Losing Control to Data-Hungry Apps – A Mixed-Methods Approach to Mobile App Privacy

Brandtzaeg, P. B., Pultier, A., & Moen, G.M.

Citation:
Brandtzaeg, P. B., Pultier, A., & Moen, G.M. Losing Control to Data-Hungry Apps – A Mixed-Methods Approach to Mobile App Privacy, Social Science Computer Review, 2018, pp 22, https://doi.org/10.1177/0894439318777706

Losing Control to Data-Hungry Apps: A Mixed-Methods Approach to Mobile App Privacy

(reference: Brandtzaeg, P. B., Pultier, A., & Moen, G.M. (2018, in press). Losing Control to Data-Hungry Apps – A Mixed-Methods Approach to Mobile App Privacy. *Social Science Computer Review* **Doi: http://journals.sagepub.com/doi/full/10.1177/0894439318777706**

Corresponding author:

Petter Bae Brandtzaeg

SINTEF, PB 124 Blindern, 0314 Oslo, Norway.

e-mail: pbb@sintef.no

Co-authors

Antoine Pultier, SINTEF: Email: Antoine.Pultier@sintef.no

Gro Mette Moen, the Norwegian Consumer Council: Email: Gro.MetteMoen@forbrukerradet.no

Abstract

Personal data from mobile apps are increasingly impacting users' lives and privacy perceptions. However, there is a scarcity of research addressing the combination of (1) individual perceptions of mobile app privacy, (2) actual personal dataflows in apps, and (3) how such perceptions and dataflows relate to actual privacy policies and terms of use in mobile apps. To address this limitation, we conducted an innovative mixed methods study including a representative user survey in Norway, an analysis of personal dataflows in apps, and content analysis of privacy policies of 21 popular, free Android mobile apps. Our findings show that more than half the respondents in the user survey repeatedly had refrained from downloading or using apps to avoid sharing personal data. Our analysis of dataflows applied a novel methodology measuring activity in the apps over time (48 hours). The investigation showed that 19 of 21 apps investigated transmitted personal data to a total of approximately 600 different primary and third-party domains. From a European perspective, it is particularly noteworthy that most of these domains were associated with tech companies in the United States, where privacy laws are less strict than companies operating from Europe. The investigation further revealed that some apps by default track and share user data continuously, even when the app is not in use. For some of these, the terms of use provided with the apps did not inform the users about the actual tracking practice. A comparison of terms of use as provided in the studied apps with actual person dataflows as identified in the analysis disclosed that three of the apps shared data in violation with their provided terms of use. A possible solution for the mobile app industry, to strengthen user trust, is privacy by design through opt-in data sharing with the service and third parties, and more granular information on personal data sharing practices. Also, based on the findings from this study, we suggest specific visualizations to enhance

transparency of personal dataflows in mobile apps. A methodological contribution is that a mixed methods approach strengthens our understanding of the complexity of privacy issues in mobile apps.

Keywords: privacy, terms of use, mobile apps, trackers, trust, location data

Losing Control to Data-Hungry Apps: A Mixed-Methods Approach to Mobile App Privacy

The privacy scandal at Facebook in spring 2018, where 87 million users and their data have been mined from a third-party application (app) hosted by Cambridge Analytica, has revealed the lack of control individual users have over their personal data. Yet, the case of Cambridge Analytica should not be evaluated in isolation. Companies like Google, Amazon, Apple, Facebook and more collect, aggregate, share, and use personal information of their users. The accumulation of user data gives almost limitless knowledge about individuals and represents a privacy risk (Esayas, 2017). The mobile app industry and data analytics are increasingly shaping users' lives and future experiences of privacy. Hence, concerns about data misuse or unsatisfactory control of users' personal data increase as global use of smartphones and mobile apps grows (Gilbert et al., 2011; Madden, 2014). In 2016 it was estimated that over a third of the world's population—2.6 billion people—would own a smartphone by the end of 2017 (Statista, 2016). Mobile apps, defined here as software applications developed for use on tablets and smartphones (Lim et al., 2015), are user-friendly and often free of charge, and they provide a variety of services from dating (e.g., Tinder) to payment (e.g., Vipps), social networking (e.g., Facebook), fitness (e.g., Endomondo) and gaming (e.g., Pokémon Go). These services may come with an often-unknown privacy risk for users.

Collecting and monetizing massive amounts of personal user data are important parts of the business model for digital services (Wang et al., 2015). Profiles on users are frequently created and are partly based on passive digital footprints, that is, data collected without users' knowledge (Thatcher, 2014). Moreover, mobile apps often provide "their functionality by accessing sensitive data (e.g., account, password, contact, financial records, medical records,

GPS, camera, and microphone)" (Gilbert et al., 2011, p. 21). Such data collection is different from active digital footprints, which are created when personal data is released by a user deliberately for sharing information (Madden, 2014). The term *personal data* is defined in European legislation as data connected to a person (Article 29, 2007), which includes a wide array of data from full names to IP addresses and device identifiers. A problem, however, is that many apps lack transparency about how they will use personal information (Sunyaev et al., 2015). Many apps also request and share detailed user information, without justifying the data collection and sharing process. For example, recently it was revealed that the gay dating app Grindr shared HIV-testing and location data with two third-party players (Ghorayshi & Ray, 2018).

Most major countries and their privacy laws require apps to have a privacy policy for the collection of personal data and use of analytics. Privacy policy is a statement declaring an app's or firm's legal policy regarding the collection and release of information about a user. Yet, the length of privacy policies is often perceived by users as too long to read (McDonald & Craner, 2008) and too complicated to understand (Brandtzaeg, Lüders, & Skjetne, 2010). In addition, the privacy policies of many mobile health apps lack transparency about privacy practices with user information (Sunyaev et al., 2015). Transparency in providing accessible information to individuals about how apps will use their personal data is key to gaining trust among mobile users (Federal Trade Commission, 2013).

Considering the forgoing, the rapid use of mobile apps raises important questions about privacy. First, little is known about users' perception of their privacy risk, interaction of apps with third-party domains, and the extent to which the dataflow of apps converges with privacy policies (Zang et al., 2015). Such analyses are in particular important for mobile payment apps,

fitness apps, and dating apps, which typically make use of sensitive user data. Payment apps may share information about shopping habits. Dating apps may share personal data concerning sexual orientation or preferences as well as continuously broadcast real-time user location to find nearby potential dates (Farnden, Martini, & Choo, 2015). Fitness apps may track location and health-related issues.

Second, most studies on mobile privacy are based in the United States. However, results from an international study clearly indicate that significant differences exist in mobile app user behaviour in different countries (Lim et al., 2015). Research also shows that the United States and Europe exhibit different approaches to information privacy (Smith, 2001). "In Europe, privacy legislation limits the ways companies can use and connect personal data, and individuals have the right to see the data collected about them, but in the United States and many other countries commercial data collection is largely unregulated" (Rettberg, 2014, p. 88). Hence, apps based in the United States may allow less privacy than European apps, which may affect Europeans experiences of trust regarding mobile privacy.

Addressing these issues, this study involved 21 popular, free mobile apps available in Norway for the open-source operating system Android. Given users' focus on mobile payment, dating, and fitness apps, this study included these apps into its investigation. Furthermore, given the US-centric research on privacy in mobile apps, it was necessary to bring cultural balance in the research on mobile privacy focusing on a European context. We do this by applying an innovative combination of methods; looking at privacy issues from a user perspective, data perspective, and policy perspective in Norway. Norway provides an ideal context for studying the impact of mobile app privacy given its exceptionally high smartphone usage (Google Consumer Barometer, 2016). Focusing on apps in Norway revealed geographical patterns of how data is

shared and stored when apps are used in a European country. Finally, this research went beyond existing studies by monitoring the transmission of data in apps over time and when the mobile device was not in use.

Limitations of the research are addressed in the following three research questions (RQ):

RQ1: What are users' perceptions of trust with regard to mobile app privacy?

RQ2: What kind of personal data (e.g., location data) do popular mobile apps for Android, including payment, dating, and fitness apps, share with first-domain and third-party trackers (and how many trackers), and does such data sharing also happen when the app is not in use?

RQ3: How privacy-friendly are the terms of use and privacy policies of mobile apps, and how do these documents correlate with users trust and the data collection and sharing activities recorded for each app?

Background

The theory of privacy regulation suggested by Irwin Altman (1975) aims to explain why people sometimes prefer aloneness but at other times like social interaction. Hence, privacy is not static but "a selective control of access to the self or to one's group" (Altman, 1975, p. 18). With new media technologies and the development of mobile apps, humans experience of privacy extend from physical space to online space, making privacy far more complex. With the use of interactive technologies, users' "ability to rely on these same physical, psychological and social mechanisms for regulating privacy is changed and often reduced" (Palen & Dorish, 2003, p. 131). Privacy management, from a user perspective, has developed to be a much more dynamic and complex mechanism of boundaries in the context of mobile apps, a context that people often struggle to understand.

Amid the complexity of privacy in new technologies, such as mobile apps, users are sometimes unaware of privacy risks and their own privacy rights (Hoofnagle, Urban, & Li, 2012; Golbeck & Mauriello, 2016). A user may have difficulty understanding an app's business model, privacy policy (Brandtzaeg et al., 2010; McDonald & Craner, 2008) and the technical functionality of an app and its privacy implications (Felt et al., 2012; Hoofnagle et al., 2012). Additionally, although third-party tools for advertisements and analytics are pervasive, an extensive survey of privacy and security issues by smartphone app developers found that developers themselves are unaware of the data collected by these tools (Balebako et al., 2014), which further complicates the matter of privacy and leads the researchers to question how average app users understand the dataflow if app developers struggle to understand privacy and security.

Digital footprints, third-party trackers, and device fingerprints (Chia, Yamamoto, & Asokan, 2012; Falahrastegar et al., 2016) have made information privacy issues more complex and often hidden from the user (Spensky et al., 2016). Studies of mobile apps specifically have revealed that companies share and leak private data to unknown destinations and third-party advertisement servers (Egele et al., 2011; Enck et al., 2010; Zang et al., 2015). A loss of control over personal data may explain why users have increasing apathy and fatigue toward online privacy (Hargittai & Marwick, 2016). Users may pay less attention to privacy because they are not able to see how personal information is tracked, how it is used, and how it is disclosed to third parties (Yu et al., 2016; Rettberg, 2014). Libert (2015) found that users do not know how to discover what kind of data mobile apps collect, how they track data, and what they do with the collected data. In general, mobile app users seem to have very little support in making decisions concerning what apps to install and trust (Lin et al., 2012). In a large scale global study by Lim et

al. (2015), only 17% of mobile app users reported they stopped using an app because it invaded their privacy. However, this percentage might be due to the fact that many app users are largely unaware of their data being shared and the implications. Consequently, the assumption of privacy being controlled by the users themselves (Tavani, 2008) is challenged by increased surveillance of passive digital footprints and the invisibility of dataflows. Greater knowledge is needed about how people can be informed and can control their own data.

A Pew Internet Project survey (Madden, 2014) reveals that 91% of adults in the United States "agree" or "strongly agree" that consumers have lost control over how personal information is collected and used by companies. According to the U.S. Federal Trade Commission (2013), a lack of attention to these trust-related concerns could be harmful to both consumers and the mobile app industry. However, concerning privacy in mobile apps, people's trust, perceptions, and expectations are not well understood (Martin & Shilton, 2016). Trust is a complex concept, and numerous definitions can be found across disciplines within the humanities, social sciences, and technological sciences (Corritore et al., 2003). Mayer et al. (1995) define trust as the willingness of the trustor (the person who trusts) to be vulnerable to the actions of the trustee (the entity to be trusted). Trust, therefore, involves a willingness to take risks when value is at stake (Mayer et al., 1995). Applied to mobile app privacy, perceived risks may relate to whether the trustor perceives the app to be safe to use and download (Joshi & Mishra, 2016).

Trust-related privacy issues are also evident when reviewing more technical studies about mobile app privacy. A recent study by Zang et al. (2015) examined 110 popular, free Android and iOS apps and identified those that shared personal, behavioural, and location data with third parties. They found that a significant number of apps share user data, such as personal

information or search terms, with third parties, and Android and iOS do not require them to notify the user that they are sharing the data. Specifically, 73% of Android apps share personal information, such as email addresses, with third parties, and 47% of iOS apps share geo-coordinates and other location data with third parties. Another study, by Njie (2013), revealed that 43 health and fitness apps identified several discrepancies between the apps' terms of use and their behaviour. One conclusion of the study was that the only way for a user to know how great a privacy risk an app may pose is to perform a technical evaluation over the dataflow, which is beyond the ability of most users (Njie, 2013).

Zang et al. (2015) identified three approaches to surveying data sharing by mobile apps:

(1) Permissions analysis reviews permission requests from a particular app either before installation or during use.

(2) Static code analysis to identify which permissions the app requests as part of its design and/or its search for third-party libraries.

(3) Dynamic analysis measures dataflow when an app is being used.

A fourth approach, not mentioned in this list, is to measure the dataflow also when the app is not being used.

In addition, studies may investigate smartphone users' level of trust in mobile apps regarding privacy (Chin et al., 2012), and potential conflicts between users' privacy expectations and the use of data collected from mobile app providers. While users expect context-related navigation, for example in weather applications, they do not expect the data to be used for targeted advertisements (Martin & Shilton, 2016).

Zang et al. (2015) encourage future researchers to continue measuring the accuracy of Internet use captured by mobile apps. They also suggest reviewing how app companies' privacy

policies relate to their actual data collection and sharing activities. While previous studies have investigated either user-oriented or technical perspectives on privacy in a US context, few studies have investigated these perspectives together. As mentioned, mobile payment apps, dating apps, and fitness apps specifically, are highly interesting in regard to privacy because they potentially process sensitive data as well as real time location data; hence, there is a need for more comprehensive and in-depth research on privacy issues in apps targeting payment, dating, and fitness. There is also a need for investigating user privacy from a European context, investigating the dataflow from Norway to the United States. This focus combined with a 48-hour analysis of each of the 21 apps studied in this mixed-methods approach provide a significant contribution to the research on privacy in mobile apps.

Method

With new app technologies emerging and issues of transparency and trust making user privacy far more complex (e.g. Palen & Dorish, 2003), this study used a mixed-methods approach to investigate privacy in mobile app use. Our approach allowed for a comparison of apps' terms of use, privacy policies, and dataflow in order to identify discrepancies between what companies *declare* they will do with user data and what they *actually* do with the data. In addition, a survey measured the use and general level of trust regarding mobile app privacy.

The strength of this research is the innovative combination of mixed methods. The following methodologies were applied in this study:

(1) Online survey

(2) Analyses of personal dataflow in apps over time (48-hour analysis)

(3) Content analysis of the terms of use and privacy policies

Online Survey

To answer RQ1, an online survey was applied to obtain initial quantitative data on users' behaviour and levels of trust regarding mobile app privacy from the users' perspectives. They were first asked about their usage of the 21 apps chosen for this study (app selection is detailed below). In line with the understanding of trust as risk perception or a willingness to assume risk (Mayer et al., 1995), this study mapped user trust in downloading apps by asking questions such as "To what extent do you have confidence that the apps you use handle your personal information in a secure manner?" and "Do you think it's okay that your personal information (such as access to your contact list or your location) is used for purposes other than making the application work?" Responses were measured on a five-point Likert scale ranging from "strongly agree" (one) to "strongly disagree" (five), with a sixth option, "don't know."

To further measure users' perceptions of privacy risk in mobile apps, the same question was asked as in the Lim et al. (2015) mobile privacy study: "Have you refrained from downloading or using mobile applications because the application requires access to information you do not want to provide (such as access to your contact lists or where you are)?" Answers included "Yes, one time," "Yes, several times," "No, never," and "Don't know." Single-item measures such as these are quick and easy to use, and although methodologists recommend multiple-item measures, this strict view has recently been challenged; several studies have demonstrated meaningful, reliable estimates for single-item measures (Bergkvist & Rossiter, 2007; Loo, 2002).

A nationally representative sample (Internet population) of individuals was selected, aged 18 or older, in Norway. The survey was launched in 2015 and outsourced to Norstat, a leading European fieldwork agency. The data were weighted by gender, age, education, and geography

according to governmental population statistics. A total of 1,005 people participated in the survey. Respondents who had neither a smartphone nor a tablet (4%) were removed from the database. Analyses were conducted on the remaining 960 respondents. Key issues found in the user survey were analysed in terms of use, privacy policies, and dataflow analysis.

Analyses of Dataflow in Mobile Apps

To answer RQ2, an analysis of dataflows in 21 free mobile apps for Android were performed to reveal what kind of data (e.g., personal data, location data) these mobile apps share with first-domain and third-party trackers.

Testing the apps.

As illustrated in Figure 1, all the mobile Android apps were tested for basic usage on two new smartphones, the Samsung Galaxy S5 and the Sony Xperia Z3 Compact. For each app, the following tests were performed (if applicable): install the app, start the app, register a user profile, close the app, start the network capture, start the app, test every feature in the app, close the app, stop the network capture, and uninstall the app.

Dating apps were tested with specific dating features between two test accounts to allow for a typical dating app scenario and also to test the proximity-based location system used by Tinder and Happn. All the tests were done indoors, except for the activity features on fitness apps that were tested outdoors. The mapping and analysis of the dataflow in app was conducted in Oslo, Norway, in 2015 to give a European context to reveal how user data in mobile apps used in Norway are moving from Europe to the United States.

Recording app communication.

Similar to Zang et al. (2015), a dynamic analysis was performed to monitor and record all communication between the apps on the mobile devices and the Internet through the man-in-the-

middle approach. A fictitious user profile was created in each of the apps that required a profile. Network communications were captured using various configurations and tools, as shown in Figure 1.

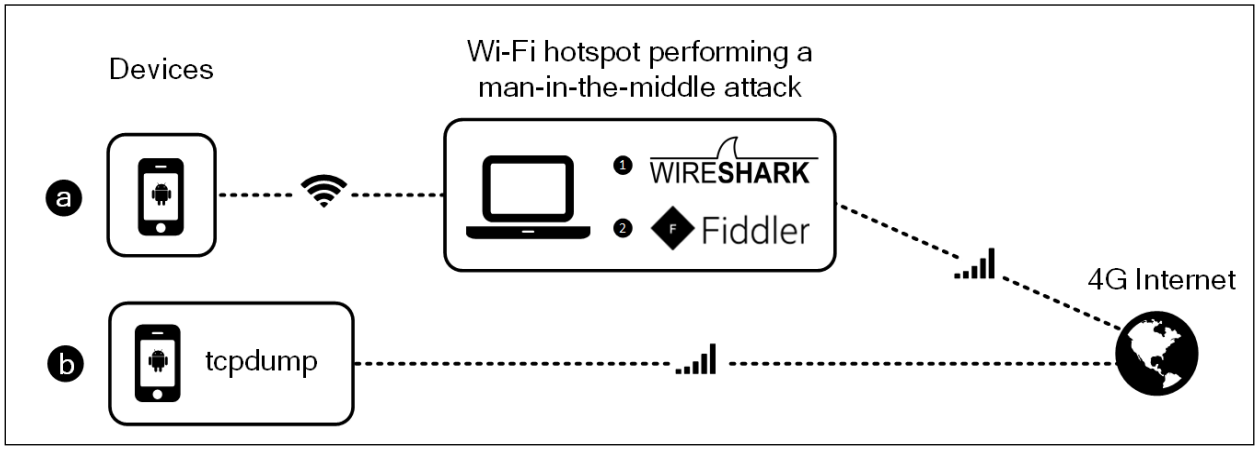

Figure 1. Overview of the dataflow analysis in apps performed on the Samsung Galaxy S5 (a) and the Sony Xperia Z3 Compact (b).

In more detail, a laptop offering a Wi-Fi hotspot intercepted the communication using Wireshark to monitor all TCP/IP traffic and using Fiddler to capture HTTP and HTTPS traffic. Data were also captured directly on a smartphone using tcpdump in order to analyse packets and profile network traffic. To test an app, typical use was simulated for up to 60 minutes. To discover whether apps were transmitting more data over time, dataflow was monitored for 48 hours while the app was not in use. As far as we know, a 48-hour analysis is a unique contribution to research on app user privacy. In all configurations, the network access was a 4G connection provided by the telecommunication provider Telia in Norway. Various configurations were used to validate results and determine whether behaviour depended on configuration. The

same test was done on the two different mobile devices to verify whether there were any device-specific differences.

Analyses.

App communication was analysed using tools such as SQLite, TextQl, APKTool, Smali, Mechanize, PruneCluster, and custom-developed Ruby scripts. For each mobile app, reports were generated that contained detected data from network communications, third-party modules, authorizations, and overviews of the contact Internet servers. HTTP and HTTPS network communications were thoroughly analysed by decoding common document formats and representations. The Android app packages were also analysed to identify third-party components and detect software access of personal information.

Content Analysis of Terms of Use and Privacy Policies

To answer RQ3, a team of three experts on digital rights related to law and informatics/media science performed a content analysis (Hsieh & Shannon, 2005) of the terms of use and privacy policies of 20 mobile apps analysed for dataflow (the YouTube app was excluded from the content analysis). Content analysis was applied to identify themes or patterns in the policies involving readability issues and privacy threats.

The content analysis was guided by the following criteria: (1) readability of the terms and policy (e.g., technical or easy-to-understand language, use of hypothetical language); (2) length (i.e., number of words) of the terms of use and policies; (3) ownership and sharing of content (e.g., sharing with a third party); (4) retention of personal data (e.g. data are kept for longer than necessary for a purpose); and (5) issues found to be legally problematic from the consumer's point of view (i.e., changing terms without notice, eviction from the service without just cause).

The privacy policies were further coded with respect to the legal experts' sentiment: positive (yes) or negative (no). Negative sentiment addressed aspects of the privacy policy that were interpreted as problematic or undesirable based on the above criteria. Positive sentiment involved issues that were not seen as problematic or undesirable to the legal experts performing the analysis.

To validate all the conclusions, two coders, a lawyer in consumer rights and an expert in consumer issues, went through all the material in the analysis to identify breaches of European law. In cases where the coding process did not lead to a clear conclusion, the particular case was discussed with the three initial coders. When this did not lead to a conclusion, the issue was coded with a question mark. These situations usually involved unclear language or contradictory policies. The terms of use and privacy policies were analysed between June 2015 and November 2016, and the conclusions are available in a report (Norwegian Consumer Council, 2016b).

Finally, to further answer RQ3, the findings of the analysis of the terms of use and privacy policies were compared with the findings of the actual dataflow analysed to identify possible discrepancies between the policies to which users consent and the actual dataflow.

Results

The results are presented in the following order: (a) the online user survey, (b) the analysis of dataflow in apps, and (c) the review of terms of use and privacy policies.

Online User Survey

As seen in Figure 2, of the apps analysed in this study, 69% of the survey sample reported to have downloaded the Facebook app, the most popular app in the sample. The three most popular Norwegian apps were Finn, WordFeud, and VG. Only 11% of the respondents had not downloaded or used any of the apps analysed. The most striking pattern was that many respondents used a variety of different apps. It was found that younger respondents download

more mobile apps than older respondents. Three out of 10 respondents over 60 years of age had not downloaded any apps at all, while nearly half (47%) under the age of 45 had downloaded 10 or more apps over the previous year.

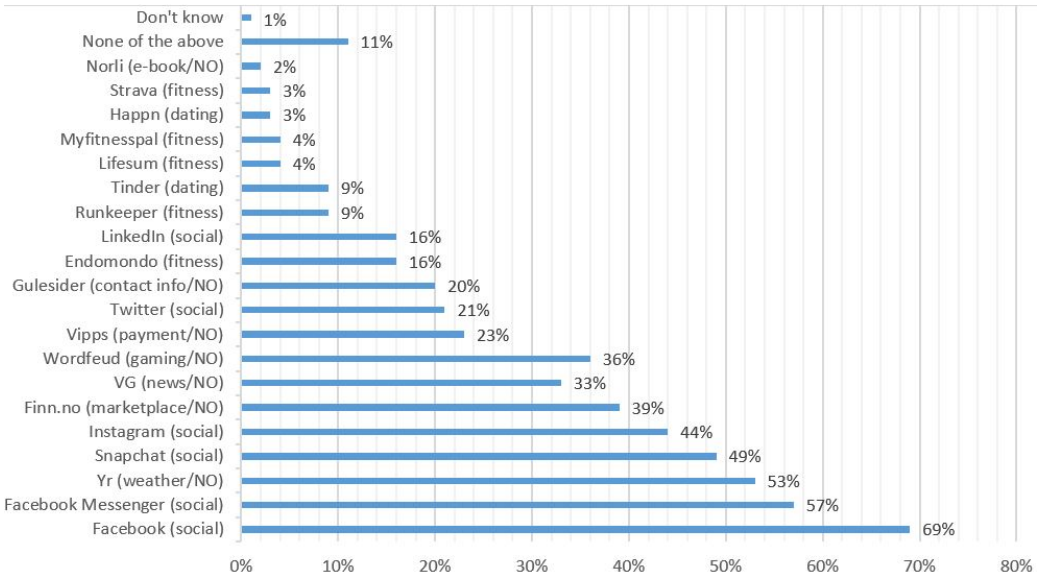

Figure 2. Overview of the popularity of apps in %. NO = Norwegian apps. N = 942.

Interestingly, over half of the respondents reported that they repeatedly refrained from downloading or using apps to avoid giving out personal information, as shown in Figure 3. The percentage was highest (60–62%) among those aged 30–49 years. A low level of trust (measured as repeatedly not downloading or using apps due to privacy issues) and age were significantly correlated ($r = .167$, $p < .001$). Among those who had little trust in app companies' handling of personal information, almost 75% reported that they had refrained from downloading or using apps. Notable differences were not found in terms of education or gender.

In addition, the percentage of those who had repeatedly refrained from downloading or using mobile apps increased with the number of apps they downloaded.

Forty percent of participants reported little trust in how apps handled personal information. Ninety percent reported being critical of their personal information being used for purposes other than app functionality. Among those who had repeatedly refrained from downloading or using apps, 96% expressed a negative attitude toward the use of personal information outside the app's functionality.

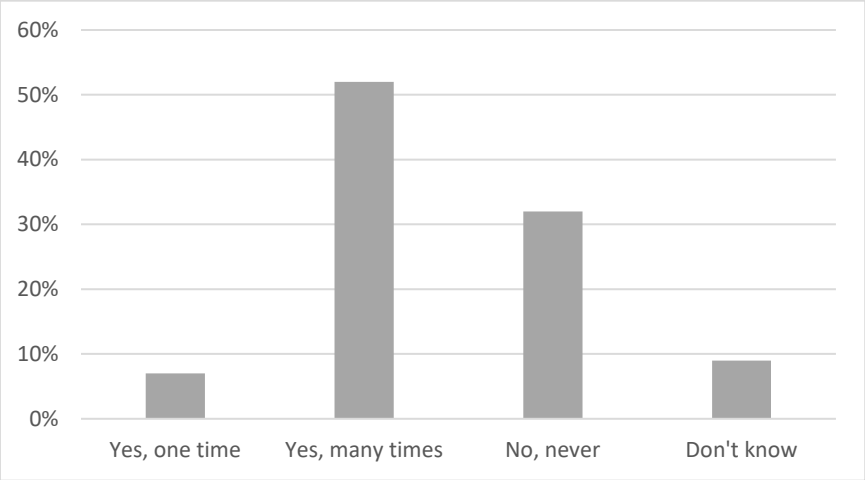

Figure 3. Responses in percentages to the question: "Have you refrained from downloading or using mobile applications because the application requires access to information you do not want to provide (such as access to your contact lists or your location)?" N = 960

Overall, the analysis of dataflows found that approximately 600 different primary and third-party domains communicated with the 21 mobile apps tested. Identification and geo-location of the contacted services highlighted that dataflows from these apps appeared only in

Europe and United States at large tech companies such as Amazon, Google, and Facebook, as shown in Figure 4.

Figure 4. Overview of the dataflow from the 21 mobile apps tested, revealing how these apps are communicating with primary or third-party domains in Europe and the United States.

Of the 21 apps studied, it was found that 12 shared personal information such as email addresses, advertiser ID, device ID, Facebook ID, or GPS location with third parties. Seven out of 21 apps shared geo-coordinates and other location data with third parties, as shown in Table 1.

Table 1

Overview of the Android Apps' Sharing of Sensitive Data (N=20)

App name and category	Personal data shared with third parties	Location shared with third parties
Facebook (Social)	NA	NA
Snapchat (Social)	NA	NA
Messenger (Social)	NA	NA
LinkedIn (Social)	NA	NA
Twitter (Social)	NA	NA
Instagram (Social)	NA	NA
YouTube (Social)	NA	NA
Tinder (Dating)	Yes	Yes
Happn (Dating)	Yes	Yes
Endomondo (Fitness)	Yes	Yes
MyFitnessPal (Fitness)	Yes	Yes
Runkeeper (Fitness)	Yes	Yes
Strava (Fitness)	Yes	NA
Lifesum (Fitness)	Yes	NA
Gulesider (Contact)*	Yes	NA
VG (Newspaper)*	Yes	Yes
WordFeud (Gaming)*	Yes	Yes
Norli-ebook (Book)*	NA	NA
Vipps (Payment)*	Yes	NA
Yr (Weather)*	NA	NA
Finn (Marketplace)*	Yes	NA
TOTAL	12	7

Note: NA = not applicable, mainly due to encrypted communication in the app indicating that no observed data was found to be shared with third-party domains by the app.
*Norwegian apps

In the Figures 5–9, coloured arrows highlight particular patterns in the dataflow. *Red* indicates Google-related domains, *blue* denotes Facebook, *green* indicates analytics, marketing, and advertising domains, and *black* marks other domains.

Social networking apps.

Facebook, Messenger, Instagram, YouTube, and Snapchat detected man-in-the-middle Secure Sockets Layer (SSL) data interception and refused the connection. Therefore, data sent by these apps could not be determined. From the user's point of view, security is enhanced because the data cannot be stolen if the SSL chain of trust is broken. However, the fact that third-party sharing could not be detected does not necessarily mean that these services provide better privacy than the other apps analysed. Furthermore, since Facebook and Google are powerful Internet actors, they are included in the ecosystem of the personal data marketplace and do not need to send data to third parties.

Figure 5 shows a pattern in which popular social networking apps investigated in this study communicated mainly with their primary domains rather than third parties. For example, YouTube communicated only with Google's servers in California. The communications in these apps, such as Facebook and Messenger, were encrypted, so monitoring them was difficult. When performing a 48-hour analysis, however, it was found that Facebook operated even when the phone was not in use, indicating that tracking was continuous.

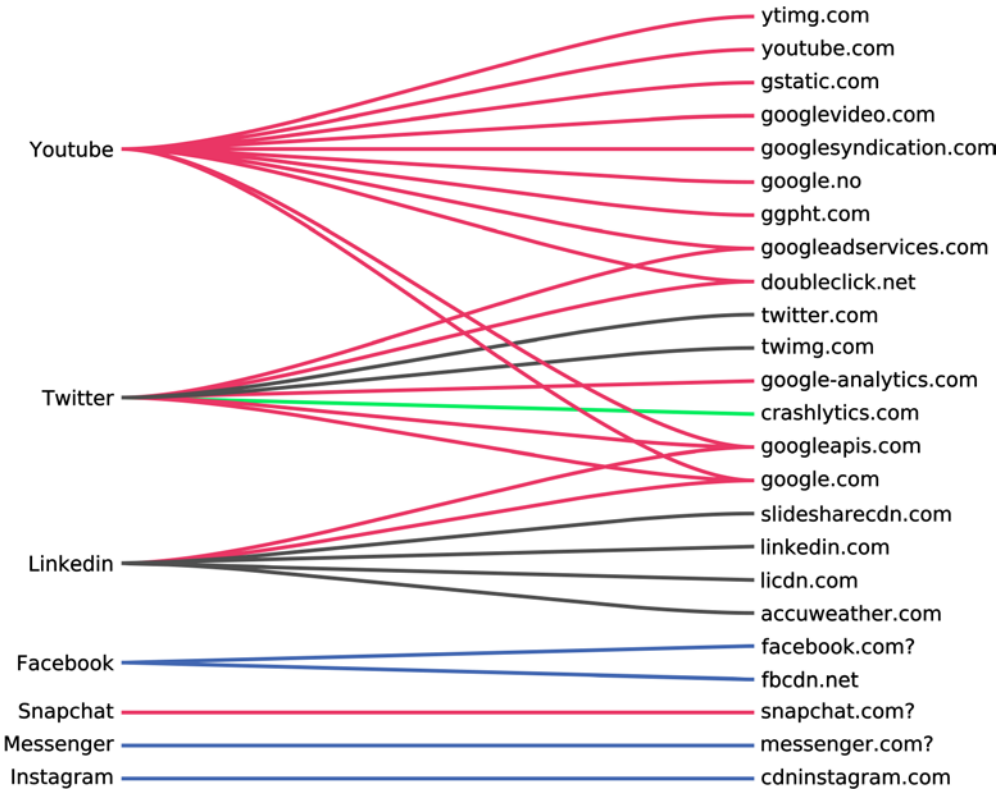

Figure 5. Overview of the dataflow in social networking apps.

Dating apps.

Dating apps for mobile devices are quite new but increasingly popular. This study investigated Tinder (launched in 2012, based in the U.S.) and Happn (launched in 2014, based in France). Figure 6 shows that both Tinder and Happn used third-party trackers, extensively communicating with Google and Facebook.

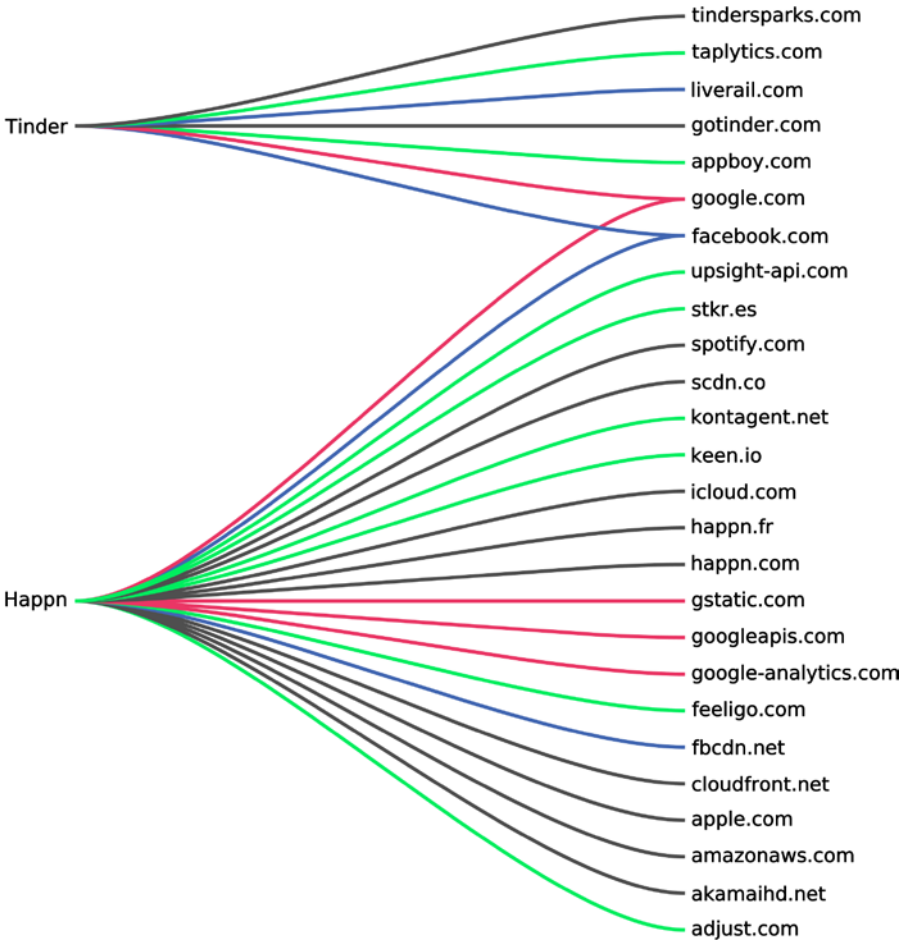

Figure 6. Overview of the dataflow in dating apps.

Happn and Tinder used real-time GPS location to show nearby users of the same app. In addition, they mapped personal identifiers; for example, Happn frequently accessed and sent important personal information, such as a combination of the Facebook ID, age, first name, birthday, job status, and gender, to Upsight, a major third-party tracking company. According to Upsight they "handle more than 500 billion data points and deliver over 1.4 billion targeted web and mobile communications every month" (Upsight, 2018). Upsight also performs custom aggregations as specified by personalized metrics to target users in, for example, marketing. The Happn user agrees to share his or her real-time GPS location when they start using the service, as

the app notes when another user is within 1–250 miles. However, sending a combination of real-time location data with personal information to third-party tracking companies is probably less known to most users. This sharing of location in combination with other data did not at the time not correspond with the confidence charter elaborated by Happn (https://www.happn.com/en/trust) (Norwegian Consumer Council, 2016b, p. 43).

Fitness apps.

As shown in Figure 7, the fitness apps tested in this study were found to contain many third-party trackers, several that are relatively unknown.

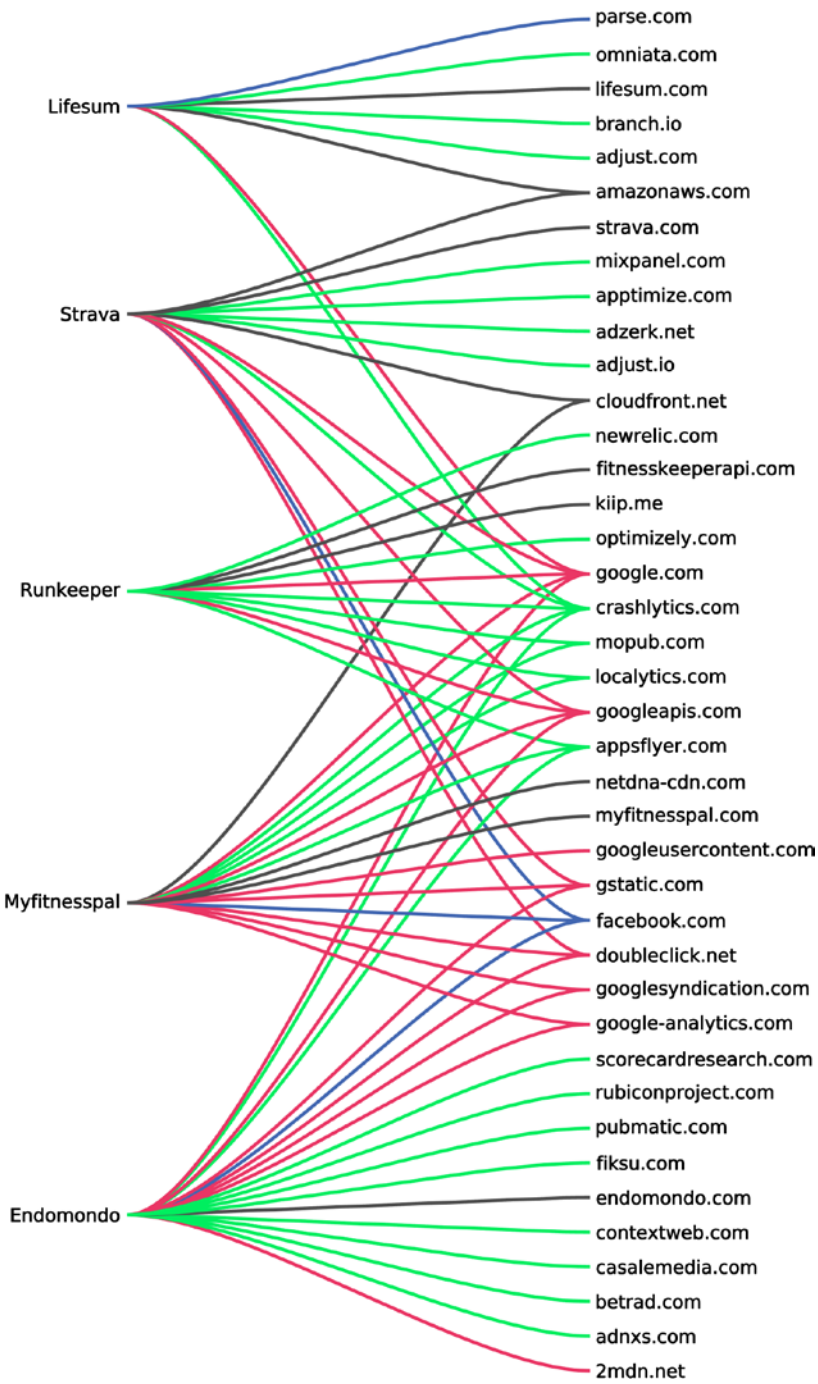

Figure 7. Overview of the dataflow in fitness apps.

The calorie-counter app Lifesum interacted with many third-party trackers that accessed information about the phone and its user, such as the hardware serial number, Facebook ID, and location. Strava worked with third-party trackers that had access to the user's International

Mobile Equipment Identity (IMEI) and device identifier, sending users' GPS positions to its own servers. Runkeeper sent users' GPS positions to Kiip.me, a third-party player that works with app optimization and marketing, even when the app was not in use. Kiip.me informs the public on their Website that they host "seven years of historical data, 120 million US devices monthly, 20 million survey responses and collect over 1 billion new data points daily" (Kiip.me, 2018). MyFitnessPal contained third-party trackers with access to personal data about the phone and its user. MyFitnessPal sent users' GPS positions to the third-party Mopub.com for targeted advertising and synchronized data when the app and phone were not in use. Finally, third-party trackers to access users' IMEI number, location, and device identifier. Endomondo also sent users' GPS position, age, and gender to Google's advertisement service and a tracker named Rubicon Project.

Norwegian apps.

Unlike the previously discussed apps, the Norwegian apps' servers were located in Norway and Sweden and did not show to the same degree the trend of excessive tracking and geo-location, except from VG, a newspaper app that used many trackers. As shown in Figure 8, American tech companies such as Amazon, Google, and Facebook have played a major role in providing services worldwide, including among Norwegian apps such as YR. This shows that data are traveling from Europe to the United States.

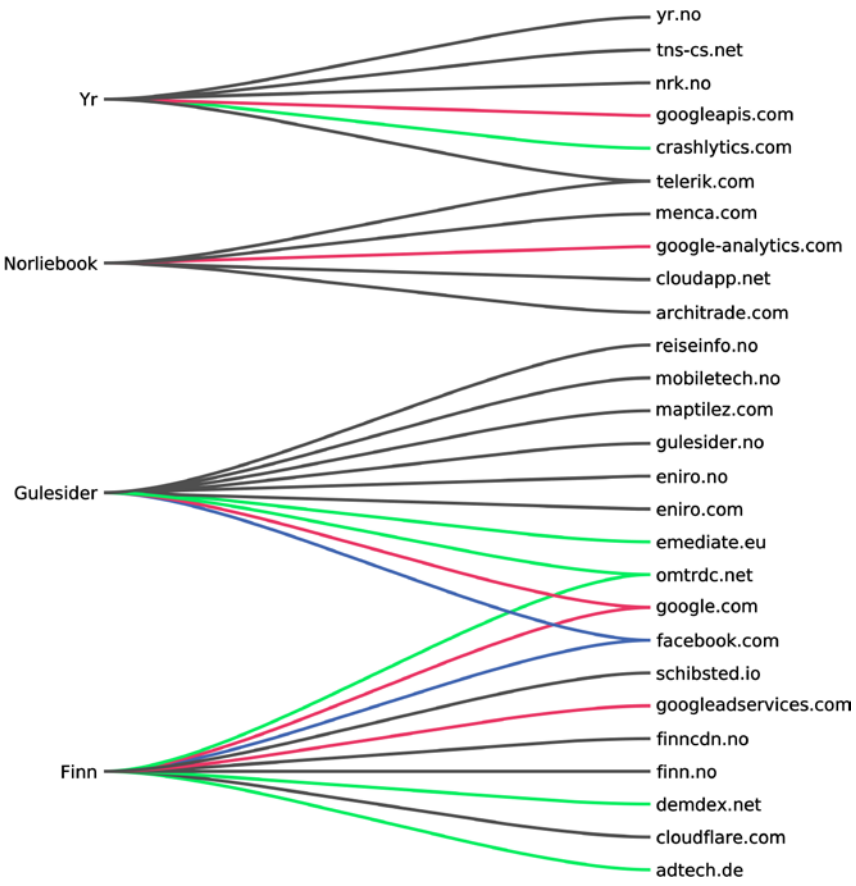

Figure 8. Overview of the dataflow in Norwegian The news app VG, as shown in Figure 9, sent information to 55 third-party trackers, typically advertising or marketing trackers and analytical trackers. This was the highest rate of data sharing among all the tested apps.

Comparing the survey with the analysis of personal dataflows in apps revealed a discrepancy between users' level of trust and dataflow. Of those who refrained from downloading or using apps, 96% expressed a negative attitude toward the use of personal information outside an app's functionality. However, 12 out of 21 apps studied shared personal information such as users' email addresses, advertiser IDs, device IDs, Facebook IDs, and GPS locations with third parties.

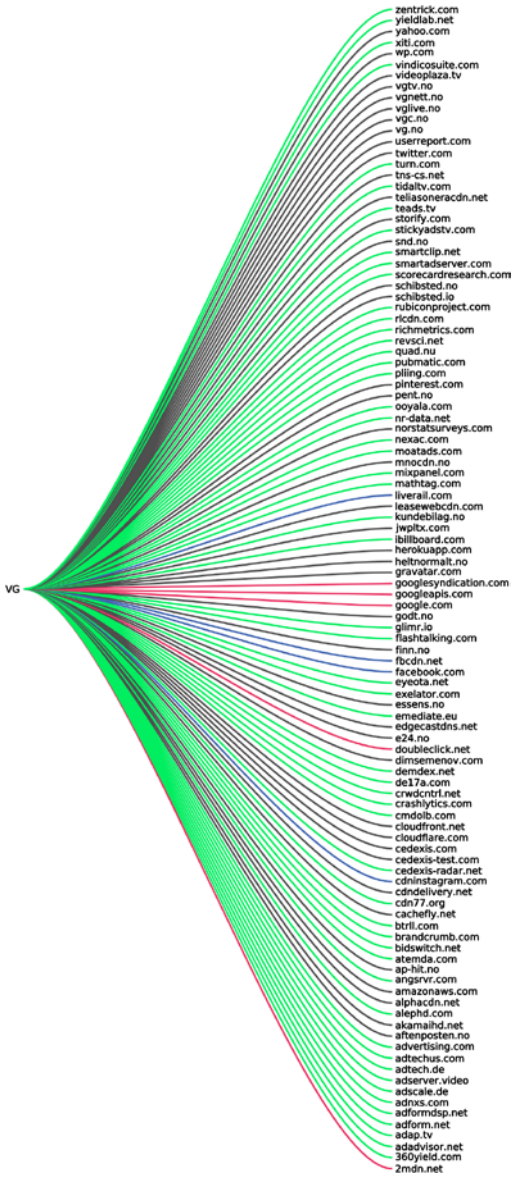

Figure 9. Overview of the dataflow in the Norwegian news app VG.

The Content Analysis of Terms of Use and Privacy Policies

The content analysis of apps' terms of use and privacy policies showed an average of 5,700 words, or 13 pages, for each app. Facebook (including Messenger), Twitter, Tinder,

MyFitnessPal, Strava, and Runkeeper all used ambiguous definitions of personal data. In addition, the terms and policies of many apps were unclear, and technical language made it difficult to understand what the app would actually do. Table 2 sums up the most notable results of the content analysis.

Table 2

Results of the Content Analysis of Apps' Terms of Use (N=20)

App name and category	Specify third parties they share data with	Third parties can only use personal data to provide the service	Limit retention period for data storage	User can delete own account	Explain required permissions	Violate own privacy policy
Facebook* (Social)	No	No	No	Yes	Yes	No
Instagram (Social)	No	No	No	No	No	No
Linkedin (Social)	No	Yes	No	No	Yes	No
Snapchat (Social)	No	No	No	No	Yes	No
Twitter (Social)	No	No	No	No	Yes	No
Happn (Dating)	X**	Yes	No	?	No	Yes
Tinder (Dating)	No	No	No	Yes	No	No
Finn.no (Marketplace/NO)	No	Yes	Yes	Yes	Yes	No
Gulesider (Information/NO)	No	Yes	No	No	Yes	No
Norli_ebook (Book/NO)	No	Yes	No	No	No	No
VG (News/NO)	No	Yes	Yes	Yes	Yes	No
Vipps (Payment/NO)	No	Yes	Yes	Yes	Yes	Yes
Yr (Weather/NO)	No	?	No	No	No	No
WordFeud (Gaming/NO)	No	No	Yes	Yes	No	No
Endomondo (Fitness)	No	No	No	Yes	Yes	No
Runkeeper (Fitness)	No	?	No	Yes	Yes	Yes
Strava (Fitness)	No	Yes	No	Yes	No	No
Lifesum (Fitness)	No	No	No	Yes	Yes	No
MyFitnessPal (Fitness)	No	No	No	No	Yes	No

Notes: NO = Norwegian apps.

*Facebook and Messenger.
**Happn violated their own privacy policy.
***Difficult to comprehend the terms and policies.

None of the apps specified the third parties with which personal data would be shared, except Happn, which claimed not to share personal data with third parties. Seven of the 20 apps clearly stated that third parties were not permitted to use personal data outside the purpose of the app. However, clear breaches of privacy policies were found in three cases.

Some terms of use and privacy policies analysed in this study can be considered to be in breach of European legislation. One such example is Tinder's policy, which claimed an irrevocable right to use user-generated content. Tinder accessed sensitive personal information about users, and according to the terms of use and privacy policies, users risked losing control of their images and other user-generated content "perpetually" and "irrevocably." Tinder could change its terms of use at any time without notifying users, and it could exclude and delete user accounts without justification. Based on the analysis, Tinder was deemed to be unfair under Section 22 of the Marketing Control Act and reported to the Norwegian Consumer Authority.

Many of the terms of use and privacy policies in this study were characterized by ambiguous language and lack of clarity, which made it difficult to conclude whether the dataflow was actually in breach of the apps' terms of use and policies. That is probably a reason for why two of the three discovered breaches of own policies occurred in apps that had very clear and privacy-friendly terms and policies.

First, the French dating app Happn clearly stated in its policy that personal data was not shared with third parties. Our dataflow analysis, however, showed that Happn shared device identifiers with a domain owned by UpSight, a major third-party tracking company that very

frequently communicated with the application about user behaviour (e.g., liking other users). Thus, when individuals used Happn, they shared information from their Facebook account, including name, age, birthday, job status, and gender, with a third-party tracker.

A second app with a clear and privacy-friendly policy was the Norwegian payment app Vipps. Its terms of use suggested that the app does not transfer information to third parties for purposes outside the functionality of the app. However, our analysis of personal dataflows in apps revealed that the app shared user data with Facebook, which was not connected to the app's function.

Third, according to the US-based app Runkeeper's privacy policy, "if you provide Personal Data for a certain reason, we may use the Personal Data in connection with the reason for which it was provided" (Runkeeper, 2015). Yet, the dataflow analysis revealed that the app often sent personal data such as Google advertising IDs to a third-party while the phone was not in use. We found that Runkeeper did not explain this in its terms of use or privacy policy. In addition, no functionality of the app was supported when the app was not in use, according to our analysis of the dataflow. Hence, this practice was found to be in breach of the app's terms of use. Based on media coverage in 2016 of our findings, Runkeeper has now made changes to the app.

Discussion

Responding to RQ1, a majority of the survey respondents reported refraining from downloading apps, indicating that users lack trust in mobile apps. Interestingly, our findings slightly contradict assumptions in previous research. While a large-scale global study by Lim et al. (2015) found that only 17% of mobile app users reported to stop using an app because it invaded their privacy, a total of 59% of the Norwegian sample herein reported the same. This

difference could be due to a large awareness of privacy issues in Norway or among mobile apps users in general, which may have increased with greater media attention on this matter of privacy.

US studies (Hoofnagle et al., 2012; Madden, 2014; Rainie & Madden, 2015) also found that users have a low level of trust in mobile app privacy. Hence, numerous app vendors and others who provide various services need to build more trust and better privacy solutions, like the Federal Trade Commission (2013) has developed, to gain more users and help users control their user data. One way of dealing with this challenge is to provide users with an understanding of the purpose for which personal data is used in an app. Past studies have shown that mobile users have a poor understanding of permissions (Wang, Hong, & Guo, 2015), and even app developers are found to lack understanding on this issue (Balebako et al., 2014). The figures presented in this study may serve as an effective approach and a useful tool to turn complex dataflows into engaging graphics that inform users about privacy.

Other research has suggested that there is a gap between consumers' expectations of privacy, especially concerning trust, and vendors' or marketers' actions; this is termed the "tradeoff fallacy" (Turow, Hennessy, & Draper, 2015). Marketers and vendors are accused of providing false justifications to users and allowing the collection and use of all kinds of consumer data. Hence, there may be a discrepancy between what users expect and the privacy protection they receive, which confirms the findings of a study by Martin and Shilton (2016).

To answer RQ2, approximately 600 different primary or third-party domains were found interacting with the 21 Android mobile apps studied. In total, 12 out of 21 (57%) apps shared personal information such as email addresses, advertiser IDs, device IDs, Facebook IDs, and GPS locations with third parties. The percentage of apps that shared personal information was likely

higher than the findings of this study as communications of data could not be tracked in all apps, including Facebook, YouTube, and LinkedIn.

The extensive sharing of data with third-party players is significant as the online user survey found that most people do not want apps to use their personal data for purposes other than the function of the app. The results of this study indicate that these concerns are legitimate. As a unique contribution to the research, this study found that some apps even tracked users when the app was not in use, indicating that tracking was continuous. This finding was revealed in the 48-hour analysis. In other words, “we don’t know all the ways in which we are being watched but we know that they are extensive” (Rettberg, 2014, p. 85). A nagging feeling of being watched may explain the low-trust perception of mobile privacy in the survey. Still, most people use those apps, explained by the "privacy paradox" (Hargittai & Marwick, 2016).

The level of third-party trackers identified in this study are similar to findings of a recent US study published in *Technology Science* (Zang et al., 2015). Yet, too little is known about many of these third-party players. In addition, this study found that most data, including personal data, is transferred from Europe to the United States, even from native Norwegian apps, which prove how personal data are traveling across the Atlantic Ocean. This might be a problem as the United States and Europe exhibit different approaches to information privacy; Europe has stricter privacy laws than the United States (Smith, 2001). For European app users, and in this case Norwegian app users, this also means that big American tech companies seem to process personal data for multiple purposes. Apps generate personal data, both when being used and when not being used, and data seem to be combined across processing activities. These findings are partly confirmed by Esayas (2017). However, evidence was not found that Facebook and Google shared personal data about app users directly with third parties. Yet, it is widely known that the use of

personal data is an important part of the business model of these companies, and the 2018 Cambridge Analytica case brings the issue of privacy to the forefront of the discussion.

All the tested dating apps and fitness apps contained many third-party trackers. The privacy of fitness apps is important as they often contain health-related data. The majority of the fitness apps tested sent real-time GPS positions of users to advertisement companies as well as the apps' own servers. It was not found that sensitive data such as body weight, size, or user performance were sent to third-party services. Still, the findings are concerning. Only the fact that someone uses a specific dating app can give indications about relationship status and other sensitive issues. It is known from previous literature that privacy policies of mobile health apps are often unclear (Sunyaev et al., 2015), although transparency in these apps is particularly important as they often involve sensitive data, which is also true for dating apps such as Tinder and Happn.

In general, privacy issues and their implications for users can be significant when user behaviour tracked by third-party services is linked or combined with personal data, such as email addresses, phone numbers, name IDs, IP addresses, cookies, and GPS locations. By combining and crosschecking data, it is possible to identify and profile a user. Third-party players can sell data to other companies and advertisers. None of the apps specified the third-parties with which personal data would be shared, which is problematic. Even the researchers of this study found it difficult to determine the nature and extent of user information that is exposed to a variety of third-party companies and what this really means. It is also difficult for users to control their personal data when it is stored by third-party trackers.

Data sharing across Europe to the United States (see Figure 4) is also complicating the matter of privacy due to the differences in privacy law between Europe and the United States.

The results from the Norwegian news apps VG (see figure 9) is also illustrating that the same tendencies of data sharing practices apply in some European apps as in US based services. While the free movement of data is at the heart of an open Internet, the mobile app industry and regulations should ensure that privacy is protected and to aid user's certainty about how data are shared and used by various companies. A challenge, is that personal data can reside in a number of locations and be stored in a number of formats.

With the increasing complexity of passive digital footprints, third-party trackers, and device fingerprints (Chia, Yamamoto, & Asokan, 2012; Falahrastegar et al., 2016), privacy issues in mobile apps are becoming more convoluted and hidden from users (Spensky et al., 2016). A more complex privacy context for users (Chia et al., 2012; Falahrastegar et al., 2016) means that we should put greater responsibility is placed on all entities involved in aggregating data. Future studies can contribute by improving users' awareness of privacy issues with mobile apps (e.g., by labelling apps with the level of impact to users' privacy). Privacy in mobile apps must be visualized or explained clearly so that users can understand how apps and third parties collect, use, and share information. To achieve the best results, such labels should be available where the consumer acquires apps (in major app stores). Also, privacy by design through opt in for sharing of personal data and granular permissions, can strengthen user privacy.

To answer RQ3, in line with Njie (2013), three apps with discrepancies between their privacy policies and their actual behaviour were identified: Happn, Vipps, and Runkeeper. Happn sent personal data to a third party, Runkeeper tracked and shared users' location when the app was not in use, and the payment app Vipps shared data with Facebook. Since Vipps' breach of its own policy was exposed in Norwegian media in 2016, the app's service provider, DNB (The Norwegian Bank) eliminated its connection to Facebook. In addition, the Norwegian Consumer

Council complained to the Norwegian Data Protection Authority about Runkeeper's practices. A few days after the complaint was filed, the service claimed to have changed the app and terminated the practice of sending information to third parties when the app is not in use. All the changes that occurred due to the results presented herein are documented in a report (Norwegian Consumer Council, 2016a). In addition, other apps investigated had problematic terms of use, without it being possible to discover discrepancies between practice and terms in this study.

The practical contribution of this study regarding RQ3 is the suggestion for designing terms of use and privacy policies to be more reader- and privacy-friendly, but even more important is the need for "privacy by design" and the minimization of data collection by apps. Mobile apps should adopt an industry standard to build trust – making it easier for users to understand where data are traveling and what purpose data are used for. Visualizations, like Figures 4–9, may facilitates understanding and transparency of the dataflow in apps, and as such make privacy control easier for users.

Limitations of the Study

This study has limitations that can be used as starting points for further research. First, our user survey but do not include more in- depth-measures to explain privacy perceptions and related behaviours during app use. Second, our analysis of dataflows in apps were done over a short period of time and in only one location (Oslo, Norway). The importance of geographic location as a variable for investigating app privacy is still not well understood. This study contributed new knowledge in investigating apps and their data sharing movements from a European context. Further research should address a comparison between various countries. Future studies should test more apps related to payment, fitness, and dating in various locations to create a larger overview of the interaction between various locations for apps and their trackers.

Another limitation is that only data shared directly with third-party trackers could be observed, and little is known about what happens after the data is shared with third-party companies such as Upsight, Kiip.me, and Mopub.com as well as Google and Facebook that host thousands of apps and user data. Future research should investigate these companies and their use of data. Further investigation of these companies is important in light of the new EU General Data Protection Regulation (GDPR). The implementation of GDPR may lead to some real change in the way mobile apps and third-party players share and use data. Companies and developers, hence, need to rethink their business models concerning how they rely on data and privacy. The operationalization of trust in mobile app privacy might be strengthened by more measures in future studies.

Finally, due to the ambiguity of some apps' terms of use and privacy policies, it was difficult to conclude whether they were in breach of their own policies, and the result was that the apps with clear privacy policies also had clear breaches of their policies, while the ambiguous policies were difficult to connect to breaches of policies. Further research should focus on how to document concrete discrepancies between terms and policies and dataflow.

Conclusion

An innovative combination of mixed methods was applied in order to understand mobile app privacy more in-depth from different perspectives. Based our user survey, it was found low user trust among mobile app users to download and use an app due to privacy issues. This low trust was justified by our finding from the analysis of personal dataflows in 21 apps revealed that data are shared from Europe to Facebook and Google domains in the United States and to several third-party domains. These results are also problematic for the following reasons:

First, this represent a privacy risk because personal user data from Europeans to a large degree is transmitted to another continent with different norms and laws regarding privacy. The accumulation of user data concerning location, consumer habits, transactions, dating, and fitness are shared from apps used in Europe, which gives US tech companies almost limitless knowledge about individuals. Highlighting data gathering of large US tech companies, such as Facebook and Google, from European mobile apps might guide app services in the United States as well as Europe to be more aware of current data sharing patterns and ways to better protect European users and their personal data.

Second, this represent a privacy concern because sharing practices of personal user data identified in this study were in many cases not explained well to the app users; in other cases, app users were misinformed in the terms of use and privacy policies. Hence, a comparison of the terms of use and the dataflow in apps disclosed that three of the mobile apps in this study violated their own terms of use. A unique finding was that some apps tracked users when the app was not in use, violating the app terms of use and privacy policies.

Our findings suggest that mobile app services should use visualizations to enhance transparency of personal dataflows in mobile apps, to make it easier for users to make choices about their privacy. In order to strengthen user trust, it is important to use privacy by design through opt-in data sharing with the service and third parties, and more transparency in personal data sharing practices.

Acknowledgements

This work was supported the Norwegian Research Council and Helsevel [grant agreement no 262848] and the Norwegian Consumer Council.

The authors would like to thank Nicolas Harrand and Finn Myrstad for their help in conducting the data flow analysis and the reviews of user terms and privacy policies in apps.

References

Altman, I. (1975). *The environment and social behavior: Privacy, personal space, territory, and crowding*. Ardent Media, NYC.

Article 29 (2007). Data protection working party's definition of personal data. Retrieved from http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf

Balebako, R., Marsh, A., Lin, J., Hong, J. I., & Cranor, L. F. (2014). The privacy and security behaviors of smartphone app developers. *Proceedings of Workshop on Usable Security (USEC).* Retrieved from http://repository.cmu.edu/hcii/265/

Bergkvist, L., & Rossiter, J. R. (2007). The predictive validity of multiple-item versus single-item measures of the same constructs. *Journal of Marketing Research, 44*(2), 175–184.

Brandtzaeg, P. B., Lüders, M., & Skjetne, J. H. (2010). Too many Facebook 'friends'? Content sharing and sociability versus the need for privacy in social network sites. *International Journal of Human–Computer Interaction*, *26*(11–12), 1006–1030.

Chia, P., Yamamoto, Y., & Asokan, N. (2012). Is this app safe? A large scale study on application permissions and risk signals. *Proceedings of the 21st International Conference on World Wide Web*. Retrieved from http://dl.acm.org/citation.cfm?id=2187879

Chin, E., Felt, A. P., Sekar, V., & Wagner, D. (2012). Measuring user confidence in smartphone security and privacy. *Proceedings of the Eighth Symposium on Usable Privacy and Security*. New York: ACM.

Corritore, C. L., Kracher, B., & Wiedenbeck, S. (2003). On-line trust: Concepts, evolving themes, a model. *International Journal of Human–Computer Studies, 58*(6), 737–758.

Egele, M., Kruegel, C., Kirda, E., & Vigna, G. (2011). PiOS: Detecting privacy leaks in iOS applications. *Proceedings of NDSS*, 177–183.

Enck, W., Gilbert, P., Chun, B., Cox, L., Jung, J., McDaniel, P., & Sheth, A. N. (2010). Taintdroid: An information-flow tracking system for realtime privacy monitoring on smartphones. *Proceedings of the 9th USENIX Symposium on Operating Systems Design and Implementation*, 393–408.

Esayas, S. Y. (2017). The idea of 'emergent properties' in data privacy: Towards a holistic approach. *International Journal of Law and Information Technology, 25*(2), 139-178.

Falahrastegar, M., Haddadi, H., Uhlig, S., & Mortier, R. (2016). Tracking personal identifiers across the Web. *International Conference on Passive and Active Network Measurement*, 30–41. New York: Springer International Publishing. Retrieved from http://www.eecs.qmul.ac.uk/~hamed/papers/pam2k16.pdf

Farnden, J., Martini, B., & Choo, K. K. R. (2015). Privacy risks in mobile dating apps. *Twenty First Americas Conference on Information Systems*. arXiv:1505.02906.

Federal Trade Commission. (2013). *Mobile Privacy Disclosures: Building Trust through Transparency*. Retrieved from https://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf

Felt, A., Ha, E., Egelman, S., Haney, A., Chin, E., & Wagner, D. (2012). Android permissions: User attention, comprehension, and behavior. Article 3. *Proceedings of the 8th Symposium on Usable Privacy and Security*. New York: ACM.

Ghorayshi, A., & Ray, S. (2018). Grindr is letting other companies see user HIV status and location data. *Buzzfeed.* Retrieved from: https://www.buzzfeed.com/azeenghorayshi/grindr-hiv-status-privacy?utm_term=.dpom8G0Jb4#.covOaWMQld

Gilbert, P., Chun, B. G., Cox, L. P., & Jung, J. (2011). Vision: Automated security validation of mobile apps at app markets. *Proceedings of the Second International Workshop on Mobile Cloud Computing and Services,* 21–26.

Golbeck, J., & Mauriello, M. L. (2016). User perception of Facebook app data access: A comparison of methods and privacy concerns. *Future Internet, 8*(2), 9. Retrieved from http://www.mdpi.com/1999-5903/8/2/9/htm

Google Consumer Barometer. (2016). Retrieved from https://www.consumerbarometer.com

Hargittai, E., & Marwick, A. (2016). "What can I really do?": Explaining the privacy paradox with online apathy. *International Journal of Communication, 10*, 21. Retrieved from http://ijoc.org/index.php/ijoc/article/view/4655

Hsieh, H. F., & Shannon, S. E. (2005). Three approaches to qualitative content analysis. *Qualitative Health Research, 15*(9), 1277–1288.

Hoofnagle, C. J., Urban, J. M., & Li, S. (2012). Privacy and modern advertising: Most US Internet users want "do not track" to stop collection of data about their online activities. *Amsterdam Privacy Conference,* 1–12. Retrieved from https://www.enriquedans.com/wp-content/uploads/2012/10/Privacy-and-Modern-Advertising.pdf

Joshi, S., & Mishra, D. K. (2016). A roadmap towards trust management & privacy preservation in mobile ad hoc networks. *ICT in Business Industry & Government (ICTBIG)*, 1–6.

Kiip.me. (2018). Retrieved from: http://www.kiip.me/moments-data/

Libert, T. (2015). Exposing the invisible Web: An analysis of third-party HTTP requests on 1 million websites. *International Journal of Communication 9*, 18. Retrieved from http://ijoc.org/index.php/ijoc/article/view/3646

Lim, S. L., Bentley, P. J., Kanakam, N., Ishikawa, F., & Honiden, S. (2015). Investigating country differences in mobile app user behavior and challenges for software engineering. *IEEE Transactions on Software Engineering*, *41*(1), 40–64.

Lin, J., Amini, S., Hong, J. I., Sadeh, N., Lindqvist, J., & Zhang, J. (2012, September). Expectation and purpose: Understanding users' mental models of mobile app privacy through crowdsourcing. *Proceedings of the 2012 ACM Conference on Ubiquitous Computing*, 501–510.

Loo, R. (2002). A caveat on using single-item versus multiple-item scales. *Journal of Managerial Psychology*, *17*, 68–75.

Madden, M. S. (2014). *Few feel that the government or advertisers can be trusted*. Washington: Pew Internet Project report. Retrieved from http://www.pewinternet.org/files/2014/11/PrivacyPanelTopline.pdf

Martin, K., & Shilton, K. (2016). Putting mobile application privacy in context: An empirical study of user privacy expectations for mobile devices. *The Information Society*, *32*(3), 200–216.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review*, *20*(3), 709–734.

McDonald, A. M., & Cranor, L. F. (2008). The cost of reading privacy policies. *Journal of Law and Policy for the Information Society*, *4*(3), 543-568

Njie, C. M. L. (2013). *Technical analysis of the data practices and privacy risks of 43 popular mobile health and fitness applications*. San Diego: Privacy Rights Clearinghouse.

Norwegian Consumer Council. (2016a). #APPWIN: An overview of changes in terms and practice. *Oslo, Norway: Norwegian Consumer Council*. Retrieved from http://fbrno.climg.no/wp-content/uploads/2016/03/appwin-update-of-changes-3-august.pdf

Norwegian Consumer Council. (2016b). APPFAIL: Threats to consumers in mobile apps. *Oslo, Norway: Norwegian Consumer Council*. Retrieved from http://fbrno.climg.no/wp-content/uploads/2016/03/Appfail-Report-2016.pdf

Palen, L., & Dourish, P. (2003, September). Unpacking "privacy" for a networked world. *Proceedings of the Conference of Human Computer-Interaction*, 129–136. New York: ACM Press.

Rainie, L., & Madden, M. (2015). Americans' privacy strategies post-Snowden. Washington: Pew Research Center. Retrieved from http://www.pewinternet.org/2015/03/16/americans-privacy-strategies-post-snowden

Rettberg, J. W. (2014). *Seeing ourselves through technology: How we use selfies, blogs and wearable devices to see and shape ourselves.* New York: Palgrave Macmillan. Retrieved from https://ssrn.com/abstract=2922572

Runkeeper. (2015). Privacy policy. *Runkeeper*. Retrieved from https://runkeeper.com/privacypolicy?showUpdatedPolicy=false

Smith, H. J. (2001). Information privacy and marketing: What the US should (and shouldn't) learn from Europe. *California Management Review*, *43*(2), 8–33.

Spensky, C., Stewart, J., Yerukhimovich, A., Shay, R., Trachtenberg, A. Housley, R., & Cunningham, R. K. (2016). SoK: Privacy on mobile devices—it's complicated. *Proceedings on Privacy Enhancing Technologies*, 96–116.

Statista. (2016). Statistics and facts about smartphones. *Statista*. Retrieved from https://www.statista.com/topics/840/smartphones/

Sunyaev, A., Dehling, T., Taylor, P. L., & Mandl, K. D. (2015). Availability and quality of mobile health app privacy policies. *Journal of the American Medical Informatics Association, 22*(e1), e28–e33.

Tavani, H. T. (2008). Informational privacy: Concepts, theories, and controversies. In K. E. Himma & H. T. Tavani eds., *The Handbook of Information and Computer Ethics*, 131–164. Hoboken, NJ: Wiley.

Thatcher, J. (2014). Big data, big questions / living on fumes: Digital footprints, data fumes, and the limitations of spatial big data. *International Journal of Communication, 8*(19), 1765–1783.

Turow, J., Hennessy, M., & Draper, N. A. (2015). *The tradeoff fallacy: How marketers are misrepresenting American consumers and opening them up to exploitation*. Annenburg School for Communication: University of Pennsylvania.

Upsight. (2018). About us. Retrieved from https://www.upsight.com/aboutUs/

Wang, H., Hong, J., & Guo, Y. (2015). Using text mining to infer the purpose of permission use in mobile apps. *Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, 1107–1118.

Wang, Y., Chen, Y., Ye, F., Yang, J., & Liu, H. (2015, June). Towards Understanding the Advertiser's Perspective of Smartphone User Privacy. *Distributed Computing Systems*, 288–297.

Yu, Z., Macbeth, S., Modi, K., & Pujol, J. M. (2016). Tracking the trackers. *Proceedings of the 25th International Conference on World Wide Web,* 121–132.

Zang, K., Dummit, J., Graves, P. L., & Latanya, S. (2015). Who knows what about me? A survey of behind the scenes personal data sharing to third parties by mobile apps. *Technology Science*. Retrieved from https://techscience.org/a/2015103001/