Consumer protection in fitness wearables

November, 2016

FORBRUKERRÅDET

Content

Coverphoto: Colourbox.com

1. Introduction

Fitness trackers – Healthy living through wristbands

In a rapidly changing landscape of digital services and devices, it can often be challenging to attain a comprehensive overview of the various available providers and products. One of the largest segments of the market of devices known as the Internet of Things (IoT) consists of fitness wearables, which are devices that are strapped directly onto the body, and outfitted with a multitude of sensors that can monitor fitness- and health related data, such as daily steps, heart rate, and sleep cycles. This information is synchronized to a smartphone application via a Bluetooth connection, after which the data is usually sent to a server and structured to provide the user with visualizations of their fitness activity, ideally allowing them to gain new insights about their habits, and hopefully incentivizing a healthy lifestyle. Some of these applications also have a social component, where users can share and compare their datasets with friends and acquaintances.

The most common form of fitness wearables are connected wristbands, also called activity trackers or fitness trackers. Around 720 000 of these wristbands (including smart watches) were sold in Norway in 2015 alone, signifying the enormous and growing popularity of the products.[1]

> Fitness wearables are internet-connected devices that are worn on the body. With the help of a multitude of sensors, the devices can track things such as step count, heart rate, and sleep patterns.

1 http://www.elektronikkbransjen.no/content/download/26331/223207/version/1/file/Elektronikkbransjen%2BMobil%2Btotalomsetning%2Btabell%2B2015.xlsx

2. Methodology

What is assessed?

Due to the popularity of activity trackers, the Norwegian Consumer Council (NCC) chose to look at potential possibilities and challenges faced by consumers, by analyzing products from four of the most popular brands on the Norwegian market. The issues that were examined, include scrutinizing the products' terms and conditions, evaluating the functionality and user settings in the connected applications, and seeing to which degree consumers are in control of their fitness data when using these apps and devices.

In many ways this analysis mirrors the NCC's previous project dealing with mobile apps,[2] with the main difference being the inclusion of a physical device beyond the smartphone itself. As will be shown, this is especially significant because whereas many smartphone apps are free to download, connected devices require a purchase.

Evaluation criteria

Before evaluating the consumer-friendliness of the different services, the NCC formulated several criteria. As a base for our analysis, we set a European benchmarking standard by applying the Data Protection Directive[3] and the Directive on Unfair Contract Terms in Consumer Contracts[4]. On top of this we also use criteria from The Citizen Lab,[5] and the European Commission's recent draft code of conduct for developers of mobile health applications.[6] In some cases we have also found it necessary to show the path companies need to direct themselves into, and hence the criteria are based on the recently adopted general data protection regulation (GDPR)[7].

2 http://www.forbrukerradet.no/appfail-en/

3 Directive 95/46/EC - http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

4 Directive 93/13/EEC - http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31993L0013:en:HTML

5 https://citizenlab.org/2016/02/fitness-tracker-privacy-and-security/

6 The Code of Conduct for mobile health app developers has been submitted for approval. Once approved, app developers can choose to commit to follow the code [June 2016].https://ec.europa.eu/digital-single-market/en/news/code-conduct-privacy-mhealth-apps-has-been-finalised

7 Regulation (EU) 2016/679 - http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679

Comparing the findings from the analysis with these pre-determined criteria, the devices were evaluated using a three-point color based scale:

- Green checkmark means that the service fulfills the criteria in a satisfactory matter
- Red mark means that the service does not satisfy the criteria
- Yellow question mark signifies uncertainty about whether the criteria are actually met.[8]

The four products chosen for this analysis are the Fitbit Charge HR, Garmin VivoSmart HR, Mio Fuse, and Jawbone UP3. The testing of apps were done using Android devices, although there seems to be little difference between the Android and iOS versions. A technical test of what the devices and apps actually do "beneath the hood" was commissioned by the NCC from the consultancy firm Bouvet, and is attached to this report.[9]

The NCC has also been in touch with the companies behind the relevant devices. Each company was contacted by e-mail, and given a week to respond to our preliminary findings. Wherever changes have been made to this report as a result of these exchanges, a note has been added. Additionally, the results are based on direct observation of changes in the terms and in the apps themselves.

8 Often this uncertainty stems from a lack of clarification in the terms or the app. Wherever the NCC deemed clarity about certain practices a necessary criterion, this uncertainty was judged to be non-satisfactory (red).

9 Attachment: Investigation of privacy issues with Fitness Trackers

3. Analysis
Consent to processing of personal data

Accessibility and readability – are the terms easily available and readable?

The first aspect of the analysis entailed checking the availability and readability of the terms of service and privacy policies pertaining to each of the products that were examined. According to the Data Protection Directive, consent is needed before processing personal data[10], and we consider this the relevant legal ground of any such processing.

The terms of service and the privacy policies are the consumer's only avenue to determine their rights and restrictions, it is vital that these are readily available to a potential customer ***before*** they commit to a purchase. These terms should be easy to find on the service provider and/or manufacturer's website, and be linked to both in the app store and as a part of the registration process when creating an account in the application.

1. Accessibility:
Are the terms easily available?

	fitbit	GARMIN	MIO	JAWBONE
The terms are available online	✓	?*	?**	✓
I get the opportunity to read the terms before accepting them	✓	?*	✓	✓

** The terms apply only to the website, while the EULA is only available in the app itself after installation.*
*** The terms are only available through the app store, not on their website.*

Through the preliminary analysis it was discovered that while Fitbit, Garmin, and Jawbone have their terms of service and privacy policy readily available on their websites, Mio's terms were not so easily found. The actual terms on Mio's website pertain only to the site itself, not to their physical wristbands or the app, and in order to find the relevant documents, potential customers have to go through Google Play or the iTunes App Store. In addition, the url for Mio's terms is obscured to a degree where it would be very difficult for a consumer to look for them, as they seem to be hosted on a cloud site outside of Mio's own

10 Directive 95/46, article 7

domain.[11] Garmin link to a privacy policy and terms of use on their website, but the terms of use only applies to the website itself, while the privacy policy applies to both. They provide an end user license agreement for the app, but as far as we have seen this is only available in the app itself. Other than this, all of the services provided a clear link to these their terms and privacy policies in the app stores and upon registration in the apps, fulfilling the requirement of linking to the terms.

Readability and consent

Since the terms and conditions are consented to by consumers before using the apps, the service provider should also attempt to make these documents readable. The absurdity of length and complication of terms have been well documented, also by the NCC during the #AppFail-campaign. The average length of terms from the 20 apps analyzed during the #AppFail-campaign was 5700 words, which equals to somewhere between 12 and 15 pages. When terms and conditions are too long and complicated for anyone who may wish to read them, it is relevant to ask whether informed consent can truly be given.

It was discovered that all four fitness apps have similarly long terms and conditions. Out of the four fitness trackers analyzed, only Mio came in at below the average from #AppFail, with roughly 4900 words (approx. 11 pages). Fitbit was the wordiest of the four, clocking in at 7500 words (17 pages), plus a 2000-word (5 pages) document detailing their privacy policy under the EU-US Privacy Shield.[12] The NCC deems it unreasonable to expect consumers to read 22 pages of terms before making use of their product, which makes the implication of informed consent problematic.

> During their #AppFail-campaign, the Norwegian Consumer Council hosted a live reading of the terms and conditions of 33 popular apps. The reading took more than 32 hours, illustrating the absurdity of expecting a user to read these documents. [13]

Although very long terms are obstacles for any consumer wishing to read and comprehend them, the actual content of the documents are of even higher importance. The use of complex and vague language makes it very difficult to really understand how the service providers actually will handle their users` data, for example:

11 https://d3b2h820vtsscl.cloudfront.net/miogo/terms/en/terms_and_conditions.html [accessed 17-10-2016]

12 This was added toward the end of the writing of this report, and can be found here: https://www.fitbit.com/legal/privacyshield [accessed 17-10-2016]

13 http://www.forbrukerradet.no/side/the-consumer-council-and-friends-read-app-terms-for-32-hours/

*"**We may combine** the personal information and/or the location information that you provide via your Account with information from other Services or third parties in order to enhance your experience and/or to improve the overall quality of the Services. For certain Services, **we may give you an opportunity** to opt out of the combination of such information."*

Mio privacy policy, emphasis added

2. Readability:
Are the terms written in clear language, and with a user-friendly layout?

	fitbit	GARMIN	MIO	JAWBONE
Word count	7522 + 2000 Privacy Shield policy	6671	4915	6136
Use of word "may" or "can":				
Terms of service	25	10	49 for both	25
Privacy policy	17	48		10
Total	**42**	**58**	**49**	**35**
The service uses clear language	✓	✗	✓	✗
The service have made an effort to make the terms readable (layout, etc.)	✓	✓	✗	✗

All of the four services employ liberal use of such vague language, although Garmin and Mio were the worst offenders. Otherwise, in the use of easily understandable language (e.g. not overly legalistic or technical), Fitbit and Mio use layman's terms where possible, while Garmin and Jawbone have terms of service that are quite difficult to parse for the average consumer. Finally, in making an effort to present the terms in a user-friendly way, Fitbit came out ahead by structuring their terms of service and privacy policy in an intuitive and clear manner, even formulating their privacy policy in the form of relevant questions and answers. All of the other services are guilty of using caps lock, which is inherently difficult to read, and on this point both Mio and Jawbone seem not to have considered user-friendliness at all, with much of the text being crammed together in lengthy paragraphs.

In sum, in our opinion the services have not done enough to ensure informed consent, as users face terms that are not easy accessible and are way too lengthy. In our opinion, the services should modify their practice according to our criticism in order to comply with European Data Protection regulation, which requires informed consent[14].

14 Directive 95/46, article 7

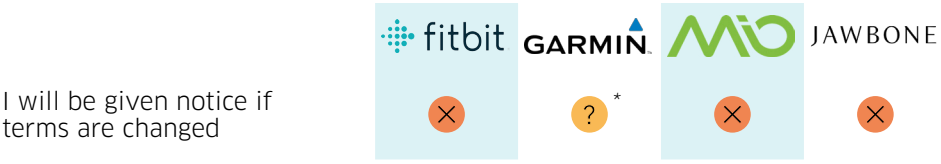
Fairness in terms

To ensure that consent will remain informed, it is essential that users are notified whenever a service changes their terms, so user notifications of modified terms should be mandatory.

Most digital services require the user to consent to the terms laid out in their Terms of Service and Privacy Policy before using the service, and this tacit approval constitutes the basic contract between the service and the user. If no notification mechanisms on changes in terms are in place, the users may suddenly find themselves having implicitly "agreed" to something that they had no knowledge of, so therefore notification is an obvious criterion in our view. Especially in the case of material changes, including functionality and user rights, the services should provide advance notice, so that anyone who does not agree to the new terms has an opportunity to export their data, leave the service, and potentially find another provider before the new terms are put into effect.

According to the Council Directive 93/13/EEC on unfair contract terms in consumer contracts, unilateral altering of terms could be regarded as unfair. When the NCC filed a complaint to the Norwegian Consumer Ombudsman in 2014 regarding Apple iCloud's lack of advance notice, we put forward that this was the case.[15] As an immediate response to the complaint, Apple changed their terms globally.

3. Advance notice:
Will the service notify me in *advance* if they change terms?



** Will notify before changes to PP, but not if they change ToS or EULA.*

4. Notice:
Will the service notify me by appropriate means?

** Promise to notify, but were observed not to do this in practice.*
*** State that "we may notify you", but it is unclear whether this actually happens.*

15 http://www.forbrukerradet.no/wp-content/uploads/2015/10/Complaint-on-Apple-iCloud-to-the-Norwegian-Consumer-Ombudsman.pdf

None of the four services the NCC analyzed write that they will notify users in advance if they are going to change their terms of service or privacy policy. Fitbit promise that in the case of material changes, the users will be notified by e-mail or inside the service itself, which gives grounds for active consent. However, on September 28th 2016, Fitbit changed their privacy policy to include a reference and link to a new privacy policy dealing with the EU-US Privacy Shield. We did not receive notification regarding this change to our test account, and the date on top of the page[16] was not amended to reflect the change. Although these changes were positive for users, it is not good practice to change these documents without giving consumers a chance to even know that something was changed. Because of this observation, we have decided to give Fitbit a red mark on this point. On notifying in advance, the Mio privacy policy is very vague, stating that

> *"**we may notify you** of any changes to this Privacy Statement via email and **may ask you** to affirmatively acknowledge consent to the changes."*

Mio privacy policy, emphasis added

This wording essentially makes no promises whatsoever. Garmin promise to notify the user about changes to the privacy policy, but does not promise this in their terms of use or end user license agreement.[17]

> *"We will provide notice to you if these changes are material and, where required by applicable law, we will obtain your consent. This notice **may be provided by email,** by **posting notice of the changes on our affected websites or by other means** prior to the change becoming effective, consistent with applicable laws."*

Garmin privacy policy, emphasis added

Although it is good that Garmin say that they will provide notice prior to the change becoming effective, this statement is undermined by vaguely stating that this notice "may be provided by email", by posting notice on the website, or other unspecified means.

Jawbone simply state that they will change the "last updated" date in the documents if they make any changes, placing the responsibility of periodically checking the terms squarely on their users. This is not an adequate solution, as it is unreasonable to expect the users to check the provider's website every time they want to use the service. Therefore, we deem this an unfair contract term, and as such in breach of the Norwegian Marketing Act, paragraph 22, and the EU directive on Unfair Terms in Consumer Contracts.

16 https://www.fitbit.com/no/legal/privacy [accessed 13-10-2016]

17 Garmin's terms of use concerns their websites, not the app. However, the Garmin Connect app includes a website service, and users should therefore be notified of changes to this document. The NCC has been in dialogue with Garmin about this, and have the impression that this will be changed.

4. Collection and processing of personal data

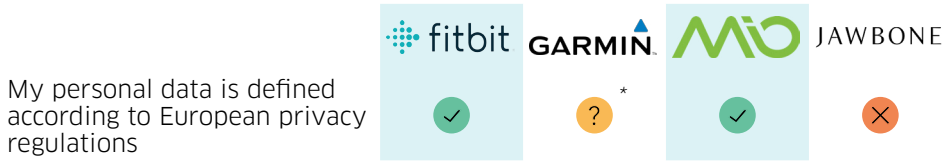
Since a main functionality of most fitness trackers is to process and visualize user data, the NCC was interested in seeing how the services process and protect their customers' data. Information such as exercise habits, location data, and heart rate can be very valuable for marketing and promotional purposes, and perhaps especially for insurance providers.[18] To avoid any current or future misuse of this data, it is important that appropriate safeguards and rights be put in place by the service providers, letting the users have at least some degree of control over what happens to their health and fitness data.

> Sensitive personal data, such as health information, is granted special protections under European data protection legislation. [19]

Definition of personal data

As the often used U.S. concept of personal identifiable information (PII) is quite vague compared to European data protection regulations,[20] the NCC wants the companies' significant European customer base to be afforded the levels of data protection that is required by European authorities. This is especially relevant when looking at fitness trackers, since fitness and heart rate data are regarded as sensitive data in a European context,[21] but not expressly so under American regulation.[22]

5. Definition of personal data:
Is data collected about me categorized according to Norwegian and European laws?



** Terms are unclear about definition of personal data.*

18 http://www.forbes.com/sites/michaelthomsen/2015/09/19/swiss-insurance-company-wants-higher-premiums-for-people-who-dont-wear-fitness-trackers/ [accessed 17-10-2016]

19 Directive 95/46/EC, article 8

20 http://www.ephmra.org/code-of-conduct/19/C-Data-Protection-and-Privacy#section-20 (3.17) [accessed 17.10.2016]

21 Directive 95/46/EC, article 8 cf. article 2 a)

22 In the United States, Personally Identifiable Information entails: "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information." Fitness data is not necessarily included under this definition. See: http://www.gao.gov/new.items/d08536.pdf (page 1) [accessed 17-10-2016]

Since three out of the four fitness trackers are based in the United States (Mio is Canadian), it was important to look at how they choose to define personal information. Perhaps unsurprisingly, the Canadian service Mio defines sensitive personal data in a satisfactory way from a European point of view:

> *"Personal information is **any information that identifies you personally**, either alone or **in combination with other information** available to us."*
>
> Mio privacy policy, emphasis added.

Since Fitbit are in the process of adopting the EU-US Privacy Shield,[23] they have pledged to treat personal data according to European standards and regulation. Garmin does not regard location data as personal data,[24] and Jawbone does not specify what they mean by personal data at all. In practice, this means that these two services can process some data regarded as personal by European standards, without regarding or treating this information as sensitive.

Data minimization – does the service provider limit their collection of user data to what is necessary to provide the functionality of the service?

Because of the consumer's right to have control of their own data, and the potential high market value of various personal information, it is important that digital services do not require more information from the user than what is necessary to provide the service. The principle of not collecting unnecessary data is called data minimization25 and is reflected in European regulation[26]. This is closely linked to the principle of *purpose limitation*, meaning that the collected data should not be used for purposes outside of the explicitly stated reasons for which it was collected in the first place.

Unlike many mobile apps and services, which are "free" in the sense that the users pay with the data they provide, fitness trackers often come with a considerable price tag. This makes it particularly important that the services do not collect information for resale, at least not without explicitly asking the user for consent.

23 https://www.privacyshield.gov/EU-US-Framework [accessed 17-10-2016]

24 Through dialogue with Garmin, the NCC has been told that this assessment of personal data concerns unrelated GPS services, not the fitness trackers. Garmin also state in their privacy policy that they will use this data in aggregate form, but their terms are somewhat unclear regarding exactly how they will treat this information.

25 https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/Dataprotection/Glossary/pid/74 [accessed 17-10-2016]

26 Directive 95/96 article 6 c)

A simple example of data minimization is found in the registration process of

6. Data minimization:
Does the service limit the amount of required personal information to what's necessary to provide the service?

many digital services. Users will normally be asked for their full name, e-mail address, and birth date. Under the principle of data minimization, it may not be necessary to ask a user for their full name where a pseudonym or nickname could be enough, and a simple birth year might suffice (if the user's age is relevant to the service at all).

All of the analyzed fitness trackers ask for the user's date of birth. It can be argued that this is necessary in order to comply with laws regarding minors' use of the services, but such issues could easily be circumvented by for example asking for a birth year, and simply requiring users born in the year in question (e.g. 2003, if the age limit is 13) to supply their exact birthday. In our opinion, it is unnecessary to ask the user for their full name.

The fitness trackers also ask for personal information such as gender, weight, and height, but these are understandably necessary for the fitness-related functions. Notably, Mio does not require a full name to register, which could be related to the app's lack of a social function (more on this later). Fitbit commendably have a prompt for *"Why are we asking this?"* explaining that this information is required to "*calculate your BMR (Base metabolic Rate). BMR is used to determine your calorie count for activities*". However, it is impossible to leave these fields empty, even if the user is not interested in tracking their calorie count in particular. In other words, these side-functions and the required information should ideally be opt-in, and not mandatory in order to use the app and wristband. Since all four services require an exact birth date, none of them sufficiently fulfills our criteria.[27]

Permissions & privacy by default – are the required permissions necessary for the app to function, and does the service respect privacy by default?

Even though the practice of granular permissions gives the user significantly more control than the "everything or nothing" approach, it is still important that

27 Mio claim that an exact birth date is required in order for their algorithms to function properly. The NCC is unconvinced that a birth year would not be sufficient, as algorithms can be changed and adapted.

the services properly explain why certain permissions are required (especially when the functionality is not obvious). We therefore require that the apps have implemented privacy by default, which is also codified in the new GDPR[28].

When downloading an app from the app store, users are informed about which permissions the app requires in order to operate on the phone. Apple phones have a granular permission function, which lets users confirm or deny specific permissions at the time they are required, instead of having to accept all permissions at the point of installation. The newest versions of Android (Marshmallow 6.0 and newer) have also incorporated this function,[29] although these versions are currently only available on a limited amount of Android devices.

A quick Google search revealed that all four of the fitness tracker providers have sites explaining these permissions, either on their FAQs or through customer support forums. Permissions that may initially seem unreasonable are explained. For example, Fitbit[30] and Garmin[31] requiring access to the phone's sms and call log, are used to send notifications to the activity tracker, meaning that the wristband will vibrate if the user receives a call or a text message.

Fitbit, Garmin, and Jawbone[32] all require camera access, but this is only used if the user wants to take a profile photo for the social portion of the app. Since Mio Go does not have a social function, it does not ask for such permissions.

The use of social profiles for some of the fitness apps raise questions of privacy. It is understandable that having the opportunity to connect with friends, either through social networks such as Facebook, or through the service provider's own separate social website, can be an important factor for motivating many users to engage in fitness-related activities. However, if the app provides a function to share fitness activities, these functions should be turned off by default, allowing users who want to share their data to do so by opting in.

7. Permissions and privacy by default:
Are the required permissions of the app necessary to provide the service, and does it respect privacy by default?

	fitbit	GARMIN	MIO	JAWBONE
The permissions are properly explained and justified	✓	✓	✓	✓
The settings respect my right to privacy by default	✗	✓	✓	✗

28 Regulation (EU) 2016/679 article 25 - http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679

29 http://android-developers.blogspot.no/2015/09/new-permissions-requirements-for.html [accessed 17-10-2016]

30 https://community.fitbit.com/t5/Android-App/Can-someone-explain-why-the-app-needs-access/td-p/583551 [accessed 17-10-2016]

31 https://forums.garmin.com/showthread.php?186243-Android-App-Permissions-Explained [accessed 17-10-2016]

32 https://jawbone.com/support/articles/000010178/android-app-permissions [accessed 17-10-2016]

Because Mio has no social function, they do not have privacy settings, and thus seem to respect the principle of *privacy by design*[33] (assuming they do not share data through other means).

The other three trackers all have privacy settings,[34] and Garmin respects privacy by default by having privacy settings set to show info to "Only Me" upon registering. Jawbone and Fitbit shares a lot of data with friends by default, and Fitbit shares the users' profile picture, average daily step count, and friends list by default.

As a side-note, Garmin offers in-app integration with the third-party fitness apps Strava and MyFitnessPal, while Jawbone suggests MyFitnessPal, Runkeeper, Runtastic, and MapMyFitness through the app's built-in "app gallery". It is not known whether these apps have a commercial relationship with the device providers, but these third party free apps make money through commercialization of user data[35].

33 See note 23

34 Fitbit requires the user to go through their website to access these, while Jawbone and Garmin allow users to change the settings in the app itself.

35 http://www.forbrukerradet.no/side/health-and-fitness-apps-violate-users-privacy/

5. Sharing of user data

Commercial third parties – is the user informed about who the service shares data with?

Due to the sensitivity of much of the data registered by the fitness trackers, consumers should get some indication of which third party services their data may be shared with, especially for commercial purposes. According to the Personal Data Directive the data subject must consent to this, and the data subject has rights to information on data collected, the right of access, and the right to object. These rights imply that the user needs the possibility to know who the third parties are, and thus we set a criterion that the services have to make available a list of third parties who might receive user data for further processing.[36]

Especially for commercial third parties, e.g. all marketing and promotional purposes, explicit consent should be sought before any collection or transmission of user data begins.

8. Third parties:
Am I informed about who the service shares my information with?

** Lists and explains some third parties, but this list is not extensive.*

None of the services analyzed by the NCC give any clear indication of who they share personal data with, although Fitbit mention some analytics third parties by name, as seen below:

Data Analytics:

Mixpanel: We use Mixpanel as our primary analytics tool to understand how our customers use the Fitbit Services and Mixpanel People to contact you about the use of our product, for example, to contact you if you have trouble syncing your Device. You can read the MixPanel Privacy Policy and opt-out.

We use Google Analytics and Optimizely analytics cookies allow us to see how you use our services so we can improve your experience. We encourage you

36 Although the NCC has observed that many services do not provide such a list, the example of PayPal illustrates that it is fully possible to do so in an accessible and informative manner: https://www.paypal.com/uk/webapps/mpp/ua/third-parties-list [accessed 17-10-2016]

to read the Google Privacy Policy. If you prefer to not have data reported by Google Analytics, you can install the Google Analytics Opt-out Browser Add- on. Likewise, you can read the Optimizely Privacy Policy and opt out.[37]

Regarding the question of who user data may be shared with, Garmin redirects users to "Garmin's publicly available filings with the U.S. Securities and Exchange Commission website to see the current list of Garmin's affiliates". This is an obscure and complicated way of informing consumers, and neither the NCC nor The Citizen Lab were able to actually discern who these affiliates are. [38]

In the technical tests commissioned by the NCC, several instances of data going to unlisted third parties were discovered. Garmin and Fitbit send a call to graph.facebook.com upon starting the app, regardless of whether the user actively attempts to connect to Facebook. If the user also has the Facebook-app installed on their phone, this allows Facebook to link the wristband to the phone's device ID.

The Garmin Connect app also notifies the ad-trackers Tags.tiqcdn.com[39] and Gigya[40] while using the app, transmitting the device's IP-address. Although the tests have not shown any clear indication that this data is transmitted for marketing purposes,[41] the information that is transmitted could be used to display targeted advertising on different platforms.[42] None of the relevant terms or privacy policies state that data is being passively sent to these third parties when using the apps.

> Personal data such as location or habits are particularly valuable to marketing companies. This info can for example be used to tailor targeted ads based on where you are, what you like, or even how you feel.[43]

37 https://www.fitbit.com/no/legal/privacy [accessed 17-10-2016]

38 This is the document Garmin refers to: https://www.sec.gov/Archives/edgar/data/1121788/000161577416004243/s102606_10k.htm [accessed 17-10-2016]

39 Owned by Tealium, who specialize in connecting and organize data sources to create customer and marketing profiles: *"With your data foundation in place through Tealium iQ Tag Management, you can create universal profiles in AudienceStream that span the entire customer journey – from unknown visitors to known customers and from every touchpoint, including offline and IoT devices."* Source: http://tealium.com/tour.html

40 Gigya specialize in creating customer profiles based on de-identifying individuals: *"Turn anonymous visitors into known customers with social and traditional registration tools that let you easily authenticate users and collect rich first-party data."* Source: http://www.gigya.com/

41 The NCC have been informed that Garmin uses Gigya for social log-in functions, but the technical tests have shown that data is transmitted on the log-in page even if the social log-in function is not used. This could be because of a technical error.

42 *Investigation of privacy issues with Fitness Trackers, p. 6*

43 https://www.theguardian.com/lifeandstyle/2015/jul/31/biometric-data-apple-wimbledon-facebook-mindshare-affectiva-unilever-coca-cola-mars [accessed 17-10-2016]

Explicit and informed consent

Related to point eight, whenever a service wants to share user data with (commercial) third parties, the user should be able to choose whether they consent to this sharing. In other words, it is not enough to bury such consent within the lengthy terms of service and privacy policy, as this is not explicit and informed from our point of view.

9. Explicit and informed consent: will the service ask me for separate consent if they want to share my data with commercial third parties?

** Indicate that they will ask for explicit consent, but use vague and non-committal language*

Here, Jawbone and Garmin are best in class, with Garmin stating that

> *"Garmin will not transfer or sell your activity data to any third party without providing you prior notice and obtaining your consent."*
>
> Garmin privacy policy

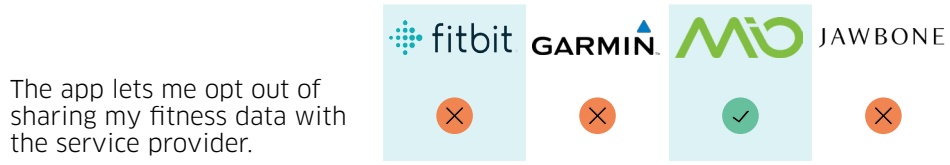
Jawbone has a similar disclaimer in their privacy policy, stating that they will never share or sell data without obtaining prior consent. Mio uses somewhat vague language here ("we *may* share"), and state that the user will be notified about data sharing *"Other than as described in this Privacy Statement*" (Mio privacy policy). In their Privacy Shield document, Fitbit states

"Fitbit generally offers Consumers the opportunity to choose whether their Personal Data may be (i) disclosed to third-party Controllers or (ii) used for a purpose that is materially different from the purposes for which the information was originally collected or subsequently authorized by the relevant Consumer.".

This is an example of choice that comes closer to adhering to the European data protection standards demanded of the Privacy Shield, but the use of "generally offers" is unfortunately vague and opens up to exceptions. It should be noted that while the terms may state that prior and explicit consent will be sought, it is difficult to ascertain whether this happens in practice.

Since not all users of activity trackers want to use the device for social or comparative reasons, the NCC would like to see a wider adoption of an option to opt-out of sharing fitness data with the service provider. It is understandable, however, that many services will not have such an option, either for functionality-related or analysis-related reasons. As shown below, it is possible to design a fitness app without collecting data from the users' phones

10. Sharing with the service provider: Does the service allow me to opt out of sharing my fitness data with the service provider?



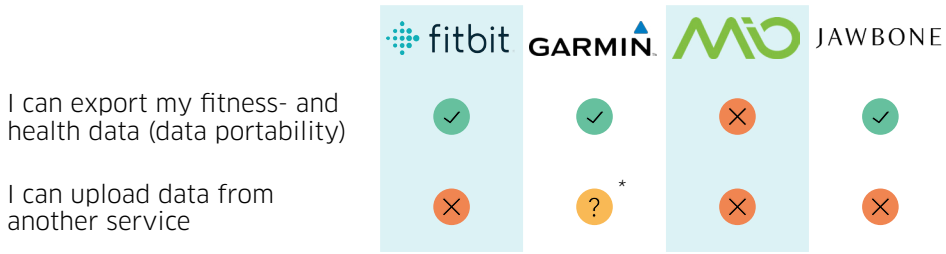
As mentioned, Mio stands out from the other three services by not having a social function. This relatively limited functionality might be why Mio includes an unticked box during registration, saying "*I agree to share my workout data with Mio*". This box can be left unticked, meaning that users can keep their workout data completely private. Providing leaving the box unchecked limits data sharing in a meaningful way, the NCC regards this as an elegant solution that respects the users' privacy. Although the integrated analytical and social functions of the other three trackers mean that the need for transmitting data online can be justified in most cases, the NCC suggest that a strictly "offline" functionality could be implemented in all four apps, for the users who simply want to record their fitness data.

6. Portability and deletion of personal data

Data portability – can the user easily move their data to or from the service?

It is important for consumers' freedom of choice that digital service providers support data portability, preferably letting users download their personal data in a standardized format so that they can easily upload their information to a potential new service. This criterion is based on the risk faced by consumers that personal data might be non-portable, which could lead to a "lock-in" effect when using digital services. This means that, for example, if you cannot bring the information from your iPhone with you to an Android system, the threshold for switching between brands becomes quite high and consequently results in lock-in effects as well as weakened competition. The criterion is also rooted in the new GDPR, in which portability becomes a right.[44]

11. Data portability:
Can I easily move my data from and to the service?



** Lets users upload their data, but in a different file format than the other services export data to.*

Fitbit, Garmin, and Jawbone all let their customers download their exercise data through their websites, through a relatively simple process. It seems that Mio has been working on implementing such a function since early 2015,[45] but they have not implemented this as of October 2016.

Interestingly, of the four services, only Garmin has a function for users to *upload* their data, although not in the file-format used by the other services (.CSV/.XLS).[46] Although other third party fitness apps will let you use the data you downloaded from for example Fitbit, it is notable that you cannot bring your downloaded Fitbit data directly to a Jawbone or Garmin device, nor vice versa.

44 Regulation (EU) 2016/679, article 20

45 http://blog.mioglobal.com/exciting-mio-go-app-updates-for-ios/ [accessed 17-10-2016]

46 Through the user profile on the Garmin Connect website.

It seems clear that the possibility to export your data should be accompanied by a similar way to import it.

Data retention policies – is the user data deleted when the account is deleted?

Because of the sensitive nature of fitness and health data, it is important that the services specify deletion procedures of user data, especially if the user deletes their accounts. An action like this will comply with the Personal Data Directive requiring purpose limitation, which also applies on storage over time.[47] Many users automatically assume that once you delete an account through a digital service, the data collected by the service is also removed from the server. As we will see, this is often not the case.

12. Data retention policies:
Is my data deleted when I delete my account?

Unfortunately, none of the analyzed fitness trackers explicitly state that they will delete user data when the account is deleted. Fitbit is probably the least worst on this point, stating that when the user account is deleted,

> *"data that can identify you will be removed from the Service"*
>
> Fitbit privacy policy

However, they continue by saying,

> *"Backup copies of this data will be removed from our server* ***based upon an automated schedule****, which means it may persist in our archive for a short period.* ***Fitbit may continue to use your de-identified data****."*
>
> Fitbit privacy policy, emphasis added

While the concept of an automated schedule for deletion is not bad in itself, there is no clear indication of the timespan between these sweeps. Additionally, the use of "de-identified data" is problematic, as there is little agreement about when data can be considered "de-identified" or "anonymized". As big data

47 Directive 95/46/EC article 6

algorithms become increasingly sophisticated, it becomes very difficult (some say impossible) to completely anonymize datasets.[48]

Mio's privacy policy states that they "*Reserve the right to retain personal information relating to you for a period of time*", without saying anything about what "a period of time" entails. In addition, the user may "***delete certain personal information*** *through that Account*", using vague language about what "certain personal information" actually is.

Similarly, Jawbone states that "*you can request the deletion of your individual user data from our system*", and in order to do this you have to contact customer support to make the request. Finally, Garmin states that "*there may also be residual information that will remain in our databases and other records, which will not be removed.*", but does not specify what this "residual information" might be.

Data retention – is the user data deleted if the user has stopped using the service, or been inactive for a longer period of time?

When a user has been inactive for a longer period of time, all personal information about the user should be treated as being expired, and should therefore be deleted from the service providers' system. The amount of time that has to pass before this happens should be clearly specified, so that data is not kept in perpetuity long after the user has stopped using the service[49].

13. Data retention:
Is my data deleted if I have stopped using the service or been inactive for a while?

	fitbit	GARMIN	MIO	JAWBONE
My data are deleted after a set period of inactivity	✗	✗	✗	✗

None of the four fitness trackers mention data retention periods at all, which leads the NCC to assume that they do not delete inactive users' data. This is problematic, since many users might delete the apps and assume that their information will not be put to further use. If inactive users' data is not deleted, it could potentially be re-used for other purposes long after the user left the service.

48 https://hbr.org/2015/02/theres-no-such-thing-as-anonymous-data [accessed 17-10-2016]

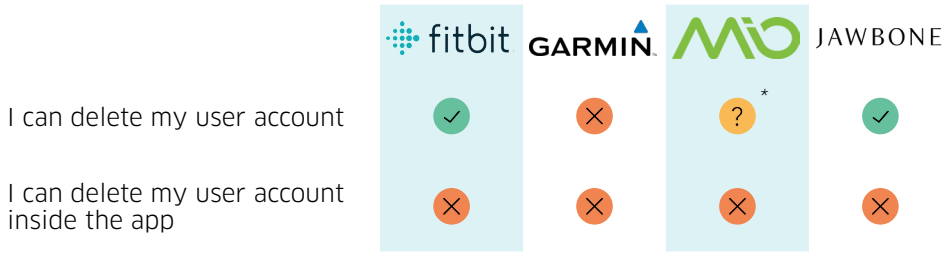
49 This is in line with WP29 Opinion 02/2013 – on apps on smart devices - http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf

Deleting an account

It should generally not be more difficult to leave a service than it is to sign up, so there should be a "delete account"-function within the apps themselves. This demand is consistent with the recommendation in WP29 Opinion 02/2013 on apps on smart devices.

All four of the analyzed fitness trackers require a user account in order to function, although various degrees of information is required (see point six). In every instance, the user is prompted to create an account upon opening the app for the first time. Account creation happens within the app, and is quick and simple in all four services.

14. Deleting an account:
Can I delete my account, and if so, can I do it directly in the app?



* *States that you can «delete certain personal information». It is unclear what exactly this entails.*

None of the four apps that the NCC analyzed allow for easy deletion of the account within the app itself. Fitbit and Jawbone requires the user to contact customer support to request deletion, which can be a lengthy and frustrating process. Mio lets the user delete "certain information" through the account, but it is unclear from the terms how to delete the account in itself. Somewhat bizarrely, hidden in a rather difficult to navigate FAQ, Garmin states that

> **"***There is no way to delete a myGarmin or Garmin Connect account."*
>
> Garmin FAQ[50]

Even though you can request to delete certain information through their customer support, one must assume that Garmin will at least store usernames and e-mail addresses forever. It is hard to believe that technical limitations prevent Garmin from letting users delete their accounts, so this practice is unacceptable.

With the rise of smartphones, apps have become dashboards for a wide variation of activities. App-designers are often experts at designing simple and compelling interfaces, and therefore important functions should be available without having to leave the app.

50 Because of the way that the site is set up, it is not possible to link directly to individual parts of the FAQ.

Termination of account – will the service notify the user if the account is blocked or terminated?

If a user's account is deleted by the service (for example due to breach of terms), the user should be notified before the account is terminated51. We deem this a fair demand on the service providers, as the users should be able to "save" or reclaim their own data and download it before it is deleted.

15. Termination of account:
Will the service notify me if my account is blocked or terminated?

** Does not mention termination of account. Because of the lack of a social function, it is unclear whether this is relevant.*

None of the four fitness trackers seems to respect this consumer right. Fitbit's terms of service puts it bluntly:

> *"If you violate these Terms, we reserve the right to deactivate your account or terminate these Terms,* ***at our sole discretion, at any time and without notice or liability to you.****"*
>
> Fitbit terms of service, emphasis added

Similarly, if any terms are breached, Jawbone reserves the right to

> *"****at its sole discretion, without notice to you*** *may: (i) terminate these Terms; (ii) terminate all rights of your Account; and (iii) preclude you from accessing the UP Service or any part of it."*
>
> Jawbone terms of service, emphasis added

Garmin simply states that they may terminate the user account in the case of breached terms,[52] without mentioning giving any notice to the user if this happens. Mio does not talk about terminating user accounts at all, but the lack of a social function connected to the user account makes it questionable whether there are any potential grounds for termination.

51 This could also be a question if the actual term infringes article 3(3) of the Directive on unfair contract terms in consumer contracts, cp annex, number 1, k - http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:31993L0013

52 Somewhat absurdly, this means that Garmin can delete the user account, but the user cannot delete their account themselves.

7. Summary

As the above points have illustrated, the various service providers all have their strengths and weaknesses when it comes to respecting consumer rights. While Fitbit has the longest word count for their terms and conditions, these documents are the most easily readable, while all of the services collect more data than necessary, and none properly specify who they are sharing user data with. Additionally, all four services have in common that none of them satisfy all of the NCC's criteria. This seems to call for an overhaul of the way that fitness trackers treat consumers' data. Health data is, as seen over the course of this report, very sensitive information, and should not be treated lightly.

Since app-operated fitness wearables is a still evolving technology, there is still time to implement consumer-protective measures and standards. In addition to the analysis of these wristbands, the NCC has written a set of tips to consumers[53], to help them peruse the technology while maintaining their rights, and a set of demands[54] to the manufacturers of these devices and services. With the new General Data Protection Regulation coming into force in 2018, many of the issues outlined in this paper will become easier to address when regarding European citizens' personal data. By implementing principles such as privacy by design, these service providers will be ready for the new regulation, and also enhance consumer trust, which is good for both users and for businesses.

53 http://www.forbrukerradet.no/siste-nytt/concumer-tips-using-activity-trackers

54 http://www.forbrukerradet.no/siste-nytt/10-demands-for-consumer-friendly-activity-trackers

Links to the terms and conditions

Fitbit

- ToS: https://www.fitbit.com/no/terms [October 22, 2015]
- PP: https://www.fitbit.com/no/legal/privacy [August 10, 2014]
- Privacy Shield PP: https://www.fitbit.com/legal/privacyshield [September 28, 2016]

Note: Fitbit updated their privacy policy for American users on August 9, 2016. This new version is not available to Norwegian users, and has not substantially changed any of the terms that the NCC has remarked upon in this report.

Garmin:

- ToS: http://www.garmin.com/nb-NO/legal/terms-of-use [July 19, 2016]
- PP: http://www.garmin.com/nb-NO/legal/privacy-statement [January 11, 2016]

Mio:

- ToS/PP: https://d3b2h820vtsscl.cloudfront.net/miogo/terms/en/terms_and_conditions.html [July 31, 2014]

Jawbone

- ToS: https://jawbone.com/legal/terms/ [December 16, 2014]
- PP: https://jawbone.com/privacy [December 16, 2014]

FOR MORE INFORMATION

Finn Lützow-Holm Myrstad
Head of section, digital services and electricity

E-mail: Finn.Myrstad@forbrukerradet.no
Mobile: +47 479 66 900