*(1), 1–36. https://doi.org/10.18637/jss.v048.i02

Sjöklint, M., Constantiou, I., & Trier, M. (2015). The complexities of self-tracking: An inquiry into user reactions and goal attainment. In J. Becker, J. vom Brocke, & M. de Marco (Eds.), *ECIS 2015 completed research papers* (Paper No. 170). European Conference on Information Systems. https://doi.org/10.18151/7217479

Spiller, K., Ball, K., Bandara, A., Meadows, M., Mccormick, C., Nuseibeh, B., & Price, B. A. (2017). Data privacy: Users' thoughts on quantified self personal data. In B. Ajana (Ed.), *Self-tracking: Empirical and philosophical investigations* (pp. 111–124). Palgrave Macmillan.

Statista. (2020). *Wearable technology: Statistics & facts*. https://www.statista.com/topics/1556/wearable-technology

Strübing, J. (2021). Selbstvermessung als Subjektivierungsweise [Self-quantification as a way of subjectivation]. In K. Brümmer, A. Janetzko, & T. Alkemeyer (Eds.), *Ansätze einer Kultursoziologie des Sports* [Approaches to a cultural sociology of sports] (pp. 231–248). Nomos.

Subhi, Y., Bube, S. H., Bojsen, S. R., Thomsen, A. S. S., & Konge, L. (2015). Expert involvement and adherence to medical evidence in medical mobile phone apps: A systematic review. *JMIR MHealth and UHealth*,

3(3), Article e79. https://doi.org/10.2196/mhealth.4169

United Healthcare. (2021). *Wellness & rewards programs*. https://www.uhc.com/employer/communication-resources/wellness-and-rewards-programs

van Dijk, J. (2020). *The digital divide*. Polity.

van Haasteren, A., Gille, F., Fadda, M., & Vayena, E. (2019). Development of the mhealth app trustworthiness checklist. *Digital Health*, *5*, 1–12. https://doi.org/10.1177/2055207619886463

Vitak, J., Liao, Y., Kumar, P., Zimmer, M., & Kritikos, K. (2018). Privacy attitudes and data valuation among fitness tracker users. In G. Chowdhury, J. McLeod, V. Gillet, & P. Willett (Eds.), *Transforming digital worlds* (pp. 229–239). Springer. https://doi.org/10.1007/978-3-319-78105-1_27

About the Authors

Noemi Festic is a research and teaching associate in the Media Change & Innovation Division, Department of Communication and Media Research (IKMZ), University of Zurich, Switzerland. Her research interests include internet use, and the use of algorithmic-selection applications in particular, and its implications on everyday life and personal well-being. Her current research focuses on how computational methods can contribute to a better empirical understanding of the role of algorithmic selection for everyday life.

Michael Latzer is professor of communications at the Department of Communication and Media Research (IKMZ), University of Zurich, Switzerland, where he chairs the Media Change & Innovation Division. His research focuses on the co-evolution of technical, economic, political, and social innovations in the convergent communications sector, in particular on information society issues, internet research, and the significance of algorithmic selection. For details, see mediachange.ch.

Svetlana Smirnova has recently completed her PhD at the Department of Media and Communications of the London School of Economics and Political Science. Her current research interests include self-tracking and self-quantification, digital selfhood, research design and methodologies. Most recently, Svetlana has served as a post-doctoral researcher on a research and development initiative focused on the use of age-assurance and parental control tools.