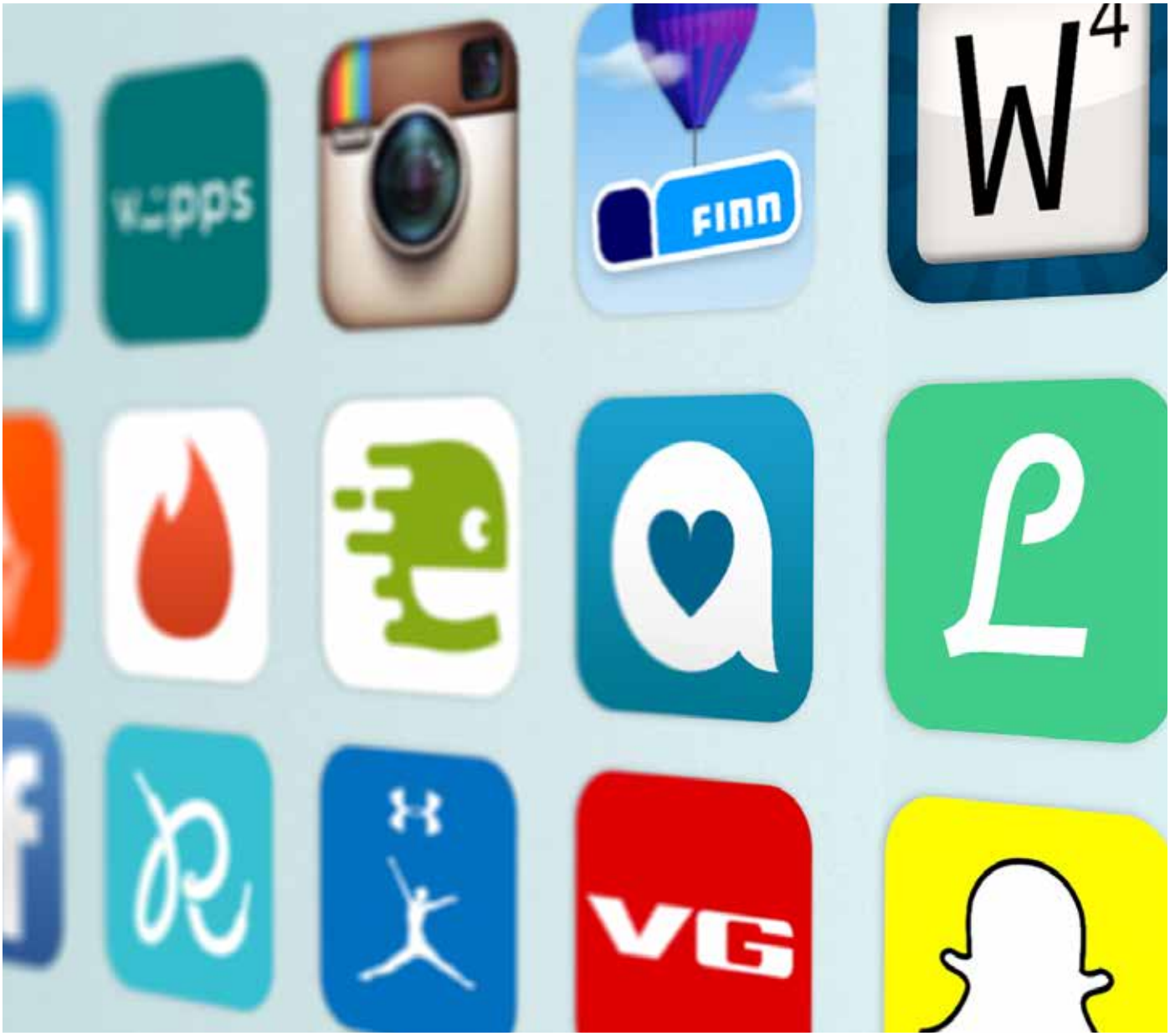

APPFAIL

Threats to Consumers in Mobile Apps

March, 2016

FORBRUKERRÅDET

The following people were involved in the study:

- Finn Lützow-Holm Myrstad, project owner
- Gro Mette Moen, senior political advisor
- Mathias Stang, advisor
- Siv Elin Ånestad, advisor
- Gyrid Giæver, legal advisor
- Øyvind Herseth Kaldestad, communication advisor
- Helene Storstrøm, graphic designer

Content

1. Summary

The Norwegian Consumer Council finds mobile apps' terms of use and privacy policies fail to uphold privacy obligations and users' consumer rights. Among the twenty apps in our research pool, we found that:

- Apps can change terms without giving users reasonable (by email etc) or advance notice. Only 4 of the apps pledge advance notice, allowing the app provider shifting capabilities or rights without the user's prior approval. Only Happn and Vipps clearly state how they will notify users about a change of terms. This lack of sufficient or advance notice is unfair (chapter 3).
- Some apps treat personal and identifiable data as non-personal data. Consequently, there is an increasing probability of personal data being processed and used counter to the demands of privacy regulations. Facebook (including Messenger), Twitter, Tinder, MyFitnessPal, Strava and Runkeeper, have unclear or ambiguous definitions of personal data (section 4.1).
- Many apps have generally unclear and complicated terms dominated by hypothetical language, such as 'may' and 'can', making it difficult for consumers to understand what the app will do. Respective to our pool of research, Snapchat, Tinder, Twitter, Instagram and MyFitnessPal have longer than average terms and use difficult and obscure language. Consequently, it is difficult for the average consumer to give informed, unambiguous consent to these terms (section 5.2).
- 7 of 20 apps fail to explain permissions and 11 of 20 apps demand permissions we find excessive or disproportionally intrusive in relation to the functionality of the app. Only 4 apps (LinkedIn, Tinder, Finn.no and Gulesider) both explain the permissions and only request permissions we understand (section 6.1 and 6.2).
- 13 of 16 relevant apps reserve the right to sublicense user-generated content to unspecified parties, while only Strava, Instagram and Happn will not. This allows the app provider to share the rights to user content with third parties. This can lead to use of the content that the user cannot foresee or approve (section 6.3).
- The apps reserve the right to share personal data with unspecified third parties for poorly specified purposes. None of the services in our research specifies with which third parties personal data is shared. Only 7 apps (Strava, LinkedIn, Finn.no, Gulesider, Nordli, VG and Vipps) clearly state that third parties may not use personal data outside the purpose of the app (section 6.4).
- 16 apps do not pledge to delete personal data after a period of inactivity. Thereby they potentially keep the information indefinitely by default. Only Finn.no, VG, Vipps and Wordfeud have time-limited data storage, but even these do not specify the length of the retention period. None of the services, according to their terms, contact former users and offer to delete their accounts if they have not used the service for a number of months or years (section 7.1).

- Endomondo, Runkeeper, Strava, MyFitnessPal, Snapchat, Tinder, Finn.no and Wordfeud Free claim perpetual or irrevocable licences to user-generated content, possibly rendering the user unable to retain control over their own content over time (section 7.2).
- 8 apps limit users' ability to withdraw consent to processing of personal data by not allowing deletion of user accounts inside the app. This includes MyFitnesspal, Instagram, LinkedIn, Snapchat, Twitter, Norli e-bok, Vipps and Wordfeud Free (section 7.3).
- 9 apps are not clear that they will delete data upon active request or termination of user account. This includes Runkeeper, MyFitnesspal, Instagram, Snapchat, Tinder, Gulesider, Yr and Wordfeud Free (section 7.4).
- A comparison between what terms pledge and actual data transfers from the apps in the report 'Privacy in mobile apps' (SINTEF, 2016), shows that apps do not necessarily adhere to their own terms and privacy policies. For example Happn sends personal data to a third party, Runkeeper tracks location when the app is not in use, and Vipps shares data with Facebook, even though the terms do not specify these capabilities (chapter 8).
- 9 apps can terminate user accounts without valid cause or notice, leaving users without access, for example, to fitness data generated over time or to a social or professional network. This includes Endomondo, Strava, Lifesum, MyFitnessPal, Instagram, Snapchat, Twitter, Tinder and Wordfeud Free. All digital services should specify what breaches justify termination of a user's service. The user should also be notified about any such decision and given the opportunity to contest it (chapter 9).

This report contests that many of the apps researched do not comply with European consumer and privacy law. This applies to both European and American services. Examples from this report can serve as the basis for further contact with app providers and complaints to relevant authorities if necessary.

Consumers do not have the option to turn back time and stop using digital services and apps. Therefore, the Norwegian Consumer Council, calls on app providers to change their terms and conditions in a consumer-friendly direction.

1. Introduction

The Norwegian Consumer Council analysed the terms, including privacy policies[1], and behaviours of 20 mobile apps. The purpose was to uncover potential threats to consumer protection hidden in the end-user terms and privacy policies of apps. This report presents a summary of the main findings and will be published as a part of a campaign on consumer protection in mobile apps. We have found what we deem to be breaches of European consumer and privacy law and hope that this report can make consumers more aware of their rights and, at the same time, raise the bar for app developers, engage enforcement agencies and contribute to making apps' business models more transparent and consumer friendly.

Why apps? The smartphone functions as both a sensor and a computer. It has become the primary digital unit. Mobile apps offer a wide range of services from which users can benefit in their daily lives. The mobile app market, however, raises concerns about consumer protection in how service providers deal with questions concerning privacy and end-user agreements.

The study was conducted by analysing terms, policies and frequently asked questions (FAQ pages) and, to some extent, using the apps. The analysis of terms and conditions was based on the methodology the Norwegian Consumer Council used to test cloud storage services in 2014[2].

The research institute SINTEF was commissioned to perform a systematic technical test[3] to detect the data flows from the apps to the service providers and third parties. The results from this test are available in a separate paper and are referred to in this report.

To limit the overall scope of the study, some topics were excluded from the analysis. We could not analyse the implications of how apps link with external devices, such as Fitbit, or how logging on to apps through Facebook or Google influences privacy.

Several services analysed are not only apps but also provide other online services. The terms and conditions generally apply to the app and other services within the brand, and in the case of Facebook and Facebook Messenger, the two services share a set of terms.

Overall, we tried to keep the study short but found it necessary to include quotations from the terms to illustrate or highlight certain points. We have included references, and we are happy to share the background materials upon request.

1 'Terms' refers to 'Terms of Services', 'Terms of Us', 'Terms and Conditions', 'User Agreement', 'Statement of Rights and Responsibilities', 'Privacy Policies' and similar policies. See the appendix for links to the reference documents for the 20 apps in question. The analysis was conducted between June and December 2015. As far as we know, only Runkeeper changed its terms between the study period and publication of this report, but the changes in these terms do not relate to any of the issues in this study.

2 '**Hazy terms in the cloud**', Norwegian Consumer Council, 2014

3 'Privacy in mobile apps', 2016, Pultier, Harrand & Brandtzæg, SINTEF

We based our assessment of the apps' terms and practices on relevant consumer and privacy laws and reasonable consumer expectations. However, this report does not constitute a complete legal or technical analysis.

Considering the millions of available apps, it was essential to limit the scope of the analysis, so we looked at only 20 apps. Even so, this analysis could only scratch the surface. Our goal was to highlight various issues, rather than analyse them in depth. We identify some problematic patterns among these apps and hypothesise that the consumer challenges we have found in these 20 apps are likely to also be present in many other apps.

The campaign on consumer protection in mobile apps is funded by the Norwegian government through the Norwegian Ministry of Children, Equality and Social Inclusion.

We wanted to shed light on several important aspects of consumer protection, and the selection of apps reflected this purpose. Firstly, we chose to look only at free apps intended for adults. Secondly, most apps, except for a few in the Norwegian category, are targeted at a global audience. Thirdly, many of the selected apps are among the most popular in their category; some are American, others European, some quite new and others more established. We also took into account findings from app sweeps conducted by the Norwegian Data Protection Authority in 2014[4] and selected apps with varying scores from PrivacyGrade, an online privacy evaluation tool. Apps were selected among three categories: health and fitness, social media and Norwegian apps.

The case to include health and fitness apps is that these apps *can* be very important tools for consumers to monitor and improve their health, and they generate sensitive, commercially valuable data. Fitness apps provide the user with exact logs of workouts, while calorie-counter apps provide nutrition logging. We chose two calorie-counter apps and three fitness apps. These apps provide similar functionalities, which makes it possible to compare them. Data gathered by these apps can be highly sensitive or reveal sensitive information about the user when collected, analysed or combined with other data sets.

The health and fitness apps were selected from among the top-listed free apps in the Health and Fitness category of Google Play and Apple's App Store in Norway on two randomly selected days (16 June 2014 and 2015):

- **Endomondo**, fitness app
- **Runkeeper**, fitness app
- **Strava Running and Cycling GPS Tracker** (Strava), fitness app
- **Lifesum**, calorie-counter app
- **MyFitnessPal**, calorie-counter app

4 'Appsveip', Norwegian Data Protection Authority, 2014

The second category of apps analysed is social media apps. They are important for consumers today in social interaction, information access, freedom of expression and many other functions. For many, it can be hard to not use a social media service or choose another network if they do not like the terms as it is difficult to move one's whole social network to another service. The definition of social media in this report includes traditional social and professional networking services and dating apps as they function in similar ways.

The social media apps selected for this study are among the most used in Norway, and most are also popular globally. Within this category, two dating apps that match users based on tracking their location are also included; one is quite new, and one is a well-known, established service. The social media apps examined in this study are:

- **Facebook** and **Facebook Messenger**, the most popular social media globally
- **LinkedIn**, which targets a professional audience and focuses on job networks
- **Snapchat**, an increasingly popular chat service that sends pictures that are shown to the receiver for only a short period of time
- **Twitter**, a service which allows publicly posting and discussing short messages
- **Happn**, a fairly new dating app
- **Tinder**, which claims to be the world's most popular dating app

For the purposes of comparison, we also included some Norwegian apps in the study. A variety of different services was selected to get an overview:

- **Finn.no**, a, highly popular digital marketplace in Norway
- **GuleSider**, a yellow pages app that provides addresses and phone numbers
- **Norli e-bok**, **an e-book** app
- **Vipps**, which enables easy money transfers regardless of bank connections
- **Yr**, a weather forecast app from the national broadcaster NRK
- **VG**, one of the largest newspapers in Norway
- **Wordfeud Free**, a Norwegian game app with international success

2. Changes in terms

Terms and conditions stipulate users' and service providers' rights and responsibilities. Many of the apps in the study are important in people's lives as they can connect users with friends and colleagues, monitor and improve users' exercise and track users' eating habits. Consequently, a negative change to terms can have impacts on the app user. The EU Directive on Unfair Terms in Consumer Contracts points out that unilateral changes to terms performed without reasonable notice to the consumer is one element that should be taken into account when assessing whether terms are unreasonable. Therefore, we analysed whether terms allow for unilateral changes without providing the consumer with reasonable notice.

Table 1. Will the app provider provide reasonable or advance notice if the terms are changed?

Social apps	Facebook	Instagram	LinkedIn	Snapchat	Twitter	Happn	Tinder
Will provide reasonable notice if terms are changed.	✓	?	✓	✗	?	✓	✗
Provides advance notice if terms are changed.	✓	?	✗	✗	✗	✗	✗

Norwegian apps	Finn.no	GuleSider	Norli e-bok	VG	Vipps	Yr	Wordfeud free
Will provide reasonable notice if terms are changed.	✓	-	?	-	✓	-	✗
Provides advance notice if terms are changed.	✓	-	?	-	✓	-	✗

More tables on the next page

Table 1. Continues

Fitness apps	 Endomon-do	 Run keeper	 Strava	 Lifesum	 My-FitnessPal
Will provide reasonable notice if terms are changed.					
Provides advance notice if terms are changed.					

Table 1 show which services, according to our analysis, provide reasonable or advance notice when making changes to their terms. Services that can change terms without such notice are marked with a red X. Services that provide such notice are marked with a green checkmark. VG, GuleSider and Yr do not demand user registration, and this limits the possibilities for notice, so we decided not to assess these apps on this point. Instagram and Twitter are marked with question marks because they have contradictory or unclear terms which made it difficult to conclude. Norli e-bok does not refer to changes to terms is also marked with a question mark.

According to our definition, reasonable notice requires that the user be actively notified through, for example, an e-mail or a notification such as a pop-up in the app. To post an updated version on the webpage of the service is *not* considered reasonable notice. Runkeeper, Tinder and Wordfeud Free regard changing the date in the heading of the terms online as appropriate notice. These services expect users to periodically check the website to see whether the date has been changed and then search the terms or policy for changes. We find that it is unreasonable to expect consumers to regularly check terms in case that they have been updated.

Fitness app Strava is an example of an app that, according to its terms, will not give any (thus, neither reasonable nor advance) notice about changes to terms. In effect, the consumer is bound by the terms, but Strava may change them at its discretion:

> *[…] you agree to follow and be bound by the Terms, which may be updated by Strava from time to time without notice to you.*
>
> Strava Terms of Service

Until recently, the cloud storage service iCloud, similar to Strava's terms, claimed a unilateral right to change the agreement 'at any time, at their own discretion and without giving users notice'. In 2014, the Norwegian Consumer Council deemed these terms 'unfair' and in breach of the Directive on Unfair Terms in Consumer Contracts and filed a complaint with the Norwegian Consumer Ombudsman. Within a few months, Apple changed these terms globally.[5]

Endomondo, Lifesum and Twitter state that they will provide notice but are not clear about how. After consideration, we have deemed this to be an acceptable practice, although we would wish for more clarity. For example, Endomondo will inform users of changes but possibly only on its site:

> *Endomondo will inform you hereof by mail, on the Site, via the Services and / or by other means deemed appropriate and adequate by Endomondo.*

Endomondo Terms and Conditions of Use

An interesting case is Instagram, which we consider to have contradictory terms on this point. While it states that it will provide 'reasonable advance notice', Instagram also states that it may give notice by simply posting notice 'on the service'. Although we find it reasonable to post the notice in the app itself through a pop-up or similar means, requiring the user to regularly check the terms is not sufficient:

> *[…] we will provide reasonable advance notice before the Updated Terms become effective. You agree that we may notify you of the Updated Terms by posting them on the Service […] Therefore, you should review these Terms of Use and any Updated Terms before using the Service.*

Instagram Terms of Use

Only Happn and Vipps clearly state how they will notify users about a change of terms; both state they will notify users via e-mail.

Although Table 1 shows that most of the app services may, according to their own terms, change terms without giving advance notice to users, there are some exceptions. Finn.no will notify users up front 'if practically possible' (our translation).

5 'Apple iCloud violates Norwegian and European law', press release from The Norwegian Consumer council, 2014

Facebook writes that advance notice will be given, but is not clear how. Although we find these statements to be a bit unclear, we have deemed Facebook and Finn.no's practices to be more acceptable than those of many other apps. However, Facebook's approach has been heavily criticised.

> The Belgian Privacy Commission commissioned Belgian researchers from the universities KU Leuven and Brussel (VUB) to complete a report on Facebook's policies and terms. According to this report, a German court has invalidated Facebook's provision for unilaterally changing terms and conditions due to the 'significant imbalance'.[6]

Vipps is clear about how and when advance notice will be given and pledges that it will make changes unfavourable to users only if it has given users two months' advance notice. One example of a change in Vipps' terms considered in users' favour for which notice was not given is lowering the fee for money transfers.

Facebook, Finn and Vipps have been found to have more acceptable terms among those analysed and will provide notice both when and in advance of changing terms. Endomondo, Lifesum, MyFitnessPal, LinkedIn, Twitter and Happn will provide notice only when changing terms, not in advance.

Some apps will not, to our knowledge, provide reasonable or advance notice about changing terms, so we find that Runkeeper, Strava, Tinder, Snapchat and Wordfeud Free provide significantly less predictability and safeguards in changing terms than consumers should expect from digital services. According to our analysis, this failing is in breach of the Directive on Unfair Terms in Consumer Contracts.

6 'From social media service to advertising network', KU Leuven, 2015

3. Personal data

Personal data are defined in European[7] legislation as data that can be connected to a person, even if the possibility of identifying the person based on the information is limited. Even if each piece of information is not identifiable, data are still personal if the accumulated data can be connected to a person[8]. Collecting, treating or using personal data results in a number of obligations for the controller of that data.

Some information is by itself enough to identify, contact or locate a person and, hence, is personal data per se. Examples of such data are names, address, telephone numbers, e-mail addresses, national identification numbers and photos showing a person's face. In online communities, user names are also considered personal data as they often contain a person's full name and can be used across several services.

According to researchers at Massachusetts Institute of Technology (MIT), only four spatio-temporal points are needed to identify an individual, and two randomly chosen points '*can uniquely identify more than 50% of the individuals*'[9]. Precise location and user behaviour can be connected to a person, so they are considered personal data. Therefore, we consider that all the apps we have reviewed collect, treat or use personal data[10].

Personal data can be combined and used in ways the users of digital services cannot foresee, even to their disadvantage through identity theft or price discrimination. Therefore, it is important that digital services do not collect more data than needed to provide the service and that they are open and clear about how data are collected, handled, stored, used and finally deleted.

3.1. Ambiguous definitions of personal data

If data are considered personal, the controller has obligations in how it treats the data, while non-personal data may be handled more freely. We, therefore, have looked at whether some apps define personal data as non-personal.

7 EU Data Protection Directive 95/46/ec, article 2 and the Norwegian law on personal data **Ot.prp. nr. 92(1998–1999)**, p. 101

8 '**Guidance to anonymization'**, the Norwegian Data Protection Agency, p 5–6, 2015 (our translation of title)

9 '**Study shows how easy it is to determine someone's identity with cell phone data**', Phys.org, 2013

10 At the time of analysis, Yr's terms were not available online. Since then, the terms have been made available, but due to time constraints, it has not been possible to update the report.

Most app providers do not clearly define what they view as personal data. In general, personal data is a very broad term in European legislation and covers both information the user provides to the app and information automatically gathered by the app. This is clearly acknowledged by the fitness app Endomondo:

> *Endomondo is among other regulation subject to the Danish Act on Processing of Personal Data. The Act adopts the European Union Directive 95/46/EC on the Protection of Individuals with regard to the processing and free movement of personal data. In this Privacy Policy personal data is referred to as personal information.*
> *[…]*
> *When you use the Services additional personal information may automatically or voluntarily be collected from you. Such personal information may include information on your athletic or recreational activities such as location information (GPS-data) and other exercise and performance information, e.g. time, speed, time spent on your activity, cadence, heart rate etc.*

Endomondo Privacy Policy

Although this term is the best example of a broad, inclusive definition of personal data we found, it still leaves out certain types of data which Endomondo receives: according to the EU advisory group of data protection authorities, known as the Article 29 Data Protection Working Party, technical data, such as unique device identifiers and location data, 'can have significant impact[s] on the private lives of the users' and are considered personal data[11]. IP addresses should also be considered personal data:

> *Unless the Internet Service Provider is in a position to distinguish with absolute certainty that the data correspond to users that cannot be identified, it will have to treat all IP information as personal data, to be on the safe side.*

Article 29 Data Protection Working Party[12]

Two apps, Happn and Lifesum, do not mention in their terms whether any technical data are collected and treated, even though they both require access to, for example, the device ID in the Android version of the app. All other social networks and fitness apps mention the collection of technical data but discuss it separately from personal data, making it difficult to ascertain whether technical data are treated differently than personal data.

11 '**Opinion 02/2013 on apps on smart devices'**, Article 29 Data Protection Working Party, 2013

12 '**Opinion 4/2007 on the concept of personal data'**, p. 17, 2007

Some apps, such as Tinder, seem to define as personal information as only information that can directly identify or reveal how to contact a consumer:

> *We may collect information that can identify you such as your name and email address ("personal information") and other information that does not identify you.*

Tinder Privacy Policy

In Tinder's case, 'personal information' seems to encompass only 'personally identifiable information' (PII), a legal term based in US privacy law. PII is a concept used by many apps, whether explicitly by name or implicitly, as in the Tinder example, and seems to be the norm for US-based apps. Demographic personal data, such as age, physical traits, gender and general location, are often described by the US term 'non-personally identifiable information'. Under European data protection law, this information is personal data and has the same data-processing requirements, so differentiating between identifying and non-identifying information does not change the legal requirements in the EU.

Similarly to Tinder, MyFitnessPal uses the term 'personal information', specifically excluding IP address and device information. 'Mobile Device Data' according to MyFitnessPal's Terms of Use, include unique device identifiers and location but are not included in the definition of personal information. In addition, MyFitnessPal defines as non-personal behavioural or technical data that, according to the definition of the Article 29 Working Party, should be considered personal:

> *MyFitnessPal automatically gathers information of the sort that browsers automatically make available, including: (i) IP addresses; (ii) domain servers; (iii) types of computers accessing the Website; and (iv) types of Web browsers accessing the Website (collectively "Traffic Data"). Traffic Data is anonymous information that does not personally identify You.*

MyFitnessPal Privacy Policy

Interestingly, Facebook also does not use the term 'personal data' but *does* use the term 'personally identifiable information', even though the data controller is Facebook Ireland, which is subject to European legislation:

> *… personally identifiable information is information like name or email address that can by itself be used to contact you or identifies who you are*

Facebook Data Policy

This is problematic as Facebook states that it shares with advertisement and analytics partners 'Non-Personally Identifiable Information', which could include many other forms of personal data.

We do not share information that personally identifies you […] with advertising, measurement or analytics partners unless you give us permission. We may provide these partners with information about the reach and effectiveness of their advertising without providing information that personally identifies you, or if we have aggregated the information so that it does not personally identify you.

Facebook Data Policy

Behavioural data encompass log data about consumers' actions in apps and their location, shopping habits, websites visited, training preferences, nutritional information and data gathered using cookie. Calorie counters collect users' nutritional and weight data over a long time period, which can be valuable to researchers, grocery chains and insurance companies, while sports trackers can track how people move in a city, helping city planners and making it possible to advertise relevant merchandise.

It is problematic that many privacy policies do not seem to recognise technical and behavioural data as personal. Furthermore, personal demographic data, such as age, physical traits, gender and general location, are often classified under the US term non-personally identifiable information. Under European data protection law, all such data are personal and have the same data-processing requirements.

If a service does not define personal data as such, there is an increased possibility that data will not be treated in accordance to privacy regulations. Therefore, it can be a problem that some categories of personal information are not recognized as such in apps. Their privacy policies could contain misleading or incorrect statements about how personal information is handled. In our survey, many apps, including Facebook, Twitter, Tinder, MyFitnessPal, Strava and Runkeeper, have unclear or ambiguous definitions of personal data, while other apps, including Snapchat and Instagram, lack such definitions at all. Apps that have adequate definitions of personal data or refer to European law, such as Endomondo, Lifesum, Happn, Vipps and Finn, are all headquartered in Europe.

4. Consent

As shown, apps retrieve and process personal data. The app provider normally reserves the right to place information on a device and retrieve data from a device. Consent provides the principal applicable legal grounds for placing app content on the device and processing personal data. According to the EU Data Protection Directive[13], the app provider should have the user's consent to process personal data.

User consent for the app provider to retrieve and process personal data is subject to the condition that the consent is specific and informed and is freely given [14]. User consent must be given before the app places information on and retrieves information from the device[15] and must be based on clear, comprehensive information provided to the user.

According to the European Commission, the recommended method for gaining consent for health apps is granular consent. This advice also applies to all other apps that require access to personal data:

> *Consent should be obtained using the most effective means to communicate with users. Granular consent, in which consent is sought during various stages of the use of the application, with additional consents being sought when a user uses the app in a new manner, can be considered a good practice if this permits the user to exercise better or more effective control over his or her personal data. Thus, consents can be obtained when installing it or at various times during use, as long as consent is obtained before processing begins.*[16]
>
> European Commission

13 Directive 95/46/EC–Data Protection Directive, article 7

14 Directive 95/46/EC–Data Protection Directive, article 2 (h)

15 Directive 2002/58/EC–ePrivacy Directive, article 5(3); see also Directive 95/46/EC–Data Protection Directive, article 7

16 'Draft code of conduct on privacy for mobile health applications', European Commission, 2016

4.1. Specific and freely given consent

We analysed whether terms are available online, in Google Play and during downloading and registration so that interested consumers can find and consider them. We have also looked at whether the user must actively consent to the terms during registration or downloading.

Table 2. Are the terms available online, in Google Play and during the downloading or registration process?

Social apps	Facebook	Instagram	LinkedIn	Snapchat	Twitter	Happn	Tinder
Terms available online.	✓	✓	✓	✓	✓	✓	✓
Terms available in Google Play.	✓	✓	✓	✓	✓	✓	✓
Terms available in downloading or registration process.	✓	✓	✓	✓	✓	✗	✓

Norwegian apps	Finn.no	GuleSider	Norli e-bok	VG	Vipps	Yr	Wordfeud free
Terms available online.	?	?	?	✓	✓	✗	✓
Terms available in Google Play.	✓	✗	✗	✓	?	✗	✓
Terms available in downloading or registration process.	✓	✓	✓	✗	✓	✗	✗

More tables on the next page

Table 2. Continues

Fitness apps	Endo-mondo	Runkeeper	Strava	Lifesum	My-FitnessPal
Terms available online.	✓	✓	✓	✓	✓
Terms available in Google Play.	✓	✓	✓	✓	✗
Terms available in downloading or registration process.	✓	✓	✓	✗	✓

Table 2 shows which services have terms available online, in the app store Google Play or during downloading and registration of the service (green checkmark) and which apps do not (red X).

Users should be informed about terms, so the terms should be easily available. App terms, for example, might be available online on the service's website, in an app store (for Table 2, we searched Google Play, not Apple's App Store), in the app/ service, as a link or as an item which must be accepted during the process of consenting to the terms.

Most of the apps make their terms available on their webpages. An exception is the weather service Yr, which, at time of analysis, did not have any available terms, conditions or privacy policy. For GuleSider, Norli e-bok and Finn.no, it is difficult to find the relevant terms online. These apps are only single services provided under larger brand names. For example, in the case of Finn.no, there are several terms and documents that could be relevant. Vipps has terms in the app and on its website but links to a different set of terms and privacy policy from the Apple App Store and Google Play. These four apps were difficult to conclude on and are therefore marked with a yellow question mark in the table. VG has a privacy policy but no other terms. Most apps link to their privacy policies in Google Play; only four do not: MyFitnessPal, GuleSider, Norli e-bok and Yr[17]. In general, the social media and fitness apps analysed have more terms available online and in Google Play than the Norwegian services.

Terms should be available during the registration process as this is when the user gives consent. Terms documents posted on the app provider's web site are not considered easily available to the user. Most of the apps (see Table 2, second row) link to terms and conditions during the downloading or registration process.

17 Some apps also have the terms available in the app, but these are available after consenting to the terms, so we have not included them in Table 2.

The terms, though, typically are referred to in fine print at the bottom of the page, as in the case of Instagram, and do not require specific action by the user.

We find that, in many apps, the contract between the user and the app service provider usually is concluded more or less explicitly during the process when the user downloads the app or registers an account. Many apps state that, by installing or using the service, the user automatically accepts its terms, conditions and privacy policy:

> *By installing our mobile application or in other way using or accessing our Services, you accept the terms and conditions of this Privacy Policy and the processing of your personal data.*

Lifesum Privacy Policy

In our opinion, clauses that claim that the user accepts the terms by using the service or accepts data sharing by using the app are not specific as proscribed by the Data Protection Directive, and we find the level of consent to be questionable. To be specific, consent should refer clearly and precisely to the scope and consequences of the data processing.

Lifesum, Happn, VG, Yr and Wordfeud Free do not link to their terms and conditions during installation and account set-up. It is problematic that the user automatically consents to data processing through use of the service without provision of links to relevant documents available directly during the process of downloading the app.

In Vipps, the user must actively click to agree to the terms and conditions before starting to use the app. During the registration process for Facebook, the user must click to continue from a page that explains acceptance of the terms. This explicit acceptance of terms is the exception, not the rule, among the apps we analysed. When processing personal and sensitive data, service providers should seek active consent. We question whether services that do not make the user actively aware of the terms while installing the app or establishing an account fulfil their obligations on this point.

We recommend that all app providers which collect personal data seek active consent to the collection and processing of such data, preferably when such data are accessed and, at a minimum, when the user starts using the service. One, though, could argue that demanding active consent through clicking boxes and pop-ups will lead to consent fatigue among users.

Many of the apps share personal data with third parties and should gain explicit consent to do so (for more on how services share data, see section 6.4). In the health and fitness apps studied, the user can pay a premium to access extra functionality. In Endomondo, paying the premium also affects privacy:

> *By using the Service without being a Premium subscriber, you explicitly consent to the sharing of de-identifiable personal information like age, gender, sports and precise location data with our advertising partners, including but not necessarily limited to Google.*

Endomondo Privacy Policy

It is interesting to note that, by using the free version of the app Endomondo, the user explicitly consents to share data with advertising partners. In our opinion, the condition of giving informed, specific consent is not fulfilled as this term is not made accessible and visible but is hidden in the privacy policy. It is not possible to give informed consent to using data as a payment method when the user does not know the market value of the data.

Also, according to the SINTEF-report 'Privacy in mobile apps' (2016), Endomondo 'sends the GPS-position, age and gender to Google's advertisement service and to a tracker (Rubion Project)'. Looking at the data flow more closely, data packages that localise a female, age 18-24 at the SINTEF building in Oslo (GPS coordinates: 'lat=59.94480773933592' and 'lng=10.7130302508024'), is sent to the domain'pubads.g.doubleclick.net'. We question how this combination of gender, age and location qualify as 'de-identifiable' and therefore if the user has given informed consent.

In addition to consenting to the terms, the user gives the service permission to access certain types of data (for more details, see section 6.2). In Android phones, such as Samsung and HTC, the user gives the app access to a list of permissions, such as contact list and location, as a step in the downloading process. On iOS phones, these permissions are requested when needed to provide functionality. We find that requesting data when access is needed is more appropriate as it gives the user the opportunity to consider the purpose of the permission and to give consent when relevant. Blanket consent to all permissions upon downloading the app is not sufficient and does not give the app provider incentive to limit permissions. Android's new Marshmallow version 6.0, which is implemented on newer Android devices, is more similar to the iOS platform and requests permissions when needed. This is a step in a positive direction for consent to permissions to access data on mobile phones.

4.2. Understandable terms and informed consent

Article 5 of the EU Unfair Contract Terms Directive (UCTD) states that, 'in the case of contracts where all or certain terms offered to the consumer are in writing, these terms must always be drafted in plain, intelligible language'.[18] To determine whether terms are readable, we assessed term length and whether the contact terms are written in what we judge to be plain, understandable language. We also considered measures taken by app providers to make their terms easy to read and the extent of the use of hypothetical language, such as 'can' and 'may'.

Table 3. Are the terms readable in terms of length and clarity of language, and has the service provider made efforts to make the terms understandable?

Social apps	Facebook	Instagram	LinkedIn	Snapchat	Twitter	Happn	Tinder
No. of pages (average 13).	15	17	28	16	13	11	18
Total nr of Words (average 5700).	6208	7636	11838	6848	6841	4343	8399
Total no. "may" and "can" (average 59,3).	32	107	138	77	77	20	85
Clear language.	✓	✗	✓	✗	✗	✓	✗
Efforts to make readable.	✓	✗	✓	✗	✗	✓	✗

More tables on the next page

18 Unfair Contract Terms Directive (UCTD)

Table 3. Continues

Norwegian apps	Finn.no	GuleSider	Norli e-bok	VG	Vipps	Yr	Wordfeud free
No. of pages (average 13).	17	8	3	7	8	–	8
Total nr of Words (average 5700).	5911	2532	1388	2611	2738	–	4100
Total no. “may” and “can” (average 59,3).	76	31	12	47	44	–	52
Clear language.	✓	✓	✓	✓	✓	–	✗
Efforts to make readable.	✓	✗	✓	✓	✓	–	✗

Fitness apps	Endo-mondo	Runkeeper	Strava	Lifesum	My-FitnessPal
No. of pages (average 13).	15	12	18	8	23
Total nr of Words (average 5700).	6152	5507	7386	3295	9076
Total no. “may” and “can” (average 59,3).	52	54	50	30	83
Clear language.	✗	✗	✓	✓	✗
Efforts to make readable.	✓	✗	✓	✓	✗

In Table 3, apps which have a less than average number of pages, words and uses of ‘may’ and ‘can’ are marked in green, while those with a higher than average number are marked in red. The services marked red have comparatively clear language or have made specific efforts to make the terms readable, while those marked with a red X have done the opposite.

To be valid, consent to the sharing of personal data must be 'informed' and 'unambiguous'[19]. If terms are very difficult to read as they are very long, ambiguous or written in overly technical, complex or vague language, a strong case can be made that informed consent is not possible for most consumers. A May 2014 report to the US president on big data and privacy[20] stresses this important point:

> *The framework for notice and consent is also becoming unworkable as a useful foundation for policy. […] Only in some fantasy world do users actually read these notices and understand their implications before clicking.*
>
> Executive Office of the President President's Council of Advisors on Science and Technology

In the 18 terms and conditions studied, we found that 11 app providers (Endomondo, Strava, Lifesum, Facebook (including Messenger), LinkedIn, Twitter, Happn, Finn.no, Norli e-bok, VG and Vipps) had taken concrete measures to make their terms easier to read.

Examples of measures some apps have taken to make terms easier to understand:

Strava:

- Presents the most important highlights at the beginning of its terms

Endomondo

- Presents the most important highlights at the beginning of the terms
- Gives a review of the defaults regarding with whom private data are shared (e.g. birthday: public, weight: only me, height: public)

Facebook (including Messenger)

- Includes clear content overview with informative symbols in the privacy policy
- Presents content in short paragraphs with guiding headlines

Norli e-bok

- Has short terms presented in clear language (3 pages)
- Writes short paragraphs with informative headings
- LinkedIn:
- Shares a short version of the main content of the terms in the left margin
- Presents two short illustrative videos explaining the privacy policy and user agreement
- Uses banner symbols with shortcuts to sections of the privacy policy, such as 'Information collected' and 'Uses and sharing of personal information'

19 'The great data race', p. 29, The Norwegian Data Protection Agency, 2015

20 'Big data and privacy: a technological perspective', Executive Office of the President President's Council of Advisors on Science and Technology, 2014

LinkedIn's terms are the lengthiest we analysed (28 pages and 12,103 words). A short version in the left margin on the terms page highlights both positive and potentially problematic aspects of the terms and gives the user useful pointers to relevant parts of the terms. The short video version, though, seems to focus only on the positive aspects of the terms and gives less useful pointers.

We found that Vipps, Norli e-bok and, to some degree, Happn have short contract terms[21] with relatively plain language. Although Strava's terms are among the longest in the study, they use plain language presented in a question–answer format, so they are among the easiest terms to read. In contrast, Worfeud's terms are quite short but are written in more complex legal language, which makes them harder to understand. A typical example is the repeated use of 'may' and 'certain methods' which makes it difficult to understand how data will actually be collected:

> *Bertheussen IT may employ third party ad serving technologies that use certain methods to collect information as a result of ad serving through Services.*

Wordfeud Free Privacy Policy

In the majority of the contract terms, we found extensive use of the term 'may'. We have found it necessary to take the worst-case scenario interpretation as our point of departure: the user must assume that the services will actually do what the terms say they 'can' or 'may' do. When used in combination with technical terms, such as 'hashed', 'third parties', 'IP address' and 'cookies', the use of 'may' can make it difficult for users to fully comprehend what the terms actually mean, as shown in the following example from Tinder's privacy policy:

> *We may combine non-personal information we collect with additional non-personal information collected from other sources. We also may share aggregated, non-personal information, or personal information in hashed, non-human readable form, with third parties, including advisors, advertisers and investors, for the purpose of conducting general business analysis or other business purposes. For example, we may engage a data provider who may collect web log data from you (including IP address and information about your browser or operating system), or place or recognize a unique cookie on your browser to enable you to receive customized ads or content.*

Tinder Privacy Policy

21 Most of the apps we analysed have both a terms document and a privacy policy. Both documents have been included in the assessment in Table 3. When measuring the length of contracts, the two documents have been combined. Yr does not have terms or a privacy policy, so it is not included. Facebook and Facebook Messenger have identical terms and have been merged inn all tables throughout the report. We could find only a Privacy Police, not Terms of Service, for the VG app.

Thus, the reader of Tinder's privacy policy should assume that Tinder *will* combine non-personal information with additional non-personal information and share it in accordance with the description above. Another rather common feature that contributes to the vagueness of terms is the inclusion of broad, ambiguous exceptions, as shown in MyFitnessPal's privacy policy:

> *Except as otherwise provided in this Privacy Policy, and when You otherwise give permission or under the following circumstances, MyFitnessPal will not share Your Personal Information with third parties.*

MyFitnessPal Privacy Policy

Some apps have clearer terms. For example, Lifesum explicitly describes the user's right to access and correct personal data:

> *You have the right to ask what personal data that we hold about you and to ask us to update and correct any out-of-date or incorrect personal data that we hold about you. Lifesum is obliged to once per annum provide you with a notification, free of charge, of whether personal data concerning you is processed or not.*

Lifesum Privacy Policy

We found that the terms for ten of the apps assessed (Strava, Lifesum, Facebook, Messesnger, LinkedIn, Happn, Finn.no, Norli e-bok, VG and Vipps) can be said to have clear language and to reflect concrete efforts to make the terms more readable. However, four of these apps have very long terms (Strava, Facebook, Messenger, LinkedIn and Finn.no). The average length of the 18 terms assessed is 14 pages, which, in our view, is too lengthy for the average consumer to read. One, however, keep in mind that Facebook, for example, delivers complex services, and three pages would probably not cover the necessary topics.

In conclusion, our assessment of readability shows that five apps (Snapchat, Tinder, Twitter, Instagram and MyFitnessPal) have terms longer than average among the assessed apps, use language we consider difficult and do not make efforts to make the terms easier to read. Consequently, it can be difficult for the average consumer to give informed, unambiguous consent to these terms.

Four apps (Lifesum, Happn, Norli e-bok, VG and Vipps) tick the boxes for clear language, shorter than average text length and efforts to make terms easier to read. Short terms, though, also have disadvantages. For Instance, Norli e-bok's terms (the shortest in this analysis) fail to mention issues, such as how terms may be changed (for more details, see section 3).

Consent and sensitive data

Article 8 of the EU Data Protection Directive (Directive 95 / 46 / EC) defines sensitive data as personal data revealing individuals' racial origins, political opinions, religious or philosophical beliefs, trade-union membership, health status or sex life. Handling sensitive data imposes extra obligations, and problems can arise if sensitive data are not handled as such. We have chosen to focus on sensitive data in two calorie-counter apps, MyFitnessPal and Lifesum, and two dating apps, Happn and Tinder.

Non-sensitive data can become sensitive when combined, even with other non-sensitive data. For example, the location, contact ('show me your friends, and I'll tell you who you are'), nutritional and other data collected by the apps in this study can create sensitive personal data as described in Article 8. Therefore, most of the apps in this study, particularly the social media and health and fitness apps, could collect and process sensitive data.

> Revealing the mere fact that people use a specific digital service can cause problems for individuals, as when Ashley Madison, a dating service that specialised in persons already in a relationship, was hacked and user identities published.[22]

For the calorie-counters and dating apps, sensitive data directly related to health and relationship status (thus implicitly sex life) are core elements. That someone uses a calorie counter implies a wish to control caloric intake and might have implications about the person's weight and health. One can infer quite sensitive information from just knowing that someone uses Lifesum, MyFitnessPal, Happn or Tinder.

Therefore, it can be problematic that MyFitnessPal claims the right to publish users' real or user names and requires that users waive their privacy rights in relation to user-generated content (for more on user-generated content, see sections 6.1 and 6.2):

> *You further agree that this license includes the right for the MyFitnessPal Parties to publish, display or otherwise use and make available your User Content and possibly your name and/or any user name of yours in connection with their exercise of the license granted under this section. You agree to waive, and hereby waive, any claims arising from or relating to the exercise by the MyFitnessPal Parties of the rights granted under this section, including without limitation any claims relating to your rights of personal privacy and publicity.*

MyFitnessPal Terms of Use

22 "Ashley Madison hack: your questions answered", the Guardian, August 20, 2015

An analysis of data practices and privacy risks in 43 health and fitness applications exposed thought-provoking examples of how sensitive data can be used in ways the user cannot predict: 'For instance, one well-known company's app lets users learn about particular drugs. What they don't tell you is that the names of drugs researched by users are sent to third-party advertisers, who can link that data to the user's web browsing history'.[23]

According to the Article 29 Data Protection Working Party[24], health data include both data generated in a professional medical context and sensor data that can be used by itself or in combination with other data to draw conclusions about a person's health status and risks.

In November 2015, the Dutch Data Protection Authority (DPA) released a report assessing the fitness app Nike + Running. The DPA concluded that data processed by Nike + make it possible to establish whether a user's health is deteriorating or improving and that this information, therefore, is 'special personal data' and can be defined as health data. In this context, the DPA found several violations of regulations. Following the report, Nike agreed to change several aspects of the app. It has become optional to share some data, such as height and weight), the information about processing of data will be improved and a retention period for inactive users will be introduced.[25]

Once, for example, weight data are collected over a period of time, it can be possible to infer users' health condition, even without combining the data with any additional data collected. The calorie-counter apps clearly collect sensitive data and possibly health data.

23 'Technical analysis of the data practices and privacy risks of 43 popular mobile health and fitness applications', Njie, 2013

24 'ANNEX health data in apps and devices', the Article 29 Data Protection Working Party

25 'Selection from DPA investigation Nike + Running app', Dutch Data Protection Agency, 2015

These apps, though, do not explicitly define what data they handle as sensitive, only as 'personal':

> *… among the personal data we may collect from you are: your email address, first and last name, height, weight, date of birth and gender. We may also, depending on your use of the Services, collect personal data about your calorie intake, weight loss goal/weight gain goal, activity/diet routines, your body measurements and BMI.*

Lifesum Privacy Policy

> *Personal Information includes, without limitation: (1) "Contact Data" (personally identifiable information about You, such as Your name and email address, as well as Your friends and contacts, if you enable access to Your contacts and address book information); and (2) "Demographic Data" (personal information about You (but doesn't specifically identify You), such as Your gender, birthday, zip code, country, height, weight, lifestyle and exercise frequency); and (3) "Fitness Data" (information about Your use of the Services (but doesn't specifically identify You), such as Your caloric intake, nutritional statistics, fitness activity, and weight loss/gain).*

MyFitnessPal Terms of Use

When setting up a profile in MyFitnessPal or Lifesum, users must report weight, height, weight goal, activity level, gender, country and birth date. Although a calorie counter would not function as well as a weight-loss tool without access to users' weight, weight goals, height and probably gender, one can question whether birth date is required. In addition to the data filled in by the user, MyFitnessPal also can access location and have a step counter functionality. The calorie-counter apps, demand much sensitive data that can be combined and give insight into users' health.

The criticism of the Nike+ Running app indicates that the two calorie counters should be modified similarly to Nike +, making registering height, gender, and birth date optional. The apps should also, like Nike + did, introduce a retention period for inactive users (for more on the indefinite storage of personal data, see section 7.1).

According to Happn's terms, by becoming members, users accept that their photos can be used to promote the application:

> *By becoming a Member, the user accepts the publication of his/her photos on the Application as well as on all materials happn deem appropriate for the promotion of the Application and its Members.*

Happn Terms and Conditions of Use

This provision is quite intrusive as the pictures according to the Terms and Conditions of Use 'must bear an accurate likeness to the Member' and can be used in a context where others will know that the person has used the dating app.

So how does Happn gain access to user's pictures? When registering for Happn, the user must log in through Facebook. At one point during the registration process, Happn lists the kinds of data it accesses through the user's Facebook account (public profile, friends list, e-mail address, birthday, work experience, pictures, personal description and likes). Clicking further at this point allows Happn to access all the user's Facebook pictures. If the user instead clicks a link to a control board, the user can choose to not let Happn access some of this data.

On one hand, privacy settings can provide the user with control of data, but on the other hand, they can also give the user a false feeling of control if, for example, the defaults are too wide, as in the case of Happn's access to users' Facebook pictures. It is worth noting that Tinder's terms and default settings relating to pictures contain similar problematic features as Happn and that, in addition, the license is 'irrevocable' and 'sub-licensable' (for more on user-generated content, see sections 6.3 and 7.2).

According to KU Leuven researchers studying Facebook, 'default settings which are configured to disclose information without the active engagement of the user do not constitute unambiguous consent'[26]. We consider this argument to also apply to the dating apps' access to user data and pictures. We find that the dating apps' access to data through vide defaults does not constitute unambiguous consent. If the default were that pictures and other personal data were not shared but the user could actively share them with the service, the practice would be more acceptable. The dating services' overly broad licences regarding users' pictures make this issue even more problematic from a privacy perspective.

These services and other apps that might deal with sensitive data should limit the amount of data collected about users, especially personal and sensitive data. Only data needed to perform the service should be collected. Apps should require active consent to more drastic and intrusive provisions, instead of hiding these provisions in terms and privacy policies. The defaults on sharing personal data should follow the principle of opt-in, not opt-out. For apps that process personal and sensitive data, especially when touching upon health data, the code of conduct for privacy in mobile health applications being developed by the European Commission can serve as a useful toolbox for developers[27].

26 'From social media service to advertising network', KU Leuven, 2015

27 'Draft code of conduct on privacy for mobile health applications', European Commission, 2016

5. Limitations of purpose

According to privacy regulations[28], those who collect, treat or use personal data must limit the scope and time span of treatment of data. The treatment of data must be limited to what is relevant and adequate[29] to provide the service. This implies, among other limitations, that data should not be used for purposes other than that for which they were collected. (The issue of time-span limitations is discussed in section 7.) For example, Runkeeper's privacy policy states that, '*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*'. This statement is an example of a purpose limitation in which, according to the terms, data will be used only for the purposes for which they were collected.

We analysed how the 20 apps deal with limitations of purpose in regards to permissions to access personal data on app users' devices, whether the licenses to user-generated content are too broad and how services may share data and licences with third parties.

5.1. Explanation of permissions

Apps request permission to access data, such as contact lists, and functionalities, such as access to the camera (for more on consent to permissions, see section 5.1). Apps should explain why they need access to personal data to provide their service. If such explanations are not available, users cannot make informed decisions about downloading and using apps. Therefore, we analysed whether the apps explain permissions.

Table 4. Does the app explain the required permissions, and are the permissions understandable?

Social apps	Facebook	Instagram	LinkedIn	Snapchat	Twitter	Happn	Tinder
Permissions are explained.	✓	✗	✓	✓	✓	✗	✗
The app does not require permissions we do not understand or find disproportionally intrusive in relation to the functionality of the app.	✗	✓	✓	✓	✗	✓	✓

More tables on the next page

28 Directive 95/46/EC - Data Protection Directive
29 Directive 95/46/EC - Data Protection Directive, article 6

Table 4. Continues

Norwegian apps	Finn.no	GuleSider	Norli e-bok	VG	Vipps	Yr	Wordfeud free
Permissions are explained.	✓	✓	✗	✓	✓	✗	✗
The app does not require permissions we do not understand or find disproportionally intrusive in relation to the functionality of the app.	✓	✓	✗	✗	✗	✓	✗

Fitness apps	Endo-mondo	Runkeeper	Strava	Lifesum	My-FitnessPal
Permissions are explained.	✓	✓	✗	✓	✓
The app does not require permissions we do not understand or find disproportionally intrusive in relation to the functionality of the app.	✗	✗	✓	✗	✗

Table 4 shows whether we found explanations for permissions that apps require (in Android's pre-Marshmallow version) and whether the apps require only permissions that, in our understanding, are essential for using the app (in Android's pre-Marshmallow version and iOS)[30]. Apps that do not explain permissions or require one or more permissions that seem excessive are marked with a red X. Apps that explain permissions and only require permissions that seem necessary and proportional to the service are marked in green.

30 We have focused on Android devices before the release of the 6.0 Marshmallow version of the operating system as the majority of users still use older versions of Android according to **Dashboards**, Android.

We searched Google Play, FAQs and apps' terms and privacy policies for explanations for requiring permissions[31]. We did not systematically check information provided in Apple's App Store as iOS permissions are explained and granted as the user uses the service.

In the first row of Table 4, a green mark indicates that one or more permissions are explained. This does not necessarily mean that all permissions are explained or that the explanation is clear enough for the user to understand the need for the permission. Some apps, such as Endomondo and Runkeeper, explain some permissions (first row), but we still find that they require questionable permissions (second row; see section 6.2). In contrast, Yr does not explain any permissions, but we understand the few permissions that it does require.

Table 4 shows that, among the services we have analysed, we find that Strava, Instagram, Happn, Tinder, Norli e-bok, Yr or Wordfeud Free do not explain the permissions they require when users downloads the apps from Google Play.

5.2. Requests for reasonable permissions

An overall principle[32] is that processing of personal data should be fair and balanced. Apps should not ask for access to more data than necessary to fulfil their service. Therefore, we analysed whether, in this context, we find the permissions understandable or disproportionally intrusive relative to the app's functionality (see Table 4).

That apps access data through requiring permissions to access, for example, location data is not in itself problematic, but some mobile apps request access to data types not necessary for the functionality of the app. One reason for such requests is the app provider's desire to monetise user data.

> According to the American Federal Trade Commission (FTC), in 2013, the app Brightest Flashlight Free, transmitted or allowed the transmission of data to third parties including advertising networks. This included precise geolocation and device identifiers, and made it possible to track users' location over time[33]. According to FTC, the service 'deceived consumers with a privacy policy that did not reflect the app's use of personal data and presented consumers with a false choice on whether to share their information'[34].

31 The permissions were analysed in June and July 2015.
32 Data Protection Directive, Directive 95/46/EC, article 6
33 '**Complaint**', FTC, 2013
34 '**FTC Approves Final Order Settling Charges Against Flashlight App Creator**', FTC, 2014

If, after searching Apple's App Store and Google Play and apps' FAQs and terms and testing apps' functionality, we still did not understand why one or more permissions requested were required for the functionality or found that the service required access to personal data that we did not view as proportionate, we regarded the permission as questionable.

It should be easy for the consumer to understand how allowing access to personal data provides useful functionality in return. However, the game app Wordfeud Free does not explain how permission to access users' 'telephone status and identity' helps provide a good service, and it is difficult for an ordinary user to understand this reason without an explanation. Other permissions are clearly relevant for the functionality of the app. For example, access to contacts makes it possible to invite friends to play Wordfeud Free, and access to files, such as pictures, enables making a profile picture. According to the research institute SINTEF's report for the Norwegian Consumer Council[35], some permissions are needed only for tracking and targeted advertising. The paid Wordfeud version requires fewer permissions.

It is difficult to understand why the Android version of the e-book application Norli e-bok requires users' exact position when we do not find any functionality of the app that seems to rely on location. However, the weather app Yr.no requests permission to access only location, which is understandably necessary for showing the weather forecast for the user's location.

If more apps explained why they require various permissions, we likely would find that more services require only necessary permissions. Runkeeper explains most requested permissions online[36] but fails to state why it needs access to the user's call log. The explanation under the heading 'Your Social Information' addresses only why contacts, not call logs, are accessed. Based on this example and that the other fitness apps do not require this permission, the call-log permission in Runkeeper seems excessive.

In Google Play, the news app VG explains that it needs to access users' precise location 'to show you the weather where you are'[37]. Weather cannot be considered a key functionality service in the VG app as the forecast is not available on the front page of the service but is hidden in in a sidebar menu. It also seems that clicking on the weather icon in the sub-menu leads the user to the VG's weather app 'Pent', which does not require access to precise location. Therefore, we question the VG app's need for access to the user's precise location. In in the iOS App Store, VG explains that it needs users' location 'to give you accurate weather forecast and relevant offers'[38]. In the iOS version, the default setting is to share location 'always', not only when the app is in use. We have not seen that location provides functionality when the app is not in use. Therefore, we find the permission to access user location in the VG app to be disproportional and questionable.

35 'Privacy in mobile apps', Pultier, Harrand & Brandtzæg, SINTEF, 2016

36 'What Android permissions does Runkeeper require and why?', Runkeeper, available here: **https://runkeeper.com/googlePlay**

37 Our translation from the original Norwegian: 'For å kunne vise deg været der du er'.

38 Our translation from the original Norwegian: 'For å gi deg nøyaktig værmelding og relevante tilbud'.

Access to users' location is necessary for the core functionality of Endomondo, but similarly to VG, Endomondo asks for access to location also when the app is not in use. We have not seen that Endomondo provides a significantly different service than Runkeeper and Strava. Therefore, requiring location data when the app is not in use among permissions Endomondo require that we find excessive. In contrast, tracking location when the app is not in active use serves the core functionality of Happn and so is not problematic in that context.

VG, however, does claim in its terms that the data are not associated with specific users, that location data are encrypted and that location data are not sold to third parties. Despite these terms, the company emphasises in a news article the practicality of the location data apps access for targeted advertising purposes:

> *Modern browsers have a geo-location API for determining the current location of a user. Users, however, have to accept location sharing every time the browser wishes to look up the users location. An app, on the other hand, only needs to ask for the permission once.*[39]

Padraic Woods, VG

As well, MyFitnessPal explains the need for most permissions. The service, though, explains that coarse location is required due to targeted advertising:

> *Coarse location data will allow us to improve the relevance of the advertisements presented to you in the app, by allowing us to target the advertising based on the location of your device. No personally identifying information is collected as part of this process.*[40]

MyFitnessPal

As far as we can understand, however, also the users' telephone ID, which is personal data can be used for advertising purposes.

Social media apps generally require many permissions. For Facebook Messenger, we do not understand the need to access the call log. Twitter and Facebook require access to read SMS and explain that this enable verification functionality. Reading SMS is quite an intrusive permission, but this permission also makes verification easier for the users. We find the intrusiveness of this permission to be disproportionate to the service it gives in return.

All apps should provide explanations for all the permissions they require and should require only permissions necessary for performing their service.

39 'VG partners with 3 advertisers to test location-based app', INMA, 2015, available here: http://www.inma.org/blogs/mobile-tablets/post.cfm/vg-partners-with-3-advertisers-to-test-location-based-app

40 'Why are the various permissions required by the android app?', MyFitnessPal, available here: https://myfitnesspal.desk.com/customer/portal/articles/490703-why-are-the-various-permissions-required-by-the-android-app-

We find that many apps request permissions whose purpose we cannot understand, even after investigation. Strava, Instagram, Snapchat, Happn, Tinder, Linkedin, Finn.no, GuleSider and Yr do not require permissions to access personal data that we find to be questionable. Only Finn.no adequately explains all the permissions and does not require excessive permissions. However, it is important to add that these permissions might be OK, it is clear that the data might be used for extensive analysis which combined with other data sets collected by the service might reveal personal information about a person[41].

5.3. User-generated content, ownership and privacy

In many apps, users generate a lot of content. Some of this content can be personal data, such as user names, private messages and pictures, while other user content, such as a Tweet, can be considered public.

We have chosen to focus on the following issues regarding user-generated content:

- **Scope of the content license:** The app provider should not be given free rein to do what it wants with content owned by users.
- **Sublicensing:** This allows the app provider to share the rights to user content with third parties, so sublicenses should be permissible only in well-defined situations**.**
- **Duration of the license:** We analysed whether the license is perpetual and can be revoked by the user. This issue is discussed in section 7.2.

The exact definition of user content varies among apps, but MyFitnessPal's definition is quite typical and shows that user-generated content can include a variety of contents, from personal data to content the user intends to share publicly or in a community:

> *"User content" is any content, materials or information (e.g., any text, information, photos, images, video, and other content and material, including nutritional information contributed to the Food Database) that You upload or post to, or transmit, display, perform or distribute by means of, the Services.*

MyFitnessPal Terms of Use

41 'How Linkedin's 'people we may know' feature is so accurate', ZDnet, 2014, available here: http://www.zdnet.com/article/how-linkedins-people-we-may-know-feature-is-so-accurate/

Table 5. May user-generated content be used for other purposes than providing the service, and may content be sublicensed to unspecified parties?

Social apps	Facebook	Instagram	LinkedIn	Snapchat	Twitter	Happn	Tinder
The service will only use the user generated content to provide the service.	✗	✗	✓	✗	✗	✗	✗
The service will not sublicense user generated content to unspecified parties.	✗	✓	✗	✗	✗	✓	✗

Norwegian apps	Finn.no	GuleSider	Norli e-bok	VG	Vipps	Yr	Wordfeud free
The service will only use the user generated content to provide the service.	✗	-	-	?	?	-	✗
The service will not sublicense user generated content to unspecified parties.	✗	-	-	?	?	-	✗

Fitness apps	Endo-mondo	Runkeeper	Strava	Lifesum	My-FitnessPal
The service will only use the user generated content to provide the service.	✗	✗	✗	✓	✗
The service will not sublicense user generated content to unspecified parties.	✗	✗	✓	✗	✗

The first row in Table 5 relates to the scope of the content licence and shows that a majority of the apps (marked with a red X) use user content for purposes other than providing a service. The second row relates to sublicensing and shows that a majority of the apps require users to grant licences to user content that are sublicensable to unspecified parties.

Some apps, such as Norli e-bok, Yr and GuleSider, do not handle user-generated content as far as we can see and consequently are not addressed in this section. Vipps and VG, handle limited amounts of user-generated content, including pictures, and do not refer to the topic. Since it is difficult to conclude when the topic is not mentioned, these two are marked with a question mark.

A Norwegian reality TV participant found that the dating service Badoo used his profile picture in an ad for the service[42]. The service justified the use of the picture with terms that gave the service a 'non-exclusive, royalty free, perpetual, world-wide licence to use the content in any way they prefer' [our translation]—a provision almost identical to those of the majority of the apps in our study.

It is a common concern among consumers that they lose ownership of pictures or other content uploaded or generated when using digital services. However, none of the services in this study directly claim ownership to users' uploaded data. For example, Snapchat states:

> *Many of our Services let you create, upload, post, send, receive, and store content. When you do that, you retain whatever ownership rights in that content you had to begin with.*

Snapchat Terms of Service

Reading the provisions concerning licences, however, one might question whether that provision in fact provides meaningful protection of the user's ownership of content. Meaningful ownership would mean that the owner has control of how the content is used and who gets to use it.

We find that the extraordinarily wide licenses many of the apps (in particular, Finn.no, Tinder, Wordfeud Free and MyFitnessPal) apply to user-generated content can be considered unfair under the Unfair Contract Terms Directive. Article 3 deems a contractual term unfair if 'contrary to the requirement of good faith, it causes a significant imbalance in the parties' rights and obligations arising under the contract, to the detriment of the consumer'.

42 '«Farmen»-Daniel (24) føler seg misbrukt i dating-reklame: - Ubehagelig', Kjendis.no, 2015

One example is the Norwegian app Finn.no's user-content license, which we found to be a highly invasive:

> *FINN has a perpetual, unlimited and royalty-free right to use texts, images, designs, trademarks and any other form of data that the Customer makes available for FINN ('The Information') for any purpose related to development, operation and marketing of existing or future Services delivered by FINN […] The usage rights also includes, among other things, the right to copy, save, redistribute and make The Information available for the public. FINN further has a right to rewrite and further develop The Information, and* ***FINN has an exclusive ownership to such rewrites and developments****. FINN also has the right to give similar usage rights of The* ***Information to any third party*** *that can use The Information in relation to development, operations and marketing […] of current or future solutions, products or services delivered by FINN or FINN's affiliates.*[43]

Finn.no, Terms of Use, our translation (emphasis added)

This license effectively allows Finn.no to modify user content and claim full ownership rights to these modifications. This is an extremely broad content license as Finn.no does not limit what kind of adaptations it may make. This license effectively enables that Finn.no to claim full ownership rights to any content based on user-generated content, leaving the app user without any rights to the modified content.

Wordfeud Free's terms offer another example of a provision in which the app provider's possible use of the user-generated content is not limited at all:

> *Any data, text, graphics, photographs and their selection and arrangement, and any other materials uploaded to the Service by you or other users (hereinafter "User Content") are subject, whether in whole or in part, to unlimited commercial, non-commercial and/or promotional use by Bertheussen IT.*

Wordfeud Free Terms of Service

User-generated content in services, such as dating apps, fitness apps, calorie counters and social media, can be extremely private, and the services should not create any doubt about whether data, such as pictures and chat content, might be published or shared in unforeseeable ways. The privacy implications of some provisions related to user-generated content are highly problematic, as illustrated by the Happn and MyFitnessPal examples in section 5.3 on consent and sensitive data.

43 Finn has announced that this term will be changed.

Another aspect to take into consideration regarding user content, specifically profile pictures, is that individuals have the right to control use of their image according to the European Court of Human Rights:

> *Whilst in most cases the right to control such use involves the possibility for an individual to refuse publication of his or her image, it also covers the individual's right to object to the recording, conservation and reproduction of the image by another person. (Case of Reklos and Davourlis v. Greece, Application No. 1234/05, ECHR)*

European Court of Human Rights

LinkedIn provides an example of terms that limit possible use of user-generated content is. The company specifies what it will not do and when it will ask for separate consent:

> *We will not include your content in advertisements for the products and services of others (including sponsored content) to others without your separate consent.*

Linkedin User Agreement

Endomondo explains and, to a certain extent, does impose some limitations on what kind of user-generated content it will share, and specifies that sensitive data, such as weight, will not be shared by default:

> *You agree and acknowledge, that we may disclose to and make publicly available on the Site or via the Services your User Generated Content, including the personal information related thereto. However,* ***personal information such as your weight, e-mail, password to the Site, phone number and any payment information will per default not be disclosed or made publicly available by Endomondo.***

Endomondo Privacy Policy (emphasis added)

In many of the apps (see Table 5), the user grants the app provider a sublicensable licence to user-generated content. That the license is sublicensable means that these rights can be transferred to other companies. These sublicensees are typically not listed. Sublicensable licenses open up the possibility of very broad content usage by service providers and should not be included in an online service unless the rights are very well defined and limited.

In MyFitnessPal, sublicensees, among a list of 11 types of actors who are not named but include employees, may also sublicense the content.

> *You hereby grant MyFitnessPal and its officers, directors, employees, agents, affiliates, representatives, service providers, partners, sublicensees, successors, and assigns (collectively, the "MyFitnessPal Parties") a* ***perpetual, fully paid-up, worldwide, sublicensable, irrevocable, assignable license****.*

MyFitnessPal Terms of Use (emphasis added)

The user is not informed who the partners, affiliates, service providers, sublicensees or possible successors who might get sublicenses to the content in the future are. The provisions for sublicensing user-generated content in a number of the apps indicate that users have no control over who might get a licence to their content. Even if the user intended for the content to be public, this can be problematic.

Facebook and Instagram are among the services that generate the most user-generated content, such as pictures. Facebook can sublicense and use user content for purposes beyond providing the app, while Instagram does not open up content to sublicensing. According to KU Leuven researchers, Facebook can use its provisions on sublicensing to 'authorise any third party to use protected content of an individual user and receive payment for it'.[44]

It is difficult for consumers to understand the possible consequences of having so much personal content that is sublicensable and can be used for other purposes than delivering the service itself. Both these services do provide an explanation of how the content may be used and limit this possible use to a larger extent than, for example, Finn.no and Wordfeud Free.

For most of the services analysed, the service provider's right to user content is not sufficiently restricted by sublicensing and purpose limitations. Only Strava, Instagram and Happn do not require sublicensable licenses to user content, and only Lifesum and LinkedIn clearly limit the use of the user-generated content to making the service function.

5.4. Third-party personal-data sharing

Personal data should not be shared with third parties without explicit permission from the user, but many of the apps we analysed share personal data with other companies for various purposes. It is a recurring problem that privacy policies only state that some sharing takes place and do not specify what data are shared and with whom.

44 'From social media service to advertising network', KU Leuven, 2015

Table 6. Does the app provider specify with what third parties personal data is shared, and may third parties use personal data for purposes other than providing the service?

Social apps	Facebook	Instagram	LinkedIn	Snapchat	Twitter	Happn	Tinder
The app provider specify which third parties personal is shared data with.	✗	✗	✗	✗	✗	-	✗
The third parties cannot use personal data for purposes independently from the app provider.	✗	✗	✓	✗	✗	-	✗

Norwegian apps	Finn.no	GuleSider	Norli e-bok	VG	Vipps	Yr	Wordfeud*
The app provider specify which third parties personal is shared data with.	✗	✗	✗	✗	✗	✗	✗
The third parties cannot use personal data for purposes independently from the app provider.	✓	✓	✓	✓	✓	?	✗

Fitness apps	Endo-mondo	Runkeeper	Strava	Lifesum	My-FitnessPal
The app provider specify which third parties personal is shared data with.	✗	✗	✗	✗	✗
The third parties cannot use personal data for purposes independently from the app provider.	✗	?	✓	✗	✗

Table 6 shows that none of the app services specify with which third parties they share personal data (red X) and that many of the services allow third parties to use personal data for purposes other than the functionality of the app (red x). Some apps specify that data are used only for the functionality in the app (green check mark).

Table 6 concerns the sharing of personal data, usually described in privacy policies, and does not consider the privacy effects of broad licenses to user content that allow sublicensing and sharing of user content (see section 6.3). We have considered identifiers, such as IP addresses and device identifiers, combined with other user information, such as location data, to be personal data (see section 4).

Happn is the only app that states that it does not share any personal information (described as 'your details') in its confidence charter:

> *happn commits never to share your details with any other member or with any third party. Your e-mail address and your real identity are strictly confidential and will never be disclosed by happn.*

Happn Confidence Charter

However, this guarantee is not elaborated upon in the privacy section of the terms and conditions. Also, note that there may be discrepancies between privacy policies (or 'confidence charters') and the actual behaviour of the app. Indeed, through technical analysis of the app, we have seen that user data in Happn *is* sent to a third-party server (see section 9).

Sharing of data with third parties is not necessarily problematic. Several apps use other companies to handle services, such as credit card transactions and mailing lists. These are cases in which sharing personal data is necessary as the third party uses the information only to perform a limited service on behalf of the app provider. The third party should not use the data for purposes independently from the app provider. A good example of this practice is Runkeeper's privacy policy, which limits what third party service providers may do with personal data:

> *We sometimes hire other companies to perform certain business-related functions. Examples include mailing information, maintaining databases and processing payments. When we employ another company to perform a function of this nature, we may need to provide them with access to certain Personal Data. However, we only provide them with the information that they need to perform their specific function, and these third party service providers will only use your Personal Data to perform the services requested by us.*

Runkeeper Privacy Policy

However, Runkeeper is ambiguous when it comes to the sharing of location data and is marked with a question mark in Table 6 because it was difficult to conclude:

> *The Services include various location-based features, such as mapping outdoor fitness activities. To provide these location-based features, FitnessKeeper and our partners and licensees may collect, use and share precise location data, including the real-time geographic location of your mobile device. For some third-party partners, such as Google, this information will be shared automatically. For others, such as HealthGraph API and Facebook, this information will only be shared with your explicit permission or if you choose to share it.*

Runkeeper Privacy Policy

It is not clear whether only single location points, which can be anonymous, or whether location history combined with identifiers (such device identifiers), which we consider personal data, are shared with third parties. Runkeeper, since we could not conclude, is marked in a yellow question mark in Table 6.

Terms do not always include a clear limitation on what third parties may do with data. For example, Snapchat has open wording which does not explicitly say what third parties, specifically 'business partners', do with personal data. This use might be problematic, but it is impossible to know:

> *We may share your information [with] service providers, sellers, and partners. We may share information about you with service providers who perform services on our behalf, sellers that provide goods through our services, and business partners that provide services and functionality.*

Snapchat Privacy Policy

In some cases, personal data may be shared with third parties for marketing purposes, but in many cases, we had difficulty understanding how the data may be shared. Very few app providers specify with which third parties they share personal data, and those who do give only examples, not an exhaustive list. VG lists 10 actors but cautions that these are examples and not a complete list.

For example, Lifesum may share personal data with unnamed affiliates, agents and business partners for marketing purposes:

> *We may use your personal data for the purposes of providing, improving and to further develop the Services, analyzing usage of the Services, providing customer support, marketing by Lifesum or our selected business partners that help us to provide these services. […] Lifesum will not share your personal data with third parties without your permission, except in the limited circumstances provided below. Personal data collected from you may be shared with our affiliates, agents and business partners. We may disclose your personal data in order to comply with a legal or regulatory obligation, if we reasonably believe that this is required by law, regulation or other legislation, or in order to protect and defend Lifesum, our business partners or users' rights and interests.*

Lifesum Privacy Policy

The way third parties are listed provides a challenge for the consumer seeking to understand what happens to personal data. What is a (business) partner? What is an affiliate or agent? What is a third party? And what is the difference among them? And how can the consumer contact them to access or delete data about them? We could not determine who Lifesum's affiliates are, and a consumer cannot be expected to understand who these actors are and whether their access to and use of personal data are legitimate.

Another phenomenon we find arising in both social media and health and fitness apps is reference in Privacy Policies to families of businesses, which can be businesses owned by the same company. Tinder, for example, is a part of The Match Group family of businesses, which includes such services as OurTime.com, BlackPeopleMeet.com, OkCupid, Twoo, Match and HowAboutWe. There seem to be no limitations on what data these services 'may' share with each other, and it is not explained to the user how the data will be used or how this sharing improves the service for the user:

> *We may obtain both personal and non-personal information about you from other Match businesses, business partners and other third parties. […]* ***We may share information we collect, including your profile and personal information such as your name and contact information, photos, interests, activities and transactions on our Service with other Match Group companies****.*

Tinder Privacy Policy (emphasis added)

In one way, this statement at least clarifies which companies may receive personal data as the list of family members is easily available. Other apps such as Snapchat 'may share information with entities within the Snapchat family of companies'. This is quite a wide, unclear definition of what these companies may access, and the names of the companies are not easily available.

LinkedIn and Facebook also share personal data within their families. LinkedIn Pulse and SlideShare are specifically named in LinkedIn's privacy policy, while Facebook's data policy links to a separate page which lists the Facebook companies, including the marketing analytics and tracking company Atlas.[45] Twitter has a similar practice and shares data with its advertising and analytics subsidiaries MoPub, TapCommerce and TellApart.[46]

In the health and fitness category, Endomondo and MyFitnessPal are owned by the same company, Under Armour. We, however, cannot see that any terms, conditions or privacy policies, other than those for third parties, open up for other provisions for sharing personal data with these companies.

MyFitnessPal does state that traffic data (including IP addresses) and mobile device data (including unique device identifiers) may be shared with a broad range of other services:

> *MyFitnessPal may share Traffic Data and Mobile Device Data […] with: […] (2) advertisers and marketing partners so that such third-parties may provide You with advertisements tailored to Your interests; and (3) service providers so that we can personalize, provide and improve our Services to Your use and interests.*

MyFitnessPal Terms of Use

Runkeeper names three of the partners or licensees which may access location data and explains that some may access data only with users' explicit permission. However, the phrase 'partners such as Google' is not a strict limitation of which parties may access data. In addition, the partners and licensees may share users' precise location data and real-time geographic location—and with whom is not clear:

> *[…] FitnessKeeper and our partners and licensees may collect, use and share precise location data, including the real-time geographic location of your mobile device. For some third-party partners, such as Google, this information will be shared automatically. For others, such as HealthGraph API and Facebook, this information will only be shared with your explicit permission or if you choose to share it.*

Runkeeper Privacy Policy

In sum, we found major differences in the apps' privacy policies. Of all the services analysed, only Strava, LinkedIn, Finn.no, GuleSider, Norli, Yr and Vipps do not indicate that third parties may use personal data for purposes other than directly aiding the app provider. Runkeeper states the same but has an unclear term governing sharing location data.

45 '**The Facebook Companies**', Facebook
46 '**Twitter, Our Services, and Corporate Affiliates**', Twitter

All other apps have unclear privacy policies that open up possibilities for third parties to use personal data for unrelated purposes.

In general, app providers should not share personal data for purposes other than giving the user better service. Such data should have an adequate purpose limitation which restricts what third parties may do with the data. We found that, although most services share data about their users, their privacy policies are unclear about specifically what kinds of data are shared, who gets access and how third parties process such data.

5.5. Sharing of anonymous data

Another issue of which to be aware when looking at how services can share personal data is the extent to which data are hashed, anonymised, de-identified or aggregated and how the services handle the possibility that, in many cases, data can be re-identified.

> In 2008, researchers re-identified Netflix users using an anonymised dataset. In a more recent study, scientists analysed anonymised credit card metadata and found that 'the uniqueness of people's behaviour made it easy to single them out. In fact, knowing just four random pieces of information was enough to re-identify 90 percent of the shoppers as unique individuals and to uncover their records, researchers calculated'.[47]

If personal data have been adequately anonymised, it ceases to be handled as personal data. Some services specify that they share personal data only in the aggregate, anonymously or in de-identified form with third parties.

An example showing that aggregated location data from workouts can identify a user is Strava's public heat map that shows users' movements. According to Strava's FAQ, the data are anonymised: 'The data provided through Metro has been anonymized and aggregated to a linear map so that cycling activity cannot be associated with a specific member of Strava's community'[48]. Even if users are not identified by name on the map, it is possible to identify where single Strava users have started or stopped in some cases, for example, in residential areas with few Strava users[49].

47 'With a few bits of data researchers identify anonymous people' New York Times, January 29, 2015.

48 FAQ, Strava

49 Heatmap, Strava

Facebook states that it receives hashes of emails from ad companies,[50] which Twitter also does[51]. Tinder states that it shares email hashes with ad companies:

> *We also may share aggregated, non-personal information, or personal information in hashed, non-human readable form, with third parties, including advisors, advertisers and investors.*

Tinder Privacy Policy

A 'hashed' email address uniquely identifies an email address without the address itself being shared, but if both parties have the same hashes, they can identify the email address from which it is derived. This is by no means anonymous information. It is not clear if Facebook and Twitter share hashes (or only receive them), but from Facebook's, Twitter's and Tinder's descriptions, hashes seem to be treated as non-identifying information, even though they can be used to single out users (see section 6.5).

MyFitnessPal may share with third parties anonymous or aggregate FitnessData[52], including users' fitness activity, which contains sensitive information, such as weight loss and gain. Users' fitness and demographic data may be shared with other users of the service but only in anonymous and aggregate form:

> *MyFitnessPal may release or share Fitness Data with third parties in anonymous form and/or in the aggregate, for statistical analysis, research, demographic profiling and other similar purposes. In addition, MyFitnessPal may share your Fitness Data along with some of Your Demographic Data, in anonymous form and in the aggregate, with other MyFitnessPal users so that You and other users can compare their own personal fitness, health and wellness situation relative to the entire MyFitnessPal community.*

MyFitnessPal Privacy Policy

Given that only four behavioural points are necessary to identify a credit cardholder and that only two precise time or locations points can identify a person in many cases, we do not know whether aggregating this sensitive data is sufficient to protect user privacy.

50 'Relevant ads that protect your privacy', Facebook

51 Twitter Privacy Policy: 'Third-party ad partners may share […] cryptographic hash [with us]'.

52 '"Fitness Data"' (information about Your use of the Services (but doesn't specifically identify You), such as Your caloric intake, nutritional statistics, fitness activity, and weight loss/gain)' (MyFitnessPal Privacy Policy).

The problematic aspects of re-identification are well demonstrated by Snapchat. Its provision illustrates that companies often cannot guarantee that the de-identified or aggregated information they share with third parties cannot be used to identify users:

> *We may also share with third parties, such as advertisers, aggregated or de-identified information that cannot reasonably be used to identify you.*

Snapchat Privacy Policy

'Reasonably' indicates that the app provider cannot guarantee that personal data shared with third parties, even in aggregated or re-identified form, cannot be re-identified or linked to users.

The exact nature of anonymization, aggregation and de-identification is not clear in any of the terms. However, as shown in section 6.4 on sharing personal data with third parties, some services share information, including such identifiers as IP addresses and mobile identifiers. It seems that data with direct identifiers, such as names and email addresses, are rarely shared, but data with pseudonymous identifiers, such as randomly generated or mobile IDs (e.g. an IMEI number), and a cryptographic hash of data, such as emails, are shared. In fact, Twitter mentions in its privacy policy that it receives such data from the advertisers (it does not mention whether it shares such data):

> *Third-party ad partners may share information with us, like a browser cookie ID, website URL visited, mobile device ID, or cryptographic hash of a common account identifier (such as an email address), to help us measure and tailor ads.*

Twitter Privacy Policy

In general, data with any form of identifiers, such as random ID numbers and hashes of identifying information, are pseudonymous data. According to the Article 29 Data Protection Working Party, 'pseudonymisation when used alone will not result in an anonymous dataset', and it is a common misconception that a pseudonymous dataset is anonymous.[53]

The apps we have analysed have vague statements regarding data sharing, so it is difficult to assess whether data shared with third parties are adequately anonymised.

In some cases, anonymization can give the user a false sense of security if re-identification proves to be possible. The possibility for re-identification underlines that, to protect users' privacy, service providers should collect only the data needed to perform their service and should share with third parties only what is needed to improve the service for users.

53 'Opinion 05/2014 on Anonymisation Techniques', Article 29 Data Protection Working Party, 2014

6. Time limitations

We analysed how the apps limit storage of personal data and licensing to user-generated content in time. In addition, we analysed whether it is easy for users to delete user accounts and whether, according to terms and privacy policies, data are deleted when the user actively deletes a user account or requests deletion of data.

Table 7. Is the storage and processing of personal data and user generated content limited in time?

Social apps	Facebook	Instagram	LinkedIn	Snapchat	Twitter	Happn	Tinder
Data storage is limited in time.	✗	✗	✗	✗	✗	✗	✗
User can revoke license to user generated content.	✓	✓	✓	✗	✓	✓	✗
User can delete own account in the app	✓	✗	✗	✗	✗	?	✓
Clear about that data is deleted upon request or when account is deleted	✓	✗	✓	✗	✓	✓	✗

Norwegian apps	Finn.no	GuleSider	Norli e-bok	VG	Vipps	Yr	Wordfeud free
Data storage is limited in time.	✓	✗	✗	✓	✓	✗	✓
User can revoke license to user generated content.	✗	-	-	?	?	-	✗
User can delete own account in the app	✓	-	✗	-	✗	-	✗
Clear about that data is deleted upon request or when account is deleted	✓	✗	✓	✓	✓	✗	✗

More tables on the next page

Table 7. Continues

Fitness apps	 Endo-mondo	 Runkeeper	 Strava	 Lifesum	 My-FitnessPal
Data storage is limited in time.	✗	✗	✗	✗	✗
User can revoke license to user generated content.	✗	✗	✗	✓	✗
User can delete own account in the app	✓	✓	✓	✓	✗
Clear about that data is deleted upon request or when account is deleted	✓	✗	✓	✓	✗

In Table 7, apps that do not stipulate that data will be deleted if the user does not actively initiate deletion (first row), apps that claim irrevocable or perpetual licenses to user content (second row), apps where we could not find a way to dele the user account within the app (third row) and apps that are not clear about that data will be deleted upon request or account deletion (forth row) are marked with a red X.

In the second row, VG and Vipps do not mention licences to user content and are marked in yellow, while Snapchat and Runkeeper are marked with asterisks as they have perpetual licences (see more in section 7.2). GuleSider, Yr and Norli e-bok do not, to our knowledge, generate user-generated content and is not included in the second row. VG and YR do not require user accounts and are not included in the third row.

6.1. Indefinite storage of personal data

To comply with European privacy regulations[54], service providers should delete personal data when storage is no longer necessary to provide the service to the user. Therefore, we analysed whether terms or privacy policies define when the service provider will delete personal data if the user does not explicitly initiate deletion of data by terminating the user account or requesting deletion of data. This section is based on the first row of Table 7.

54 Directive 95/46/EC - Data Protection Directive, article 1

Many users simply stop using a service or uninstall the app when they do not use it any more. Those actions do not delete the user's account and, with it, personal data, such as workout details. Many users will never actually delete their user account, possibly believing that deleting the app deletes their data. Even if service providers do not share the data with third parties or abuse the data, service providers might be vulnerable to data breaches. This possibility underscores the importance that companies delete user data when the data are no longer needed, not only when a user actively requests deletion of data or terminates a user account.

Many apps do inform users in various ways that uninstalling the app does not delete the data, but we find that this measure is not sufficient. The app services should limit the timespan of storage and processing of personal data, not transfer responsibility for initiating data deletion to the user.

Although all the apps process personal data and should limit doing so in time, very few actually refer to these practices in their terms and privacy policies. None of the apps analysed specify an actual time span for how long data are saved. The best-case examples are VG, Vipps, Finn.no and Wordfeud Free, which state that data will be saved for the 'period necessary for purposes specified in this Privacy Policy' (Wordfeud Free Privacy Policy) or similar general unspecific terms. We do not find this statement to be sufficiently precise, but compared to the other apps, it is a best-case example.

Some apps state very clearly that they will keep data until users delete their account. For instance, Facebook states that 'information associated with your account will be kept until your account is deleted' (Facebook Data Policy). This means that, by default, all the data users generate in Facebook are saved indefinitely. In social media services, such as Facebook, the user receives the useful functionality of data stored over time. Indefinite storage of personal data, however, is not acceptable from the perspective of privacy.

Other apps, such as Happn and Lifesum, do not mention whether data storage is limited in time but will delete data upon request or termination of user accounts (see section 7.4 on whether data are deleted upon request).

Snapchat has vague provisions regarding deleting data, even though it claims in its blog[55] that snaps and messages are deleted immediately:

> *…in many cases the messages sent through our services are automatically deleted from our servers once we detect that they have been viewed or have expired*
> *…We can't guarantee that messages and corresponding metadata will be deleted within a specific timeframe.*

Snapchat Privacy Policy

55 http://blog.snapchat.com/

That most of the apps retain data indefinitely unless the user does something actively violates privacy regulations. None of the services, according to their terms, contact former users and offer to delete their accounts if they have not used the service for a number of months or years. However, it would also be problematic if services deleted important social or fitness data without notice to users. Most of these services have access to users' contact details, so notifying them in advance is an available option. Introducing a retention period of, for example, two years before data are deleted if the app has not been used would help app users limit data storage in services they no longer use.

6.2. Indefinite licence to user-generated content

While privacy policies in general fail to limit data storage and processing in time, we found that overreaching content licenses introduce an equally serious problems with regards to the (un)limited use of personal information. In particular, the use of all-encompassing perpetual and irrevocable licenses is highly problematic. We analysed how terms limit service providers' licences to user-generated content in time. This section is based on Table 7, second row.

Snapchat's terms are unnecessarily broad, especially when seen in light of the seemingly temporary nature of snaps and messages in the service:

> *But you grant Snapchat a* ***worldwide, perpetual,*** *royalty-free,* ***sublicensable, and transferable license*** *to host, store, use, display, reproduce, modify, adapt, edit, publish, create derivative works from, publicly perform, broadcast, distribute, syndicate, promote, exhibit, and publicly display that content [see quote above on ownership] in any form and* ***in any and all media or distribution*** *methods (now known or later developed).*

Snapchat Terms of Service (emphasis added)

In sum, this paragraph implies that the pictures and messages sent through the service may be used in ways users cannot foresee and that users' pictures may be distributed in all media and even through distribution methods that have not yet been developed. When confronted with this possibility, Snapchat replied that snaps and chats 'are automatically deleted from our servers once we detect that they have been viewed or have expired'[56]. It states that the paragraph quoted only relates to content shared publicly, such as Live Stories, and that the company has never stockpiled private pictures. That the company includes another provision in the privacy policy that contradicts this one in its terms is not a valid argument.

It is highly problematic that a service requires a perpetual licence to user content, even if the user stops using the service, as is the case with Snapchat.

56 http://blog.snapchat.com/

It is, however, potentially even more problematic that several apps, including the dating apps Tinder and MyFitnessPal, claim an irrevocable licence to user content:

> *By posting Content as part of the Service, you automatically grant to the Company, its* ***affiliates, licensees and successors, an irrevocable, perpetual,*** *non-exclusive,* ***transferable, sub-licensable,*** *fully paid-up, worldwide right and license to (i) use, copy, store, perform, display, reproduce, record, play, adapt, modify and distribute the Content, (ii) prepare derivative works of the Content or incorporate the Content into other works, and (iii) grant and authorize sublicenses of the foregoing in* ***any media now known or hereafter created.***

Tinder Terms of Use (emphasis added)

'Content' in Tinder includes 'text messages, chat, videos (including streaming videos), photographs, or profile text, whether publicly posted or privately transmitted' (Tinder Terms of Use). Users of this dating app likely would be shocked if these provisions were actually used and if Tinder's successors or affiliates irrevocably displayed pictures that can identify the user worldwide (see more in section 5.3).

Snapchat and Runkeeper claim 'perpetual', not 'irrevocable', licences. However, Snapchat's and Runkeeper's agreements do not offer a mechanism to revoke a license and specify that, in the event of termination, the content license will survive termination of accounts. Therefore, we do not see that these services' licence to user content is, in fact, revocable.

LinkedIn, in contrast, is among the exceptions that limit the licence in time and clarify how to end the licence:

> *You can end this license for specific content by deleting such content from the Services, or generally by closing your account, except (a) to the extent you shared it with others as part of the Service and they copied or stored it and (b) for the reasonable time it takes to remove from backup and other systems.*

LinkedIn User Agreement

Among the services we analysed, Lifesum, Facebook, LinkedIn, Instagram, Twitter and Happn, according to their terms, do not claim perpetual or irrevocable licences to user-generated content.

Endomondo, Runkeeper, Strava, MyFitnessPal, Snapchat, Tinder, Finn.no and Wordfeud Free claim perpetual or irrevocable licences to user-generated content, which we find to be highly problematic. That the owner of digital content does not even have the right to withdraw the right to display highly private content is simply absurd and constitutes a serious breach of privacy regulations and consumer rights. Endomondo, Runkeeper, Strava, MyFitnessPal, Snapchat and Tinder fail to limit both storage of personal data and licensing in time.

6.3. Ease of account deletion

It is easy to delete an app from mobile phones, but deleting the app does not delete personal data. In most apps, the user account must be deleted before the data are deleted (see section 7.2). We analysed whether apps have made it easy for users to terminate user accounts based on whether users can terminate their accounts in the app. This section is based on Table 7, third row.

If one can create a user account in the app, deleting the account in the app should also be possible. Unfortunately, many apps require the user to move to another platform to delete the account, for example, by contacting user support by email or going to a webpage. We consider this step to make termination of an account unnecessarily difficult for the user. Many of these services have web-based equivalents, and the app is one of the front ends. Our view, however, is that it should not be harder to delete than establish a user account, so if it is possible to register in the app, it should be possible to delete the account in the app.

Among the apps that allow deleting accounts inside the app, many, such as Facebook and Facebook Messenger, have hidden this functionality deep in the app, and finding it can take some time.

In Happn, users can 'de-activate', but not delete the account inside the app. If the account is not used for three months upon de-activation, the account and data will be deleted. It can be problematic that users of the dating app must wait for three months before the account is actually deleted, if the account is visible to other users in the mean-time.

Many users will not delete their user accounts in digital services even if they stop using a specific app as they do not want to lose content, such as pictures and workout data. Therefore, it is important to make it easy for users to bring data with them, both to safeguard data and to enable more easily changing services, for example, from one fitness app to another.

For example, Strava makes it very clear how to export data, workout by workout or in bulk[57]. In fact, three of the services we analysed (Strava, MyFitnessPal and Endomondo) have developed a method to sync workout data, so the user can switch between apps for different purposes while accessing a full picture of their data[58]. We have not analysed the privacy implications of this functionality.

This kind of interoperability can make it easier to leave one service for another, increasing user choice. That the three services do not alert users about changes in terms in advance (see section 3), however, reduces this effect. The user cannot leave the service and bring the data before the change is implemented if advance notice is not given.

57 'Exporting your data and Bulk Export', Strava

58 'Garmin announces automatic sync with Strava, MapMyFitness and Endomondo', DC Rainmaker

6.4. Data deletion upon request or account deletion

Even if the user has previously given consent by accepting the terms, consent can be withdrawn. When a user deletes a user account, the app provider generally no longer has a legitimate purpose to store personal information. In this case, data should be deleted[59]. Therefore, we analysed whether the terms stipulate whether personal data will be deleted upon request or when users delete or deactivate their accounts. This section is based on Table 7, forth row.

It should always be possible for consumers to terminate their relationship with a service provider. Deleting all data when terminating an account is an effective way for consumers to control and limit where their information is stored.

Endomondo provides a best-case example of clarity about deleting data upon deletion of accounts:

> *Once you have deleted your account, all of the data associated with that account will be permanently deleted and removed from our database. Please note that the data cannot be retrieved.*[60]

Endomondo support

In contrast, MyFitnessPal, for example, is not clear about whether all personal data are deleted when a user account is terminated:

> *If You would like MyFitnessPal to delete Your Personal Information from its system, please contact us at* **removal@MyFitnessPal.com** *with a request that we delete Your Personal Information from its database. MyFitnessPal will use commercially reasonable efforts to honor Your request; however, MyFitnessPal may retain an archived copy of Your records as required by law or for other legitimate business purposes.*

MyFitnessPal Privacy Policy

Many services state that they will maintain some records as required by law. Although this claim might seem like a blanket excuse, it is difficult to contest. However, keeping data for unspecified business purposes is not acceptable, especially when not limited in time, as in the example of MyFitnessPal.

Some apps provide seemingly contradictory information about what happens when a user account is terminated. One example is Instagram, which has the following and, as far as we can see, conflicting information in its Privacy Policy and online FAQ:

59 Directive 95/46/EC - Data Protection Directive, article 1
60 **Support, manage account**, Endomondo

Following termination or deactivation of your account, Instagram, its Affiliates, or its Service Providers may retain information (including your profile information) and User Content for a commercially reasonable time for backup, archival, and/or audit purposes (Instagram Privacy Policy) When you delete your account, your profile, photos, videos, comments, likes and followers will be permanently removed […]

Instagram Online FAQ

It is not clear to us how long 'commercially reasonable' is, and based on this, it is also unclear whether the service will delete data when requested or when a user deletes a user account. We assume that Instagram and other services have internal guidelines regarding data deletion timeframes, and we see no reason that these timelines should not be public to give consumers more predictability.

Facebook's FAQ and Privacy Policy thoroughly explain that some data are deleted, while others are more permanent in nature and will not be deleted. The explanations seem reasonable:

Information associated with your account will be kept until your account is deleted […] When you delete your account, we delete things you have posted, such as your photos and status updates. […] Keep in mind that information that others have shared about you is not part of your account and will not be deleted when you delete your account.

Facebook Privacy Policy

As shown, some apps also claim the perpetual or irrevocable right to use user-generated content. This claim also seems to be at odds with terms that let users fully delete their own data. For example, Endomondo will delete personal data, quite clearly according to one term, but, in another states that it will keep licence rights to user-generated content irrevocably. Much user-generated content is personal data, so this stance seems contradictory.

It was difficult to conclude whether Runkeeper, GuleSider, Yr and Wordfeud actually delete data. Therefore, they were deemed to be unclear on the issue. For example, Runkeeper focus on whether users can access data again after terminating accounts. Whether data are actually deleted, however, is not clear. GuleSider and Yr do not require user accounts but, nevertheless, should make it possible for the user to demand that user data be deleted as these apps collect personal data.

In Lifesum's terms and other information available online, it is not clear whether data are deleted. The service does clearly state that, when users delete accounts inside the app, data are deleted.

Only half of the apps claim that data will be deleted upon request or when users delete their accounts. Happn is among the few that provide information about how long it takes to delete information after a user de-activates an account: 'The Member's details will be kept for a period of 3 months before being permanently erased' (Happn Terms of Service).

It is not acceptable that services, such as MyFitnessPal, Instagram, Snapchat, Tinder, Runkeeper, GuleSider, Yr and Wordfeud Free, are not clear that user data will be deleted upon request or when the user deletes the user account. Additionally, services that will delete data upon request should specify the timeframe in which they will do so.

7. Terms versus actual data flow

The analysis in this report is limited to the information contained in documents, such as terms and privacy policies, and, for some issues, information and functionality in the app. This analysis relies on information from app providers and might not give an accurate picture of what *actually* happens to data when a consumer uses an app. Therefore, we commissioned the research institution SINTEF to perform a technical analysis of the Android version of the apps; the results are presented separately the report 'Privacy in Mobile Apps'[61]. The two reports were written concurrently, so this report does not compare all of SINTEF's findings with the terms analysis, but we find it useful to point out some clear discrepancies between what we found in the terms and what the technical analysis uncovered.

One example involves the dating app Happn, the second the fitness app Runkeeper, and the third the bank app Vipps.

> In a report written for Privacy Rights Clearing House, the terms and behaviours of 43 health and fitness apps were compared, and several discrepancies between app terms and behaviour were discovered. One conclusions from the study is that 'the only way for a user to know how great a privacy risk an app may be posing is by doing a technical evaluation– something beyond the ability of almost all users'. [62]

Happn is advertised in Apple's App Store and Google Play as '100 % safe and confidential', and its Confidence Charter states that:

> *Happn commits never to share your details with any other member or with any third party. Your e-mail address and your real identity are strictly confidential and will never be disclosed by happn.*

Happn Confidence Charter

61 'Privacy in mobile apps', Pultier, Harrand & Brandtzæg, SINTEF, 2016

62 'Technical analysis of the data practices and privacy risks of 43 popular mobile health and fitness applications', Njie, 2013

This statement is quite reassuring from a privacy concerned user point of view. However, according to SINTEF's report, this may be misleading:

> *Happn shares device identifier to a domain owned by UpSight, a major third-party tracking company, communicating very frequently about all user behaviour (e.g. liking other users, etc.) in the application. Every time users use the Happn app they are sharing information from their Facebook account, including name, age, birthday, job status, and gender, with a third-party tracker.*

SINTEF, 'Privacy in mobile apps'

We can only understand that UpSight is a third party, and clearly according to SINTEF's research, this third party receives not only 'details', but a combination of personal data. Sending personal data such as direct identifiers such as Facebook account and first name together with data such as birthday, job status and gender plus the user's activity in the app to third parties seems to be in direct conflict with that the quote from the confidence charter mentioned above. Name, Facebook account and birthday can be enough to reveal someone's identity. We do not find that this is explained in terms of use, confidence charter, FAQ or Google Play, and can therefore not see that the user has consented to it.

The only other indirect reference to third parties that we find in Happn's documents is that «*Certain data is invisible to other Members of the Application.* This data *will not be sold*» (Terms of Use, emphasis added). Possibly, this implicitly informs us that all data visible to other members of the service *can be sold*. If that is the case, it is problematic and should as a minimum be stated clearly.

Even if this extensive sharing of personal and sensitive data was explained thoroughly in the confidence charter and terms, SINTEF's findings in regard to Happn would illustrate how too much personal data is sent to a third party.

Happn is further one of the apps where one can initiate deletion of the user account in the app, the app also promises to delete data when the user deletes the user account. Based on the terms Happn seems to have among the more acceptable terms relating to time limitation on data storage (see chapter 7). SINTEF however finds that:

> *Happn stores a cookie that is not removed when uninstalling the application; consequently, a directory still remains on the user device containing some data. This implies that the users lose their ability to permanently remove the app and delete their personal information.*

SINTEF, 'Privacy in mobile apps'

It is also interesting to note that Runkeeper that does not to our knowledge provide functionality based on location when the app is not in use, according to the SINTEF report track user's location when the app is not used.

In the chapter on the 48 hours report that explains how data flow when the mobile phone is not used, SINTEF explain that:

> *We found that the GPS position is fetched and transmitted by Happn, which is one of the main application features. More surprisingly, we also detected that GPS location was sent by MyFitnessPal and Runkeeper when the applications are not in use. The users can then be geo-tracked whenever the GPS function is turned on.*

SINTEF, 'Privacy in mobile apps'

MyFitnessPal providers a step counter functionality. This can explain the GPS tracking when the app is not in use. For Runkeeper, we do not understand the need for location when the app is not in use. Runkeeper claim that, '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' (Terms of Service). Further, the online explanation of app permissions does not refer to location tracking when the app is not in use:

> *Location: We hope this one is self-explanatory, but we do in fact use your location to track your workouts. The GPS hardware exists on your phone and Runkeeper needs this permission into order to use your phone's GPS so we can be your workout buddy on the road!*[63]

Runkeeper, Understanding permissions

Tracking location when the mobile phone is not in use is not self-explanatory. In addition, the explanation of the use of location information includes a screenshot of the iOS request for permission: '*Allow Runkeeper to access your location* ***when the app is in use?***'

A third example comes from the bank application Vipps. Its terms suggest that the app does not transfer information to third parties for purposes outside the functionality of the app (see section 6.4). However, according to SINTEF, the app communicates with Facebook when starting up, although the app does not have any clear functionality related to Facebook: '*Vipps contacts Facebook with a personal identifier when starting-up (we suspect the presence of a deactivated "connect with Facebook" button)*'.[64]

SINTEF suggests that the presence of Facebook-related functionality in Vipps might be an oversight, but it is worrying from a privacy perspective that a high-security app, such as a banking application, has such oversights. Regardless, the terms do not seem to open up for sharing personal identifiers with Facebook.[65]

63 '**Understanding permissions**', Runkeeper

64 'Privacy in mobile apps', Pultier, Harrand & Brandtzæg, SINTEF, 2016

65 The service provider DNB has announced that the terms will be changed so that the communication with Facebook is covered, and that Vipps users will be given the possibility for opting out.

Overall, the terms in these examples did not provide sufficient information to the users about the data flow. This shows that even long, difficult-to-understand terms and privacy policies do not cover what actually happens to user data. This failure illustrates that the terms are not necessarily the conclusion to what actually happens to user data. This makes it practically impossible for users to give informed consent.

8. Termination of user accounts without reason or notice

The EU Directive on Unfair Terms in Consumer Contracts[66] stipulates that a term may be unfair when it enables 'the seller or supplier to terminate a contract of indeterminate duration without reasonable notice except where there are serious grounds for doing so'. In apps, account termination by the service provider without predictable reasons effectively leaves the consumer without any rights, and the user can lose access to an important network and data. Therefore, we analysed whether the apps' terms allow the termination of user accounts without reasonable reason or notice.

Table 8. Can the service block or terminate a user account without valid reason, and will a user be notified if an account is blocked or terminated?

Social apps	Facebook	Instagram	LinkedIn	Snapchat	Twitter	Happn	Tinder
The service will only terminate the user account or block the user's access with valid reason.	?	✗	?	✗	✗	✓	✗
The service will provide notice if the user is blocked or the user account is terminated.	?	✗	✓	✗	✓	✓	✗

Norwegian apps	Finn.no	GuleSider	Norli e-bok	VG	Vipps	Yr	Wordfeud free
The service will only terminate the user account or block the user's access with valid reason.	✓	-	?	-	✓	-	✗
The service will provide notice if the user is blocked or the user account is terminated.	✓	-	?	-	✓	-	✗

More tables on the next page

66 The Directive on Unfair Terms in Consumer Contracts

Table 8. Continues

Fitness apps	 Endo-mondo	 Runkeeper	 Strava	 Lifesum	 My-FitnessPal
The service will only terminate the user account or block the user's access with valid reason.					
The service will provide notice if the user is blocked or the user account is terminated.					

Table 8 shows which services, according to our analysis, comply with the obligation to provide notice and valid reasons for terminating a user account. Services that terminate user accounts for any reason or will not provide notice are marked with a red x. Services that follow reasons we consider acceptable or will provide notice are marked with a green check. LinkedIn is marked in orange as it has unclear or conflicting terms, as explained later. GuleSider, Yr and VG do not require user accounts and are not included in Table 8.

Several apps may terminate users' accounts without any reason or notice. This one-sided provision shows an imbalance between the service provider and the consumer. One example is the dating app Tinder, which specifies that it is not required to refund unused fees or even disclose the reason for terminating a user account:

> *The Company may terminate or suspend your account at any time without notice if the Company believes that you have breached this Agreement, or for any other reason, with or without cause, in its sole discretion. Upon such termination or suspension, you will not be entitled to any refund of unused fees for in app purchases.*
> *The Company is not required to disclose, and may be prohibited by law from disclosing, the reason for the termination or suspension of your account.*

Tinder Terms of Use

Another example is the fitness app Endomondo:

> *Endomondo may at any time, at its own discretion for any or no reason, and without any warning or notice, edit or remove in whole or in part any Users account and User-generated content and further to restrict Users use of all or any part of the Services.*

Endomondo Terms and Conditions of Use

Wordfeud and Strava specify that they will not give '*advance*' notice, while Lifesum states that violations of the terms will lead to a 'direct' termination of the account, implying that no notice will be given.

Runkeeper must have 'reasonable cause' to terminate an account but might or might not give notice:

> *We may terminate this Agreement, disable your account, and/or put your account on inactive status, in each case at any time with reasonable cause or violation to these terms of service agreement, and with or without notice. We shall have no liability to you or any third party because of such termination or action.*

Runkeeper Terms of Service

MyFitnessPal's terms might seem reasonable at first glance as either party may terminate the agreement at any time:

> *Either party may terminate this Agreement and its rights hereunder at any time, for any or no reason at all, by providing to the other party notice of its intention to do so in accordance with this Agreement. This Agreement shall automatically terminate in the event that You breach any of this Agreement's representations, warranties or covenants. Such termination shall be automatic, and shall not require any action by MyFitnessPal.*

MyFitnessPal Terms of Use

This impression, however, does not take into account the asymmetrical relationship between the user and the provider of the service. Of course, the user can terminate the agreement at any time and for any reason, but there should be just cause for a company to terminate a user's account.

MyFitnessPal should provide notice to the user when terminating an account for reasons other than breach of agreement. However, notice will not be given if the company considers the user to be in breach of the agreement, so this arrangement is not considered sufficient advance notice.

Other services have unclear or contradictory terms. LinkedIn, on one hand, specifies that the agreement may be terminated if the user breaches the agreement or law or misuses the services but, on the other hand, claims elsewhere in the Terms of Services that it may terminate the agreement at any time:

> *… LinkedIn reserves the right to restrict, suspend, or terminate your account if LinkedIn believes that you may be in breach of this Agreement or law or are misusing the Services (e.g. violating any Do and Don'ts).*
>
> *… LinkedIn or You may terminate this Agreement at any time with notice to the other. On termination, you lose the right to access or use the Services.*

LinkedIn, User Agreement

Facebook vaguely describes when it may close an account: 'if you violate the letter *or spirit* of this Statement' (Facebook Terms of Service). The service will provide notice of closed accounts through e-mail or 'at the next time you attempt to access your account'. That the user realises that an account is closed when attempting to log on hardly qualifies as notice.

A Facebook account belonging to Norwegian activist Hege Storhaug was closed following a campaign by people who disagree with her[67]. Storhaug complained that she had not been given notice of the account closure. In her case, the user account was re-opened as upon consideration (and media pressure), Facebook found that her actions did not qualify among the possible reasons for terminating her user account.

Some of the studied services may close only accounts with a valid reason, such as violation of the terms of service. The Consumer Council is of the opinion that this should be standard in all app terms.

While Tinder's account termination policy is unfavourable to consumers, the other dating service, Happn, has one of the more consumer-friendly terms on account termination among the services analysed.

67 '**Hege Storhaugs Facebookprofil ble stengt**', VG, 2015

Its terms clarify under what circumstances accounts may be terminated:

> *Happn is fully entitled to terminate the contract between Happn and the Member should the Member not abide by these T&Cs, or should the Member's account be temporarily suspended owing to the Member's failure to modify the poor conduct of which the he/she is accused. In the event of non-payment of Credits acquired and following receipt of a formal notice for payment via email which has not been acted upon within 8 days […] Any act of serious misconduct, namely any distribution of content which disturbs public order or violates public decency […].'*

Happn Terms and Conditions of Use

Happn also gives the consumer the opportunity to respond to the decision and to correct mistakes that could lead to termination of accounts. Most of the terms we analysed do not mention this option, but we find that allowing it is highly positive from a consumer's perspective.

Endomondo, MyFitnessPal, Instagram and Tinder may terminate accounts without notice or valid reason, which we find unjustifiable. Only Facebook, Messenger, Happn, Finn.no and Vipps both must have what we consider fairly reasonable cause to terminate user accounts and will notify the user upon termination.

In our opinion, all digital services, including free apps, should specify what breaches justify shutting a user out from the service. The user should also be notified about any such decision and given the opportunity to contest it.

9. Applicable law

Mobile apps are, by nature, global services that pose new challenges concerning legal compliance. Consumers should benefit from a high level of consumer protection. In the previous sections, we have compared terms and conditions to European regulations. This section briefly describes the various clauses on jurisdiction referenced in this study.

Forum clauses stipulate where disputes between users and service providers should be solved. These clauses, along with clauses on applicable law, are widely used in the services' terms and conditions.

Snapchat provides an example of a typical forum clause that is not especially user friendly for European users of the service:

> *To the extent the parties are permitted under these Terms to initiate litigation in a court, both you and Snapchat agree that all claims and disputes in connection with the Terms or the use of the Services will be litigated exclusively in the United States District Court for the Central District of California. If, however, that court would lack original jurisdiction over the litigation, then all claims and disputes in connection with the Terms or the use of the Services must be litigated exclusively in the Superior Court of California, County of Los Angeles. You and Snapchat consent to the personal jurisdiction of both courts.*

Snapchat Terms of Service

Within the EU, cross-border disputes in consumer contracts are subject to the Brussels I Regulation, which establishes rules for jurisdiction if a professional practices commercial or professional activities in the consumer's domicile state or the professional directs[68] such activities towards the state. According to article 17 (2) of this regulation, the professional will be deemed to be domiciled in the consumer's domicile state if the professional has a branch, agency or other establishment in another member state.

It can be questioned whether a forum clause in a standard consumer contract complies with consumers' right to a fair trial[69] and the EU Directive on Unfair Terms in Consumer Contracts. The forum clause establishes a presumption that any arbitration clause in a consumer contract is invalid according to European case law[70]. In our context, this raises the question of whether users or consumers can take legal actions in their home legal venue.

68 CJEU joined cases C-585/08 and C-144/09 (Pammer & Heller).

69 Article 6 of the ECHR

70 CJEU joined case C-240/98 to C-244/98 (Océano).

When identifying applicable law, it is essential to take into account, among other factors, the parties involved and their localisation. Many of the services are based in the United States, and most of these claim to be governed by American law. Although MyFitnessPal and Tinder market their services towards Norwegian consumers in the Norwegian language in, for example, app stores and in the apps themselves, they nevertheless require that disputes be resolved in California or Texas. We find it peculiar that terms in Norwegian stipulate that US law applies. However, MyFitnessPal's terms, for example, clarify that, if there is a difference between the Norwegian and English versions, the English version must apply.

Some services, including the six Norwegian services, Endomondo, Lifesum, Facebook, Messenger, LinkedIn and Happn, are, as far as we can see, governed by law in different European countries. According to the terms, Facebook and LinkedIn are governed by Irish law, even though they are American companies. Runkeeper, Strava, MyFitnessPal, Instagram, Snapchat, Twitter and Tinder are governed by US law.

In this report, we have referred to relevant EU legal framework: the Data Protection Directive, Directive on Unfair Terms in Consumer Contracts, ePrivacy Directive and Directive on Unfair Terms in Consumer Contracts. European regulators, thus, can play a role in this issue.

According to article 4.1(a) of the Data Protection Directive, the national law of a member state is applicable to all processing of personal data carried out 'in the context of an establishment' of a controller in the territory of that member state. Pursuant to article 4.1(c) of the Data Protection Directive, the national law of a member state is also applicable in cases when the controller is not established on the territory but uses equipment in the territory of that member state. The device of a mobile phone is instrumental in the processing of personal data from and about the user, so this criterion is usually fulfilled. However, it is only relevant when the controller is not established in the EU.

According to the consent requirement (see chapter 5), article 5(3) of the ePrivacy Directive applies to any information, regardless of the nature of the data stored or accessed. The scope of this article is not limited to personal data but extends to information of any type of data stored on a device. The consent requirement in article 5(3) of the ePrivacy directive applies to services offered '*in the Community*', that is, to all individuals living in the European Economic Area (EEA), regardless of the location of the service provider.

The Data Protection Directive and the ePrivacy Directive are both imperative laws in that individuals' rights are non-transferable and are not subject to contractual waiver. This means that the applicability of European privacy law cannot be voided by a unilateral declaration or contractual agreement, for instance, that only the law from a jurisdiction outside the EEA applies.

10. Appendix: Reference documents: terms and policies

App	Document title and link	Date of update to version reviewed
Health and Fitness		
Endomondo	Terms and Conditions of Use	26 February 2014
Endomondo	Privacy Policy	26 February 2014
Runkeeper	Terms of Service	8 November 2012*
Runkeeper	Privacy Policy	15 November 2011
Strava Running and Cycling GPS Tracker	Terms of Service	14 January 2014
Strava Running and Cycling GPS Tracker	Privacy Policy	25 March 2009
Lifesum	Terms and Conditions	11 October 2013
Lifesum	Privacy Policy	11 October 2013
MyFitnessPal	Terms of Use	11 June 2013
MyFitnessPal	Privacy Policy	11 June 2013
Social Media		
Facebook, including Messenger	Statement of Rights and Responsibilities	30 January 2015
Facebook, including Messenger	Data Policy	30 January 2015
Instagram	Terms of Use	19 January 2013
Instagram	Privacy Policy	19 January 2013
LinkedIn	User Agreement	23 October 2014
LinkedIn	Privacy Policy	23 October 2014
Snapchat	Terms of Service	28 October 2015
Snapchat	Privacy Policy	28 October 2015
Twitter	Terms of Service	18 May 2015
Twitter	Privacy Policy	18 May 2015
Happn	Terms and Conditions of Use	-
Happn	Security and Privacy	-
Tinder	Terms of Use	31 July 2015
Tinder	Privacy Policy	31 July 2015
Norwegian apps		
Finn.no	Terms of Service (PDF available through Google Play)	31 March 2014
Finn.no	Privacy Policy	16 April 2015
GuleSider	Terms	2013
GuleSider	Privacy Policy	-
Norli e-bok	Terms of Use	-
Vipps	Terms of Service	
Yr	Not found	-
VG	Privacy Policy (no Terms of Use)	14 October 2013
Wordfeud Free	Terms of Service	-
Wordfeud Free	Privacy Policy	-