

Fitness Tracker Policy Question Set

Open Effect; Version 1.0

I. Policy Questions

A. Is there a link to the privacy policy on the app store page?

ANALYSIS:

- significant variance in whether privacy policy just relates to tracker or corporation actions more generally
- Xiaomi privacy policy/ToS not evidently accessible from website. No link to it in the Play Store

Company	Short Response	Detailed Response
Apple	N/A	On product page, there is a link to Apple's privacy policy and a link to Apple's 'Privacy' value. Both are in the footer of the Apple Watch product page.
Basis	iOS (Yes) // Android (Yes)	Combines Web and Fitness Tracker privacy information on same page.
Bellabeat	iOS (Yes) // Android (Yes)	Both link to the privacy policy. There is a separate ToS agreement that is linked at the bottom of the company's webpage.
Fitbit	iOS (Yes) // Android (Yes)	Comprehensive, and includes account information, device information, purchase information, and web browsing information, and that various services (e.g. adding friends, location functions).
Garmin	iOS (Yes) // Android (Yes)	Comprehensive and all on the same page. Includes discussions of advertising, web beacons and cookies, device information, apps, etc.
Jawbone	iOS (Yes) // Android (Yes)	Privacy policy defaults to Jawbone's Website Privacy URL.
Mio	iOS (Yes) // Android (Yes)	Principally has information about the company's website privacy policy.
Withings	iOS (Yes) // Android (Yes)	Brings to list, where privacy policy (along with application terms of use, policy on data protection, etc) linked.

Xiaomi	iOS (Yes) // Android (No)	iOS includes privacy policy on same page as the Mi Band User Agreement.
--------	---------------------------	-------------------------------------------------------------------------

B. Is there a link to the application's/device's privacy policy on the vendor's website?

ANALYSIS:

- all companies other than Jawbone and Xiaomi have easily accessible/discoverable links to their privacy policy on corporate websites

Company	Short Response	Detailed Response
Apple	Yes	On product page, there is a link to Apple's privacy policy and a link to Apple's 'Privacy' value. Both are in the footer of the Apple Watch product page.
Basis	Yes	At bottom of homepage.
Bellabeat	Yes	At bottom of homepage.
Fitbit	Yes	At bottom of homepage.
Garmin	Yes	At bottom of homepage.
Jawbone	Sort of	From bottom of page, go to website privacy -- there is an item on the horizontal menu for 'software and services'. This lists the pertinent information about what the devices collect.
Mio	Yes	At bottom of homepage.
Withings	Yes	At bottom of homepage.
Xiaomi	Yes*	At bottom of homepage. However, privacy policy on homepage is not the same as is available from the iOS store.

C. Is there a unique policy for the tracker, or does a generic policy hold across services?

ANALYSIS:

- It is rare for companies to break down just how fitness applications and devices collect data or are addressed by corporate privacy policies because of how the policies aggregate much of the company's privacy information in a single document. Jawbone, Xiaomi, and (to some extent) Apple are best at separating out data.

Company	Short Response	Detailed Response
Apple	Generic + some specificity	Apple's privacy commitments are broken up in a series of locations. Their privacy policy, as an example, does not specifically mention Apple Health or Fitness, though specific information about how these services are secured is accessible when reading the "Privacy Built In" part of Apple's website.
Basis	Aggregate Policy	They have one page, which includes privacy-related information concerning: automatically collected information from websites and behavioural ads; registration information; information collected from devices; the use of collected information; sharing of collected information; policy concerning collecting children's information; as well as about links to other sites, security, and preferences. It also includes contact information for company's privacy officers.
Bellabeat	Aggregate policy	The single privacy policy applies to both the website as well as the company's mobile application.
Fitbit	Aggregate policy	On a single page, Fitbit describes how it collects and uses information from its devices, online services, and web presence.
Garmin	Aggregate policy	One a single page, Garmin describes how it collects information from communications (between customers/company), customer support transactions, purchases, promotions, postings to their forums and online

		properties, location information, and event logs, activities and activity data, server logs, and cookies and “other technology, as well as use of apps”.
Jawbone	Unique ToS and Privacy Policy	Accessible by clicking a link on the company’s aggregated privacy policy and ToS.
Mio	Generic	A generic policy for website-collected data is provided. There is no explicit mention for fitness tracker-related products or data collection.
Withings	Generic	The privacy policy applies to all Withings products and services. The company includes notes where either biometric or activity data is collected throughout the privacy policy.
Xiaomi	Unique	Only linkable from iOS app store; can’t find it from public Xiaomi website.

D. Is there a reference to national laws, international guidelines, or regulatory instruments? Are specific nations’ laws mentioned?

ANALYSIS:

- 4/9 claim EU-SH compliance; while arbitration or proceedings are often (3/9) mentioned, there is divergence where in the US such arbitration must take place.

Company	Short Response	Detailed Response
Apple	Yes	A range of different international guidelines are cited. These include: Safe Harbour-EU/Swiss frameworks , information about members of the European Economic Area and Switzerland is processed in Cork, Ireland; APEC principles are also abided by.

		<p>While the Apple website terms of use note that jurisdiction is constrained to the US, unless a complaint is brought by a resident of the EU.</p> <p>The Apple Watch licensing document states that the “Licence will be governed by and construed in accordance with the laws of the State of California, excluding its conflict of law principles. This License shall not be governed by the United Nations Convention on Contracts for the International Sale of Goods, the application of which is expressly excluded. If you are a consumer based in the United Kingdom, this License will be governed by the laws of the jurisdiction of your residence. If for any reason a court of competent jurisdiction finds any provision, or portion thereof, to be unenforceable, the remainder of this License shall continue in full force and effect.”</p>
Basis	Yes	<p>1) Notes data may be stored on servers in the US or “in other countries that may not be required to adhere to the same level of personal data protection as required in the EU.”</p> <p>2) US-EU Safe Harbor Framework</p> <p>3) US-Swiss Safe Harbour Framework</p> <p>4) BBB EU Safe Harbour (for unresolved privacy complaints under the Safe Harbour principles)</p>
Bellabeat	Yes	<p>PRIVACY POLICY: “Some elements of the Service may be hosted on servers located in countries outside your home country, such as in the European Union or in the United States. The laws applicable to the protection of personal data in such countries may be different from those applicable in your home country. By registering with the Service, you consent to personal data about you being transferred outside your home country.”</p>

		<p>ToS: “The laws of the State of California, without regard to or application of its conflict of law provisions, will govern these Terms, and any claim, cause of action or dispute arising out of or relating to these Terms will be brought solely in the courts of the County of San Francisco, State of California. You hereby consent to the jurisdiction of and venue in such courts and waive any objection as to inconvenient forum.”</p>
Fitbit	Yes	<p>PRIVACY POLICY: The company asserts that its Services are wholly hosted in the US and advised “that United States law may not offer the same privacy protections as the law of your jurisdiction.” The same document notes that Fitbit complies with US-EU Safe Harbour Framework as well as the US - Swiss Safe Harbour framework. In the case that a complaint arises, Fitbit commits to resolving these sorts of complaints to the BBB EU Safe Harbour, operated by the Council of Better Business Bureaus.</p> <p>TOS: All court processes will occur in the State of California. Arbitration will be first attempted, unless a person opts out of arbitration clause within 30 days of activating service. Jury trials are waived by both parties. Class actions are waived. Small claims may be taken up in other jurisdictions in the US.</p>
Garmin	Yes	<p>Privacy Policy: Notes that Garmin complies with U.S.-EU Safe Harbour and the US-Swiss Safe Harbour framework. If users have questions or concerns regarding compliance they are directed to contact the Garmin webmaster and, if unsatisfied with the response, submit “an eligible Safe Harbour mediation claim” to JAMS International. Such a claim will be “mediated in accordance with the JAMS International Mediation Rules.”</p>

		<p>ToS: Generally legal issues linked to the Garmin Site will be taken up in Kansas State. The exception is citizens of EU countries, who agree to be governed by English law and to London, England as the forum in which legal actions will be resolved.</p>
Jawbone	Yes	<p>Users consent to US jurisdiction for arbitration of any claims, specifically conducted in San Francisco, California. No mention is made of Safe Harbor law.</p> <p>The Privacy Policy notes that those in the European Economic Area can contact Jawbone via their UK subsidiary "with questions or concerns regarding Jawbone's data processing activities and compliance with European data protection laws." Though we analyzed the Canadian-localized version of the privacy policy, we also examined the Ireland-localized privacy policy. The Irish polict also did not refer to Jawbone/its subsidiary's data processing obligations or practices under EU law.</p>
Mio	Not really	<p>No explicit note is made to the jurisdiction the company requires or expects legal issues to be brought up. There is no mention of EU-Safe Harbour or OECD Principles, or Canadian privacy laws. The company asserts that it adheres to PCI for payment processing.</p>
Withings	Yes	<p>Applications Terms of Use: Notes that agreement is governed by the courts in the State of Massachusetts . There is no mention of EU-Safe Harbour or OECD Principles, or regional/national privacy laws. The company asserts that if arbitration is taken up, then it will be administered by Judicial Arbitration and Mediation Services, Inc. (JAMS).</p> <p>It should be noted that the company may believe there is no need to comply with</p>

		Safe Harbour on the basis that Withings commits to storing data in different locations. Specifically, 8. Where are your personal data kept? notes the following: <ul style="list-style-type: none"> • Europe: Ireland • North America: United States • South America: Brazil • Asia: Japan/Singapore • Australia: Australia
Xiaomi	Yes	ToS: Notes that the agreement is governed by the Republic of Singapore. No reference to other nations' laws or data instruments.

E. Are there references to any country's health laws?

ANALYSIS:

- This is a significant, if unsurprising, finding: companies that positioned their devices as mHealth might note medical information, but fitness/wearable companies have/are skirting this designation

Company	Short Response	Detailed Response
Apple	No	--
Basis	No	--
Bellabeat	No	However, Bellabeat has an extensive discussion in the ToS asserting that "Bellabeat is not a diagnostic tool and does not promote or recommend any particular form of medical treatment."
Fitbit	No	--
Garmin	No	--
Jawbone	No	--
Mio	No	--
Withings	No	--
Xiaomi	No	--

F. Does the company possess a privacy designation (e.g. TRUSTE mark, Privacy by Design)?

Company	Short Response	Detailed Response
Apple	No	--
Basis	No	---
Bellabeat	No	--
Fitbit	No	---
Garmin	No	---
Jawbone	No	---
Mio	No	--
Withings	No	--
Xiaomi	No	--

G. Is there a statement about which courts must be appealed to?

ANALYSIS:

- Users generally agree to US jurisdiction though specific courts vary. The sole Canadian company has no mention of jurisdiction and the Chinese company's legal policy states that conflicts are taken up in Singapore.

Company	Short Response	Detailed Response
Apple	Not really	<p>There are references to various principles that Apple adheres to (mentioned at 1D), and the Website terms of service note that <i>website-based</i> complaints are brought first in the US unless a complainant is an EU citizen (in which case a complaint can be brought in the relevant nation).</p> <p>The Apple Watch licensing document states that the "Licence will be governed by and construed in accordance with the laws of the State of California, excluding its conflict of law principles. This License</p>

		shall not be governed by the United Nations Convention on Contracts for the International Sale of Goods, the application of which is expressly excluded. If you are a consumer based in the United Kingdom , this License will be governed by the laws of the jurisdiction of your residence . If for any reason a court of competent jurisdiction finds any provision, or portion thereof, to be unenforceable, the remainder of this License shall continue in full force and effect.”
Basis	No	--
Bellabeat	Yes	ToS: “Governing Law and Resolution of Disputes The laws of the State of California, without regard to or application of its conflict of law provisions, will govern these Terms, and any claim, cause of action or dispute arising out of or relating to these Terms will be brought solely in the courts of the County of San Francisco, State of California. You hereby consent to the jurisdiction of and venue in such courts and waive any objection as to inconvenient forum.”
Fitbit	Yes	TOS: federal or state courts of San Francisco County, California . Exceptions are for small claims, which may occur in other courts i the US.
Garmin	Yes	ToS: US District Court of Kansas , or any Kansas State court sitting in Johnson County. Exceptions are made for EU citizens , who agree to be governed by English law and take up claims in London, England .
Jawbone	Yes.	Terms of Use: Arbitration will be taken up in San Francisco, California by the American Arbitration Association . Use of the devices are governed by the laws of California, USA .

Mio	No	--
Withings	Yes	Withings - Applications Terms of Use: this document asserts that the terms of use "and all actions related thereto shall be governed, controlled, interpreted by and construed in accordance with the laws of the State of Massachusetts (USA) without regard to principles of conflict of laws."
Xiaomi	Yes	The ToS notes that the agreement "is governed by the laws of the Republic of Singapore . Disputing parties should strive to resolve any disputes in relation to the terms of this Agreement amicably. If an imicable settlement is not possible, the disputing parties agree to submit to the non-exclusive jurisdiction of the courts of Singapore. "

H. Does the privacy policy reference the terms of service, or vice versa?

ANALYSIS:

- Despite the interwoven nature of companies' terms of service and privacy policy documents, they are not always linked to one another in actual policy/legal documents

Company	Short Response	Detailed Response
Apple	Yes	The privacy policy refers to the Terms and Conditions, and the Apple Watch ToS reference Apple's privacy policy.
Basis	No	---
Bellabeat	Yes	Privacy Policy: Though terms of Use are noted, there is not a direct link to them. Also, the website uses 'Terms of Service' and not 'Terms of Use.' ToS: Though the Privacy Policy is noted, there is not a direct link to them in the ToS.
Fitbit	Sort of	ToS: refers to Privacy Policy, with link.

		Privacy Policy: though terms of service are noted, there is not a link to the ToS within the Privacy Policy . It is available at the footer of the site.
Garmin	No	---
Jawbone	Sort of	Users can click the Terms of Use from the Privacy Policy, and vice versa. The Privacy Policy references the terms of use as a reason to potentially disclose a user's data. The Terms of Use does not explicitly reference the Privacy Policy.
Mio	Yes	The Privacy Policy and Terms of Service note one another. However, both apply generically and are written for the website-collected data and do not mention fitness collection at any point.
Withings	Sort of	Withings has multiple Terms of Use; some refer to the Privacy Policy. There is no evident hyperlink in the Privacy Policy that links to a Terms of Use document.
Xiaomi	Yes	ToS: item 10. notes that the Privacy Policy is "incorporated into and forms part of this Agreement." Privacy Policy: no mention.

I. Is the privacy-related information all in one place?

ANALYSIS:

- Many companies separate privacy information from that which prescribes where complaints with legal bearing can be taken up, hindering individuals from fully understanding how the company in question governs its devices, applications, and customers' personal information.

Company	Short Response	Detailed Response
Apple	Not Really	There are various ways to get to the Privacy Policy, such as in footer of website or via the company's Privacy value. Then, there are different pages for a variety of privacy-related issues (e.g.

		government requests, application-level privacy protections, ways for users to manage their own privacy).
Basis	Yes	---
Bellabeat	No	While the Privacy Policy is comprehensive, legal information pertaining to courts (e.g. "The laws of the State of California, without regard to or application of its conflict of law provisions, will govern these Terms, and any claim, cause of action or dispute arising out of or relating to these Terms will be brought solely in the courts of the County of San Francisco, State of California. You hereby consent to the jurisdiction of and venue in such courts and waive any objection as to inconvenient forum.") is separated into the ToS.
Fitbit	No	While the Privacy Policy is comprehensive, arbitration and legal information (e.g. courts, waiving of rights, etc) are exclusively detailed in the ToS.
Garmin	No	While Privacy Policy is comprehensive, legal information pertaining to the courts and waiving of rights (i.e. "You irrevocably waive, to the fullest extent permitted by law, any objection which you may now or hereafter have to the laying of the venue of any such proceeding brought in such a court and any claim that any such proceedings brought in such a court has been brought in an inconvenient forum.")
Jawbone	No	While the Privacy Policy is comprehensive, legal information pertaining to arbitration and waiving of jurisdictional prerogative is established in their Terms of Use for the UP device.

Mio	No	The Privacy Policy makes no explicit mention for data collected in the course of providing a fitness-related wearable. The closest it comes to affirming this is when describing 'Information Collection and Use' that the company collects "other information that you decide to provide us with, or that you decide to include in your public profile."
Withings	Sort of	Withings has a page where along the left side of the page are links to different legal documents (e.g. data protection policy, privacy policy, policy on cookies, countries products provided to, etc.). Many of these documents interlink with one another. However, knowing which policies have to be read and what, specifically, they cover is not necessarily apparent by looking at the titles of the documents themselves.
Xiaomi	Yes	The User Agreement and Privacy Policy are part of the same page, so though separate documents one follows the other on the page.

J. Is there information about when the privacy policy was last updated? Does it note content changes?

ANALYSIS:

- While many companies identify when their policy was last updated, users cannot ascertain what (if anything) substantively changed. Thus, they must engage in ongoing (and laborious) efforts to see how, and to what extent, a company is modifying its data handling, collection, and disclosure practices.

Company	Short Response	Detailed Response
Apple	Yes (last updated) // No (content changes)	Last updated, no link to prior policies.
Basis	Yes (last updated) // No (content changes)	While last update is noted, content changes are not discussed.

Bellabeat	No // No	While the Privacy Policy asserts that a notice will be placed, to indicate the date the Privacy Policy was created, there is no date on the current policy. Specifically the policy reads: "From time to time we may change this Privacy Policy. You can tell when changes have been made to the Privacy Policy by referring to the Last Updated legend on top of this page. If we materially change the ways in which we use and disclose personal data, we will post a notice in the Service and send an e-mail to our registered users. Your continued use of the Service following any changes to this Privacy Policy constitutes your acceptance of any such changes made."
Fitbit	Yes (last updated) // No (content changes)	Last updated is noted. Content changes are not. Though there is a link to past Privacy Policies at the bottom of the current privacy policy, it resolves only to a 404 error when 'Canada' is the identified country. They resolve when selecting 'United States' as the identified country the user is from.
Garmin	Yes (last updated) // No (content changes)	While last update is noted, content changes (and past privacy statements) are not discussed.
Jawbone	Sort of (effective as of date) // No (no content changes)	<p>The Terms of Use show the date when they were last updated and effective as of.</p> <p>There is an 'effective as of' date for the Privacy Policy, but no indication of when the policy was last updated. Jawbone does, however, commit to "change the last updated date above to let you know we made a change." They do not commit to discussing what those changes might be or notifying users of such changes.</p>
Mio	No	--

Withings	Yes (last updated) // No (content changes)	The policy does note when it when it was last updated. It does not specify what the changes were.
Xiaomi	No	The Privacy Policy does not have an 'effective as of' date, or set of previously posted privacy policies. Though the company commits to posting "changes on all the Xiaomi websites" we were unable to actually find the User Agreement and Privacy Policy from the Xiaomi website itself. We could only find it by clicking the privacy policy link in the iOS store.

K. Are past versions of the Privacy Policy available?

ANALYSIS:

- Only Withings makes past policies accessible

Company	Short Response	Detailed Response
Apple	No	--
Basis	No	They are not accessible from the Privacy Policy; if they exist, they are not linked from the policy itself.
Bellabeat	No	It is unclear if there are updates to the policy. The company states that there will be dates on the top of the page, but no indication of when the policy was generated are displayed there or elsewhere on the page.
Fitbit	No/Sort of	<p>While there is a link to past policies at the bottom of the website, it does not resolve to past policies and instead resolves to a 404 error when 'Canada' is the identified country. They resolve when selecting 'United States' as the identified country the user is from.</p> <p>The 'United States' website shows past privacy policies.</p>

Garmin	No	They are not accessible from the Privacy Policy; if they exist, they are not linked from the policy itself.
Jawbone	No	They are not accessible from the Terms of Use or Privacy Policy. If they exist, they are not linked from the policies themselves.
Mio	No	--
Withings	Yes	They are available through links at the end of the current Privacy Policy.
Xiaomi	No	--

- L. Does the company reserve the right to change the privacy policy or terms of service? Will the company notify the users of changes and, if so, how?

ANALYSIS:

- While all companies commit to notifying users -- though often in vague or non-specific ways -- no company commits to notifying users in the applications associated with the company's fitness device(s).

Company	Short Response	Detailed Response
Apple	Yes	Apple "may update its Privacy Policy from time to time. When we change the policy in a material way, a notice will be posted on our website along with the updated Privacy Policy."
Basis	Yes; multiple ways of notifying users	Basis reserves right to change its policy "from time to time." The company commits to notifying users by: 1) revising data at top of policy; 2) potentially contacting individual by email or posting update notice on homepage. Suggests "you access the Services to stay informed about our information practices."
Bellabeat	Yes // Yes	Bellabeat notes that from "time to time" the company might change its policy, and that the legend at the top of the

		<p>page will display one set of changes and, second, that for material changes there will be a “notice in the Service” and the company will “send an email to our registered users.”</p>
Fitbit	Yes // Yes	<p>The company may change its policy, though in doing so will not include previously collected data under the new terms. If modifications “substantially” change users’ rights then Fitbit will summarize the changes via an email and provide a notice on the Fitbit website.</p>
Garmin	Yes // multiple ways of notifying users	<p>Garmin reserves the right to update their policy as they add new products and applications, update their offerings, or as technologies/laws change. They will provide notices to individuals by email, posting notice of updated policy on websites, or by other means (consistent with applicable law) where the changes are material and where Garmin must obtain user consent.</p>
Jawbone	Yes // Left unspecified	<p>Jawbone notes that it may update its privacy policy. The company does not commit to informing users of these updates or changes. There are no mentions of whether the company can update its Terms of Use, nor whether it will notify users of updates to the Terms of Use.</p>
Mio	Yes // left unspecified	<p>The Terms of Service notes that the company “can revise these policies, terms, and conditions at any time by updating this posting, and your use after such change signifies your acceptance of changed terms. Please check these terms of use periodically for changes.”</p> <p>In the “Other Uses” section of the Privacy Policy, the company notes that it “reserves the right to change or update this policy, or any other policy or practice, at any time, with reasonable</p>

		notice to users of its website. Any changes or updates will be effective immediately upon posting our site(s)."
Withings	Yes // left unspecified	"We may change our confidentiality policy to adapt to your needs, to the evolution of the legal framework or when we develop our products and services. We shall inform you of any modification performed."
Xiaomi	Yes	The company may update its privacy policy. Xiaomi will seek "fresh consent" before collecting additional personal information or when the company wants to "use or disclosure your personal data for new purposes." However, notification is limited to posting the "changes on all the Xiaomi websites, so that you may be aware of the information we collect and how we use it." Continuing to use a product or service amounts to accepting the new terms/agreement.

II. Procedures for Users

- A. Is there a privacy officer noted in the privacy policy? Is privacy-related contact information provided?

ANALYSIS:

- While no company actually identifies their privacy or data protection officer (if they even possess them), all have some way to contact the company about privacy-related issues. 4/9 of companies have a clear privacy-specific email address.

Company	Short Response	Detailed Response
Apple	No // Yes	Apple does not list a specific privacy officer. However, they provide the option for people to contact Apple using a contact form on the company's website (http://www.apple.com/ca/privacy/contact/).

Basis	No // Sort of	No specific privacy officer, or office, is noted. Email is for ' support@mybasis.com ' as opposed to a dedicated privacy email address.
Bellabeat	No // Sort of	No specific privacy officer is noted. Email is for ' hi@bellabeat.com ' as opposed to a dedicated privacy email address.
Fitbit	No // Yes	<p>While no specific person is noted, there is a Privacy Officer email and letter mailing addresses.</p> <p>Email: privacy@fitbit.com</p> <p>Mailing: Privacy Officer Fitbit, Inc. 405 Howard Street San Francisco, CA 94105</p>
Garmin	No // Sort of	No specific privacy officer is noted. Email is for " webmaster@garmin.com " and the mailing address is to the Webmaster at the Garmin Kansas City location.
Jawbone	No // Sort of	No specific privacy officer is noted. The Privacy Policy recommends individuals to contact info@jawbone.com if they have questions; the same email is for EU-based customers who want to contact the company about European Data Protection compliance. The Terms of Use also provides the address for Jawbone's General Counsel.
Mio	No // Sort of	No specific privacy officer/office is noted. Email can be sent to info@mioglobal.com or sent by letter mail to an address at the end of the privacy policy.
Withings	No // Yes	No specific privacy officer is noted, though email can be sent to privacy@withings.com or mailed to an address. These are listed at the top of the privacy policy.

Xiaomi	No // Yes	While no specific data privacy officer is noted, users are provided with the email for a data protection office or officer (dataprotectionSG@xiaomi.com)
--------	-----------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

B. Has a complaints process been laid out? In its entirety?

ANALYSIS:

- Only one company, Jawbone, makes explicitly clear how a legal complaint process may unfold. In all other cases customers must perform additional research to learn about filing complaints with third parties, such as arbitration bodies.
- Apple commits to helping individuals understand relevant complaint avenues.

Company	Short Response	Detailed Response
Apple	Not really	<p>The License for the Apple Watch established that it is governed by the laws of the US, and that it “shall not be governed by the United Nations Convention on Contracts for the International Sale of Goods, the application of which is expressly excluded. If you are a consumer based in the United Kingdom, this License will be governed by the laws of the jurisdiction of your residence.”</p> <p>While Apple does not assert any specific regulator to whom a user can complain to, the privacy policy does note that all privacy-related communications to the company, “are examined and replies issued where appropriate as soon as possible. If you are unsatisfied with the reply received, you may refer your complaint to the relevant regulator in your jurisdiction. If you ask us, we will endeavor to provide you with information about relevant complaint avenues which may be applicable to your circumstances.”</p>
Basis	Sort of	The company notes that per its Safe Harbour principles, it “commits to resolve complaints about your privacy and our

		<p>collection or use of your personal information.” Where agreement cannot be reached, Basis will refer unresolved complaints to the BBB EU SAFE HARBOUR, operated by the council of Better Business Bureaus.</p> <p>There is no specific details on how a complaint would proceed, either when complaining to a company or to the BBB EU Safe Harbour group.</p>
Bellabeat	Not really	<p>ToS: States that information collected by Bellabeat might be stored “outside your home country, such as in the European Union or in the United States. There is a “questions or concerns” section in the privacy policy, but no formal complaints process.</p>
Fitbit	Sort of	<p>ToS: States that all information collected by Fitbit is governed by Privacy Policy. However, in any cases of legal action the action is to be heard in a State of California (San Francisco) court. Arbitration is required, unless opting out of this within 30 days of signing up to the service. There are no detailed explanations of the steps involved in arbitration, save that Fitbit prefers to begin with unofficial negotiation prior to formal legal processes.</p> <p>Privacy Policy: Fitbit notes that, per its Safe Harbour principles, it “commits to resolve your complaints about your privacy and our collection or use of your personal information.” Where agreement cannot be reached. Fitbit will refer unresolved complaints to BBB EU SAFE HARBOUR, operated by the Council of Better Business Bureaus. There is no specific details on how a complaint would proceed, either when complaining to a company or to the BBB EU Safe Harbour group.</p>

Garmin	Sort of	<p>TOS: when it comes to the Garmin site, users are directed to contact Garmin by letter mail, telephone, or email. Non-EU users agree that all legal issues will be taken up in a Kansas federal or district court. EU users will be governed by English law in London, England.</p> <p>Privacy Policy: There is information provided to residents of the EU; they can contact Garmin's webmaster and, if unsatisfied with the response, submit an eligible Safe Harbour mediation claim to JAMS International to be mediated per the JAMS International Mediation Rules. There is no mention of procedures non-EU users can use.</p>
Jawbone	Yes	<p>Terms of Use: Section 17 outlines the arbitration process, at length, over 14 subsections. It walks a person through the arbitration process in detail.</p> <p>Privacy Policy: There is no information about the complaints process in the Privacy Policy.</p>
Mio	No	<p>The terms of service include a 'Disclaimer of Warranties and Limitation of Liability,' and concludes with: CERTAIN STATE'S OR COUNTRY'S LAWS DO NOT ALLOW LIMITATIONS ON IMPLIED WARRANTIES OR THE EXCLUSION OR LIMITATION OF CERTAIN DAMAGES. IF THESE LAWS APPLY TO YOU, SOME OR ALL OF THE ABOVE DISCLAIMERS, EXCLUSIONS, OR LIMITATIONS MAY NOT APPLY TO YOU, AND YOU MIGHT HAVE ADDITIONAL RIGHTS."</p> <p>This is the closest the company gets to noting that complaints might be possible. No mention is made to jurisdiction or arbitration.</p>
Withings	Sort of	<p>The company notes in its Applications Terms of Use that arbitration is what will be used to resolve all complaints</p>

		(outside of those that can be asserted in a small claims court). The Judicial Arbitration and Mediations Services, Inc. (JAMS) will be the arbiters and all arbitration will be on an individual (as opposed to group, or class action) basis. There is no indication about what, specifically, arbitration will entail.
Xiaomi	No	While there is a note that complaints should be resolved amicably, there is no specifics about appealing to the Singapore legal system.

C. Does the company state in either its privacy policy or terms of service who you can escalate complaints to (i.e. regulator)?

ANALYSIS:

- Most significant item, here, is Apple's willingness to help to identify how to lodge a complaint.

Company	Short Response	Detailed Response
Apple	Sort of	While Apple does not assert any specific regulator to whom a user can complain to, the privacy policy does note that all privacy-related communications to the company, "are examined and replies issued where appropriate as soon as possible. If you are unsatisfied with the reply received, you may refer your complaint to the relevant regulator in your jurisdiction. If you ask us, we will endeavor to provide you with information about relevant complaint avenues which may be applicable to your circumstances."
Basis	Sort of	Where a complaint is not resolved between the individual and company, Basis commits to referring/recommending individuals go to BBB EU Safe Harbour and lodge complaints there.
Bellabeat	No	--

Fitbit	Sort of	<p>ToS: When a complaint cannot be addressed informally it proceeds to arbitration. If arbitration is unsuccessful legal challenges shall happen in a judicial process in the state or federal court in San Francisco. Jury trials are waived by all parties.</p> <p>Privacy Policy: Where a complaint under EU safe Harbour is not resolved, the company commits to referring/recommending individuals to go to BBB EU Safe Harbour and lodge complaints there.</p>
Garmin	Sort of	<p>ToS: Complains about the Site can be sent to the Webmaster. Anything that needs legal remediation occurs in Kansas State courts. For EU-users, they can appeal to English courts in London, England.</p> <p>Privacy Policy: There is no specific appeals process for individuals, save to contact the Webmaster. EU users can contact Garmin's webmaster and, if unsatisfied with the response, submit an eligible Safe Harbour mediation claim to JAMS International to be mediated per the JAMS International Mediation Rules.</p>
Jawbone	Sort of	<p>Terms of Use: Arbitration will be conducted by the American Arbitration Association under its rules; for international (i.e. non-US) customers arbitration is conducted by the American Arbitration Association in San Francisco, California, "under its rules for international arbitration, and you and we agree to submit to the personal jurisdiction of the U.S. Federal Court in San Francisco, California in order to compel arbitration, to stay proceedings pending arbitration, or to confirm, modify, vacate or enter judgment on the award entered by the arbiter."</p>
Mio	No	--

Withings	Sort of	Applications Terms of Use: Arbitration will be conducted by the Judicial Arbitration and Mediation Services, Inc. (JAMS). There is nothing that specifically suggests <i>how</i> a complaint will be lodged with JAMS.
Xiaomi	No	--

D. Is there a statute which limits access to data? Does access correlate with time of period after which an application was deleted? A user's account deleted?

ANALYSIS:

- In several cases companies have 'outs' under which they can retain data indefinitely, even after account deletion. It is not clear whether a subscriber/user could make a request after they have formally deleted their account.

Company	Short Response	Detailed Response
Apple	No	Apple states that "[a]ccess, correction, or deletion requests can be made through the regional Privacy Contact Form." Barring this, no mention is made about access to, or deletion of, one's data that is held by Apple.
Basis	No	There is no discussion in the Privacy Policy about how long data is retained, during use of the service or after a user leaves the service. To have data deleted, individuals are told to contact support@mybasis.com.
Bellabeat	No	There is no mention in the Privacy Policy about how long data is retained, during use of the service or after the user leaves the service. Individuals are told to delete data through the application or by contacting the company.
Fitbit	Sort of.	Fitbit commits to retaining PII as long as the user maintains an account. Identifiable information will be deleted

		<p>when deactivating an account, which requires contacting support. Removed data will include: email, name, photos, friends lists, links to sites like Facebook and Twitter.</p>
Garmin	Sort Of.	<p>Garmin states they will store data for as long as “necessary to fulfill the purposes outlined in this Privacy Statement unless a longer retention period is required or permitted by law.” (emphasis mine). Later in the policy, the company notes that even when requesting data be deleted that Garmin will respond to requests consistent “with applicable law” (i.e. EU or Kansas State/US, depending on the user). Moreover, Garmin may decline to process requests “that jeopardize the privacy of others, are extremely impractical, or would cause us to take any action that is not permissible under applicable laws.” Data may also be retained for “recordkeeping” purposes and “residual information” may remain in Garmin’s “databases and other records, which will not be removed.”</p>
Jawbone	Sort of	<p>The company notes that users can delete particular data items by opening the ‘help’ menu in the UP app. There is no place to delete specific data in that area of the iOS application, however. Users can also delete data on the band from the app, or go to a web interface to “request the deletion of your individual user data from our system.” Individuals can also contact support@jawbone.com to have their data deleted, as well as “the deletion of your individual user data from any third party apps that may be connected to up.”</p> <p>Data can be downloaded as a CSV file, though there is no indication how long after requesting a deletion that data can be downloaded.</p>

		Some data will have been “aggregated into anonymized system usage statistics” and remain on Jawbones servers and systems after a data deletion request has been processed.
Mio	No	--
Withings	Sort of	The company notes that it retains data indefinitely, or until you delete your account in Section 7 of the Privacy Policy. While the company notes that you have a right to access and export your data it is unclear how all encompassing this right is or how, specifically, an individual would exercise this right.
Xiaomi	Sort of	<p>The company notes that once it obtains “sufficient information to accommodate your request for access or correction of your personal data, we shall process in accordance with the laws of your country. While we try our utmost in acceding to your requests, unreasonably repetitive or unrealistic requests or those that put others’ privacy at risk may be declined.” Moreover, a “reasonable fee” may be imposed in some cases.</p> <p>If the User Agreement is terminated, the Xiaomi may “delete your User Content from our active database. We do not have any obligation to you as a result of terminating the Agreement in relation to your Mi Account or your User Content.”</p> <p>No mention is made, at any point, of how long or if data is retained after it is deleted following a request to their data protection email address.</p>

III. Capture of Personally Identifiable Information

- A. Does the company define ‘personally identifiable information? Does it capture all fitness data collected?

ANALYSIS:

- Only one company, Xiaomi, explicitly identifies fitness tracker data as PII; some may have definitions of PII that ultimately include fitness tracker data, but it is generally unclear from reading their privacy policies. In turning to the next question we see many companies do **not** identify fitness data as PII.

Company	Short Response	Detailed Response
Apple	Yes // No	<p>Apple does not include fitness data as a kind of personal information that the company collects*. It defines personal information as: name, mailing address, phone number, email address, contact preferences, credit card information, government ID-related information which is sometimes collected “when setting up a wireless account and activating your device, for the purpose of extending commercial credit, managing reservations, or as required by law.”</p> <p>*NOTE: Apple fitness data is stored in encrypted manners on Apple’s servers, such that they do not have access to it. As such there remains a question whether this storage of encrypted data -- which Apple itself cannot access -- constitutes the collection of personal OR non-personal information.</p>
Basis	Only implicitly	<p>Automatically collected information does not seem to constitute PII for basis whereas “Information you give us” does. The company asserts it does not link a specific name to fitness data - it is unclear whether the company regards such information as ‘PII’.</p>
Bellabeat	Only implicitly	<p>The company defines PII as “information that relates to an identified or identifiable natural person” and sensitive PII means “personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union</p>

		membership, and the processing of data concerning health or sex life.” It excludes fitness-related information from ‘sensitive’ information. Fitness information is PII to the extent the company maintains the information related to an identified or identifiable person.
Fitbit	Largely implicitly	PII is “data that includes a personal identifier like your name, email or address, or data that could reasonably be linked back to you.”
Garmin	Yes they do. Fitness not PII	PII is “information that identifies a particular individual.” Information includes: account creation, registration, purchase information, newsletter signup information, promotional-related information, when contacting support personnel, name, mailing address, phone number, email address, and payment card information.
Jawbone	No	--
Mio	Yes // Potentially implicitly	The privacy policy, though focused on data collected via the company’s website, does note that: “Personally identifiable information that we may collect ... may include your IP address, full user name, password, email address, city, time zone, telephone number, and other information that you decide to provide us with, or that you decide to include in your profile.” IF “other information that you decide to provide us with” includes fitness tracker data then steps etc are noted as PII by the company.
Withings	No // perhaps	Privacy Policy: Withings does not explicitly define ‘personal data’ in its privacy policy. It does, however, denote a series of different kinds of data that are collected or disclosed in the course of engaging with Withings products and

		<p>services: identity data, body metrics data, activity data, environmental data, and cookies -- technical features.</p> <p>These terms are not specifically identified but, instead, associated with different kinds of activities. Thus users can develop an (incomplete) understanding of how the terms capture different categories of data collection and use.</p> <p>Applications Terms of Use: in section 9, Data Protection, Withings asserts that personal data constitutes “any information relating to an identified or identifiable natural person. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.” At no point are examples or more details of how this statement is associated with Withings’ actual operations made clear to the reader.</p>
Xiaomi	Yes // Mostly	<p>Personal information includes: email address or mobile phone number, device information (e.g. IMEI), location related information (e.g. location area code, mobile network and country code); name, delivery address, order details (when purchasing product), order number, invoice date, list of purchased items and contact details (when making service request); age, height, weight, gender, “data relating to your activities, such as those obtained from our sensors and features on Mi Band and your sleeping patterns,” and “[w]hen you share content or send information to family and friends, we may collect personal information of those people, such as their names, email addresses,</p>

		<p>telephone numbers, and mailing addresses (if we need to send a product to them).</p> <p>However, some of this information is *also* considered 'non-personal data' when collected via other means. When creating a Mi Account they collect language preferences, postal code, area code number, and time zone, and profession; the area code number is previously noted -- for when creating a Mi Account -- as personal information. If opting in to their user experience improvement program, then use of website, products, and services does not constitute collection of personal information. When using services or functions based on location information then the collection of that geographic information is not personal information. When tracked by cookies, the collected cookie-data is not personal information. Internet browser log information (e.g. IP address, browser type, language, reference source, operating system, data/time/click data) is not personal. The Mi Band's unique ID code and approximate geographical location (when it is first used/activated) is not personal information.</p>
--	--	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

B. What is personally identifiable information versus non-personally identifiable information? Does the company differentiate between these categories?

ANALYSIS:

- Several companies do not identify location information as PII; the same is true for fitness-related data. Troublingly, in many cases it is not fully clear how a company specifically distinguishes between PII and non-PII, to the effect of preventing users from understanding companies' data handling practices.

Company	Short Response	Detailed Response
---------	----------------	-------------------

Apple	It does differentiate	<p>PII*: name, mailing address, phone number, email address, contact preferences, credit card information, government ID-related information which is sometimes collected “when setting up a wireless account and activating your device, for the purpose of extending commercial credit, managing reservations, or as required by law.”</p> <p>Non-PII: occupation, language, zip code, area code, unique device identifier, referred URL, location, and time where an Apple product is used; aggregated information concerning how individuals use Apple services (e.g. iCloud and iTunes and other products); collect and store details of search queries (“Except in limited instances to ensure quality of our services over the Internet, such information will not be associated with your IP address”); with consent may collect data about how individuals use their devices and applications to help app developers improve their apps; cookie-based information (e.g. IP address information) is not considered personal information unless otherwise identified under local law.</p> <p>*NOTE: Apple fitness data is stored in encrypted manners on Apple’s servers, such that they do not have access to it. As such there remains a question whether this storage of encrypted data -- which Apple itself cannot access -- constitutes the collection of personal OR non-personal information.</p>
Basis	Per III, A, the company only implicitly differentiates between PII and non-PII	<p>PII: name, e-mail address, date of birth, age, weight, height, activity level, purchase information.</p> <p>Non-PII: IP address, type of browser used to access website; access times, pages viewed, page visited before navigating the website. Computer and mobile device used to access services (including hardware model, OS and version, unique device IDs, and mobile network information). Cookies, data from tracking pixels/beacons.</p>

		<p>Unclear (“From Your Device, Storage of Information”): information about your activity and body’s response, including time, heart rate, skin temperature, ambient temperature, galvanic skin response, accelerometer data.</p>
Bellabeat	Unclear	<p>The company differentiates between PII and sensitive PII, but it is unclear the extent to which some of the data collected, such as IP address information, or UDID, is sufficiently linked to an identifiable person that it constitutes PII for the company.</p>
Fitbit	Sort of.	<p>PII: generally is information that has an identifier. Examples include name, email or address.</p> <p>Non-PII: that which is ‘de-identified’.</p> <p>Unclear: Fitbit lists a range of other types of data the company collects, noted in the following, none of which is explicitly classified as either PII or non-PII. Data items include: height, weight, gender, date of birth, information collected when signing in with either Facebook or Google identity services, food logs, alarms, personalized profiles, messages on fitbit forums, IP addresses, cookies, log data pertaining to syncing between a device and the Fitbit cloud service (e.g. IP address, time of sync, etc), shipping address information, location information (e.g. GPS, device sensor information, Wi-Fi access points recorded, cell tower IDs), steps, sleep quality information.</p>
Garmin	Yes	<p>PII: name, mailing address, phone number, email address, payment card information.</p> <p>Non-PII: location information, ad event information, activity data (e.g. steps, location, distance, pace, activity time, calories burned, etc.), server log information (e.g. IP address, browser type, browser language, data/time of</p>

		request, time(s) of visit(s) to websites, cookie-related and collected information, application usage data (e.g. time/data application accesses Garmin services, information and files downloaded by the app based on device number, analytics information about use of mobile apps, including device state information, device hardware and OS information, information about application functions, physical location of device when application crashes).
Jawbone	Does not differentiate	<p>Information collected includes: information provided upon downloading/configuring application (name, email address, postal address, account name, password, photo, gender, height, weight, date of birth), address book and Facebook contacts (uploaded to Server, no indication information is subsequently deleted), data inputted to app (including: what eat and drink, mood, 'other activities'). When use/sync Device it transmits "activity and physical information to us including, but not limited to, detailed physical information based on monitoring your micro movements, including when you are asleep, when you are awake, when you are idle, and your activity intensity and duration. Some Jawbone deices also capture heart rate and other biometric data. This data is translated into information such as your sleep patterns, calories you burn, activities undertaken and your trends and progress. This data can also provide information on certain conditions you may have. Your Device may store up to nine months of data at a time. Your device and UP app may also transmit precise location data." (emphasis not in original).</p> <p>Apps themselves may transmit: device type, manufacturer, model, operating system, device ID, version of app.</p>

		Jawbone may combine data received through the IP Service with “information we receive about you from other sources, for example , via our websites, requests you may send us, or promotional campaigns.” (emphasis not in original).
Mio	Unclear differentiation	<p>PII is: name, email address, mailing address, credit card number and expiration date, IP address, full user name, password, city, time zone, telephone number, “and other information that you decide to provide us with, or that you decide to include in your public profile.”</p> <p>It is unclear whether other data collected -- such as in log data which captures “IP address, browser type or the domain from which you are visiting, the websites you visit, the search terms you use, and any advertisements which you click” are necessarily PII, though the company notes that it can link IP addresses with other personally identifiable data “in case of violation of the Terms of Service.”</p>
Withings	Unclear Differentiation.	<p>The Privacy Policy itself does not differentiate between identifiable and non-identifiable information, save when noting that the company may “produce statistics and analyses using collected data. They would first be anonymized beforehand to assure your privacy to be protected.”</p> <p>The Applications Terms of Use provides somewhat more information concerning what is, presumably, personally identifiable data. Namely, it is: “any information relating to an identified or identifiable natural person. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an</p>

		<p>identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.” Based on this definition, anything that does <i>not</i> identify an individual would not constitute PII. It is unclear how to square the company’s definition of PII with its actual service and product offerings.</p>
Xiaomi	Does differentiate	<p>PII: when creating/logging into Mi account (email address, mobile phone number, device related information (IMEI), location related information like area code, mobile network, and country code), buying products (Mi Account ID, name, phone number, delivery address, order details), for service (order number, invoice date, list of purchased items, contact details); Activating Mi Band (age, height, weight, gender); syncing Mi Band (“data relating to your activities, such as obtained from our sensors and features on the Mi band and your sleeping patterns); Sharing content (when sharing information with other people, collect those persons’ names, email addresses, telephone numbers, and mailing addresses)</p> <p>Non-PII: language preference, postal code, area code number, time zone in which you use service, profession, statistics collected as part of user experience improvement program (e.g. use of official website, productions functions, services, information from mobile device for diagnostic purposes), location information (e.g. for weather, advertising, map-based information), cookies and “other technical elements” (as part of: website, online services, interactive applications, email messages, advertising), from web browser (e.g. IP address, browser type, language, reference source, Operating system, date, time, click rate), “[w]hen you first use and active your Mi band, the</p>

		device's unique identification code and approximate geographical information may be collected."
--	--	--------------------------------------------------------------------------------------------------------

C. Does the company distinguish between sensitive and nonsensitive information?

Company	Short Response	Detailed Response
Apple	No	--
Basis	No	--
Bellabeat	Yes	Personal Data: information that relates to an identified or identifiable person. Sensitive Personal Data: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.
Fitbit	No	--
Garmin	No	--
Jawbone	No	--
Mio	No	--
Withings	No	--
Xiaomi	No	--

D. Does the company distinguish between capturing child versus adult persons' data?

ANALYSIS:

- the majority of companies distinguish between collecting data from minors/adults; some automatically delete such information when identifying age, others all a parent/guardian to authorize children's' use of device and associated applications

Company	Short Response	Detailed Response
----------------	-----------------------	--------------------------

Apple	Yes	“Accordingly, we do not knowingly collect, use or disclose personal information from children under 13, or equivalent minimum age in the relevant jurisdiction, without verifiable parental consent. If we learn that we have collected the personal information of a child under 13, or equivalent minimum age depending on jurisdiction, without first receiving verifiable parental consent we will take steps to delete the information as soon as possible...If at any time a parent needs to access, correct, or delete data associated with their Family Sharing account or child’s Apple ID, they may contact us through our Privacy Contact Form .”
Basis	Yes.	Users must be 18 years old to use the basis service. “If we learn that we have collected children’s personal information without parental consent, we will delete it from our systems.”
Bellabeat	Yes	You must be at least eighteen (18) years of age to register to and use the Service. This Service is not directed to children under 13. We do not intend to collect personal data from children under 13.
Fitbit	Yes.	Fitbit is “not directed” at those under age 13. They ask to be notified if an under-13 users is identified. There is no clarity concerning what will then happen to alleged under-13 accounts.
Garmin	Yes.	Garmin’s products and applications “are not directed” to those under age 13. Garmin asks those under 13 to not provide PII of any type to Garmin. If the company learns it has youth’s data, it commits to deleting information about such users “as soon as possible.”
Jawbone	No	--
Mio	No	--
Withings	Yes	Individuals must be over the age of thirteen to use Withings’ products. Note

		<p>that the company asserts that “minors” must have had their parents/guardians contact the company to notify the company that the minor can use the device/service.</p> <p>If Withings is alerted that they have collected data about individuals under the age of thirteen then in the course of providing products or services, without parental consent, then the company will delete the data permanently from its servers as soon as informed of such.</p>
Xiaomi	Yes	<p>The company considers it up to children’s parents to determine if the children can use the device. The company does not actively seek information pertaining to minors (age left undefined). If parents/guardians believe that minors have contributed data without parental consent, those parents/guardians are invited to contact the company so the minors’ data can be removed and unsubscribed from the Xiaomi services.</p>

E. Can adults consent to a child’s signup? Are there any special procedures?

ANALYSIS:

- 4/9 of companies permit parents/guardians to consent to minors’ user of fitness trackers and associated applications

Company	Short Response	Detailed Response
Apple	Yes	<p>“Children under the age of 13, or equivalent minimum age in the relevant jurisdiction, are not permitted to create their own Apple IDs, unless their parent provided consent through the Apple ID for Students Program or as part of the child account creation process in Family Sharing. For example, a parent must review the Apple ID and Family Sharing</p>

		Disclosure and agree to the Consent to Apple's Collection, Use and Disclosure of Your Child's Information ; and the iTunes Store Terms and Conditions , before they can begin the Apple ID account creation process for their child. Learn more about Family Sharing , the Apple ID for Students program and Restrictions for children's accounts."
Basis	Seemingly	While users must be 18 years old to use the service, the company will (seemingly) not delete information of minors if they learn that parents have consented to their children using/send data to basis services.
Bellabeat	No	There is no mention of parental consent authorizing under 18 or under 13 users.
Fitbit	No.	There is no mention of parental consent authorizing under-13 users.
Garmin	No	There is no mention of parental consent authorizing under-13 users.
Jawbone	N/A	--
Mio	N/A	--
Withings	Yes	Parents of minors can consent to their use of the products or services, and must email the customer service department in order to authorize the product/service's delivery to the minor.
Xiaomi	Yes // No	--

IV. Disclosure of Information

- A. Are there specific or general identifications of organizations to whom data is shared? Is explicit (e.g. "will") or possible (e.g. "may") language used?

Company	Short Response	Detailed Response
Apple	No	THIS ANSWER APPLIES JUST TO FITNESS/HEALTH

		<p>Apple asserts that “Apps that work with Health are prohibited by our developer guidelines from using or disclosing Health data to third parties for advertising or other use-based data mining purposes other than improving health or for the purpose of health research. We also require apps that work with Health to provide a privacy policy that’s available for you to review. Your data in the Health app and your Health data on Apple Watch are encrypted with keys protected by your passcode. Your Health data only leaves or is received by your iPhone or Apple Watch when you choose to sync, back up your data, or grant access to a third-party app. Any Health data backed up to iCloud is encrypted both in transit and on our servers.”</p>
Basis	No specific organizations. Explicit and possible language, both.	<p>No specific other companies are noted in the sharing of information. Definitive statements exist for NOT sharing personal information for promotional practices, and WILL share information for business practices (e.g. processing payments). MAY share information with authorities under court order, as required by law, or to protect the company’s (or another’s) rights, property, or safety. Aggregated and deidentified information MAY be shared or sold to third parties; research/marketing noted as rationales, but they are non-exclusive.</p>
Bellabeat	No specific organizations. Explicit and implicit language	<p>The company MAY disclose personal data with service providers (payment processors, storage companies), to public authorities (i.e. law enforcement), or to subsidiaries/affiliates/subsequent owner of business/partners. Automatically collected data MAY also be disclosed to: service providers (e.g. data analysis companies), public authorities, or</p>

		subsidiaries/affiliates/subsequent owner/partners.
Fitbit	Yes	<p>Fitbit is explicit about the advertising and analytics companies that it uses. However, Fitbit does not identify to whom fitness data may be shared, though does recognize that the company WILL disclose information if required to under government obligation or to protect Fitbit, its employees, or its service. In such cases, Fitbit will try to notify the end user. Data MAY also be disclosed in the case of a sale of the company or bankruptcy. The company MAY sell or share aggregated and deidentified data to partners and the public.</p> <p>Analytics/advertising partners include: AppNexus, DataXu, DoubleClick and DoubleClick Flashlight; Google Adwords Conversion; AdRoll; Twitter Advertising; LiveRamp; Advertising.com; Bidswatch; Facebook Custom audiences; Genome; SearchForce; Mixpanel, Google Analytics; New Relic; KissInsights; Optimizely.</p>
Garmin	General identifications	<p>Garmin MAY share with affiliates; it suggests users find/read its 10-K form, filed to the SEC (I was unable to find this, at the link provided). It MAY use third parties to operate their business; while payment providers are given as an example, the language is expansive such that ANY business practice could be outsourced. The company MAY provide information to others with user consent or as required under applicable law. It MAY transfer or information to affiliates, subsidiaries, or third parties in the event of reorganizations, mergers, sales, joint ventures, assignment, transfer, or other disposition of "Garmin's business, assets, or stock" such in connection with bankruptcy or other proceeding.</p>

Jawbone		<p>Terms of Use: No discussion Privacy Policy: With consent, data is shared with third party app/service. Jawbone USES third parties to deliver services and run business (subject to confidentiality agreements). They SHARE aggregated statistics. They MAY SHARE personal information for business deals, such as the sale/transfer of business assets. They MAY DISCLOSE personal information to comply with law, protect and defend their rights and property, in emergencies to protect any person, or in connection with investigating/preventing fraud.</p>
Mio	Yes	<p>The company SHARES information with other parties for some purposes, including: fulfilling orders, offering products and services in connection with website, communicating with customer, completing credit card transactions, enabling access to partners' sites, improving shopping experience. The company reserves "the right to sell, transfer or otherwise share some or all" of customers' PII in connection with corporate transactions (e.g. bankruptcy). Information is SHARED with third-parties who provide hosting and maintenance, customer relationship, database storage and management, and direct marketing for the company. Also, information MAY be disclosed to government, law enforcement officials, or private parties to enforce and comply with the law. The company MAY disclose information in the case of emergency situations or as necessary to "identify, contact or bring legal action against someone who may be causing injury or interference with (either intentionally or unintentionally) our rights or property, other Physical Enterprises, Inc. website users, or anyone else that could be harmed by such activities."</p>

Withings	Nonspecific statement	<p>Privacy policy: "Some services require the involvement of other companies. This is the case for example for online payments on our www.withings.com website. In order for this service to work, we have to transmit certain data to our partners that allows you to be identified and process to a secured payment."</p> <p>Moreover, data are shared when compelled by "[c]ertain laws, administrative or court rulings." Withings commits to informing their users of such disclosures "as soon as possible."</p>
Xiaomi	Yes	<p>Company uses 'may' to indicate a non-extensive listing of to whom data may be shared with. In all cases, the company notes the sorts of organizations with whom information is shared as opposed to be specific organizations with whom it is shared.</p> <p>Data may be shared with other Xiaomi group companies, and only for providing or improving products as opposed to for marketing purposes. Data may be shared with others parties because of applicable laws and/or regulations, because of "an emergency that threatens the life, health, or safety of the individual or another individual", to prevent crimes or due to legal proceedings, in "cases in which the purpose of the disclosure is clearly in the individual's interests, and if consent cannot be obtained in a timely way", because of "any investigation or proceedings", where served with a production order from LEAs where the order certifies "that the personal data is necessary for the purposes of the functions or duties of the officer", and where "disclosure is to a public agency and such disclosure is necessary in the public interest."</p>

- B. Does the company use the term “selling” or “sharing” or some equivalent language in discussing the disclosure of personal information?

ANALYSIS:

- In most cases, companies may sell data in the case of a bankruptcy. Apple, Withings, and Xiaomi seem to be the exceptions

Company	Short Response	Detailed Response
Apple	Yes* * does not seem to apply to Apple Watch or Health or Tracking	Apple may share some information with wireless carriers for the purposes of setting up a device (i.e. iPhone). There is no actual mention of selling OR sharing Health or Fitness related information, though there is a note that individuals can grant access to Health data to third-parties.
Basis	Yes	In relation to: the sale of the business and its assets to another company, as well as in cases of sharing de-identified and aggregated information (e.g. for marketing or researcher).
Bellabeat	Yes	The company notes that data could be sold, leased or otherwise disclosed to “our subsidiaries and affiliates; or a subsequent owner, co-owner or operator of the Service and their advisors in connection with a corporate merger, consolidation, restructuring, or the sale of substantially all of our stock and/or assets or other corporate reorganization, in accordance with this Privacy Policy.” This holds for both information that is manually inputted as well as automatically collected data.
Fitbit	Yes	In relation to: the sale of the business and its assets to another company, as well as in cases of sharing de-identified and aggregated information.
Garmin	Yes.	Garmin may share data with affiliated entities or third parties, more generally,

		to help operate Garmin's business, websites, or administer activities on Garmin's behalf. Data may also be transferred in the case of events such as bankruptcies or related proceedings.
Jawbone	Yes	In relation to: sharing aggregated statistics or sharing information for purposes of a business deal.
Mio	Yes	In relation to: sharing information "with our agents, representatives and trusted service providers and contractors"; in "statistical or aggregated non-personal information about our users with advertisers, business partners, sponsors and other select third parties, or in the case of bankruptcy or other corporate transaction.
Withings	Not really	The company uses the term 'share' a lot in the privacy policy but in almost all cases its a reference to users being able to choose to share information. There is no discussion of what the company will do with data in the case of bankruptcy or other equivalent event.
Xiaomi	No	--

- C. Does the organization discuss the potential sharing of information with state authorities? Is there sufficient information about such sharing to let individuals understand a company's procedures (e.g. as demonstrated through a LEA guide)?

Company	Short Response	Detailed Response
Apple	Yes // Yes	Apple asserts that "It may be necessary – by law, legal process, litigation, and/or requests from public and governmental authorities within or outside your country of residence – for Apple to disclose your personal information. We may also disclose information about you if we determine that for purposes of national security, law enforcement, or other issues of public importance, disclosure is necessary or

		appropriate.” The company published transparency reports at http://www.apple.com/privacy/government-information-requests/ and includes guidelines for LEA requests for US, EMEA, and Japan and APAC nations.
Basis	Yes // No	There is a note that information may be shared in response to court order or applicable law. There is not clarity what courts/authorities/processes would be adhered to.
Bellabeat	Yes // No	The company acknowledges that it might disclose information to public authorities as the company is “legally required to do so or if we need to protect our rights or the rights of third parties.” It is not clear what courts/authorities/processes would be adhered to.
Fitbit	Yes // No	The company states that they may share information if Fitbit believes “disclosure is reasonably necessary to comply with a law, regulation, valid legal process (e.g., subpoenas or warrants served on us), or governmental or regulatory request, to enforce or apply the Terms of Service or Terms of Sale, to protect the security or integrity of the Fitbit Service, and/or to protect the rights, property, or safety of fitbit, its employees, users, or others. If we are going to release your data, we will do our best to provide you with notice in advance by email, unless we are prohibited by law from doing so.”
Garmin	Yes // No	Garmin states it may disclose users’ information to others as it believes is necessary or appropriate: “(a) under applicable law or regulation, including laws or regulations outside your country of residence; (b) to comply with legal process; (c) to respond to requests from public authorities and law enforcement officials, including officials outside your country of residence; (d) to assist or

		support theft investigations involving Garmin products or property; (e) to enforce any of our terms and conditions or policies; (f) to protect our operations or those of any of our affiliates and subsidiaries; (g) to protect the rights, privacy, safety or property of Garmin, its affiliates and subsidiaries, you, or others; or (h) to permit us to pursue available remedies or limit the damages we may sustain.
Jawbone	Yes // No	Jawbone states it may disclose users' personal information to "comply with relevant laws, regulatory requirements and to respond to lawful requests, court orders, and legal process" or in "an emergency" or "in connection with investigating and preventing fraud." It is not clear what specific processes are in place to evaluate claims, appeals process, or notification to users.
Mio	Yes // No	The company cooperates "with government and law enforcement officials or private parties to enforce and comply with law. We may disclose any information about you to government or law enforcement officials or private parties as we, in our sole discretion, believe necessary or appropriate to respond to claims, legal process (including subpoenas), to protect the property and rights of Company or a third party, the safety of the public, or any person, to prevent or stop any illegal, unethical, or legally actionable activity, or to comply with the law."
Withings	Yes // No	The company simply states that, "[c]ertain laws, regulations, administrative or court rulings may compel us to communicate certain personal data to a third party. Apart from where this is prohibited, we shall inform you as soon as possible if we have to transmit some of your data." There is no

		note about the specific processes or procedures that authorities must go through in order for Withings to process a request.
Xiaomi	Yes // No	<p>The company's privacy policy notes the following terms of sharing information with authorities: "in which the disclosure is required or authorized based on the applicable laws and/or regulations"; "in which the disclosure is necessary for the prevention of crime or legal proceedings"; "in which the disclosure is necessary for any investigation or proceedings"; "in which the disclosure is to any officer of a prescribed law enforcement agency upon production of written authorisation signed by the head or director of the law enforcement agency, or a person of similar rank, certifying that the personal data is necessary for the purpose of the functions or duties of the officer"; "in which the disclosure is to a public agency and such disclosure is necessary in the public interest."</p> <p>Many of these terms are undefined, and it remains unclear what jurisdictions or terms or analysis Xiaomi includes as part of the disclosure process. There is not linked LEA guidelines report.</p>

D. Are there specific notes concerning sharing information with insurance companies?

ANALYSIS:

- This is helpful, regardless of the limited answers provided

Company	Short Response	Detailed Response
Apple	No	--
Basis	No	--

Bellabeat	No	--
Fitbit	No.	--
Garmin	No.	--
Jawbone	No	--
Mio	No	--
Withings	No	--
Xiaomi	No	--

E. Are there guarantees of data confidentiality in the case of bankruptcy or sale of the company?

ANALYSIS:

- All companies that acknowledge possibility of bankruptcy (5/9) state may sell data

Company	Short Response	Detailed Response
Apple	No* * not mentioned at all	Bankruptcy not mentioned in the documents analyzed.
Basis	No	Data may be sold in bankruptcy or sale of company scenarios. Users would be notified of the sale/transfer.
Bellabeat	No	Though bankruptcy not explicitly mentioned, the company does acknowledge that data collected manually and automatically might be sold or otherwise disclosed to a "subsequent owner, co-owner or operator of the Service and their advisors in connection with a corporate merger, consolidation, restructuring, or the sale of substantially all of our stock and/or assets or other corporate reorganization."
Fitbit	No	Data may be sold in connection with the sale, merger, bankruptcy, or sale of

		assets or reorganization of the company. Users would be notified if PII would be transferred to another company. Any transferred PII would remain subject to Fitbit's existing Privacy Policy.
Garmin	No.	Data may be transferred in the event of events linked with bankruptcy or similar events.
Jawbone	No	Data may be shared for the purposes of a business deal (or negotiation of a business deal); such a deal may include: a merger, financing, acquisition, or bankruptcy transaction or proceeding.
Mio	No	The company may transfer, share, or sell data for the purposes of a business deal. Such a deal may include: future merger, acquisition, reorganization or sale of assets or in the event of bankruptcy.
Withings	No* * not mentioned at all	Bankruptcy is not mentioned in the documents analyzed.
Xiaomi	No* * not mentioned at all	Bankruptcy is not mentioned in the documents analyzed.

V. Security of Personally Identifiable Information

A. Are commitments made about the security of user data?

ANALYSIS:

- Apple, Xiaomi, and Withings (to a point) have defined security assertions. Other companies' are much higher level statements.

Company	Short Response	Detailed Response
Apple	Yes	Apple asserts that "[y]our data in the Health app and your Health data on Apple Watch are encrypted with keys protected by your passcode. Your Health data only leaves or is received by your

		iPhone or Apple Watch when you choose to sync, back up your data, or grant access to a third-party app. Any Health data backed up to iCloud is encrypted both in transit and on our servers.”
Basis	Sort of	Non-specific assurances provided that the company has implemented “reasonable security measures” to protected data.
Bellabeat	Sort of	The company takes “reasonable measures” to protect data from unauthorized access/loss/misuse by third parties but does not offer a guarantee of either data security or data integrity. They specifically note that the company “cannot guarantee that our security measures will prevent third-parties such as so-called hackers from illegally obtaining access to personal data. We do not warrant or represent that personal data about you will be protected against, loss, misuse, or alteration by third parties.”
Fitbit	Sort of	Fitbit assures users the company “take the security of your data seriously.” A general statement concerning security is made (“a combination of technical and administrative security controls to maintain the security of your data”) along with recommendation that users contact support if they have additional questions.
Garmin	Sort of	The company “takes reasonable security measures” to protect the personal information that it controls. In the case where individuals believe their interaction with Garmin “is no longer secure” the users are asked to contact Garmin. No mention is made to securing non-personal information.
Jawbone	Sort of	The company assert it applies “organizational and technical measures

		to ensure access to your information is limited to persons with a need to know” though includes a caveat that “neither we -- nor any company -- can fully eliminate security risks.”
Mio	Kind of	The company asserts that it does not retain credit card information for customers’ “own security.” When third party service providers are used, they are required to “maintain the privacy and security of your data.”
Withings	Kind of	Withings has a pretty high-level description; note that this stands in difference to their earlier statements about where users’ data resides. Specifically, “[y]our data are mainly stored on servers located in France Where are your personal data kept equipped with the latest security equipment and advanced security techniques and procedures. Access is strictly restricted and various security controls, consisting of security staff, security doors and biometric readers, must be passed. Remote access to the servers is highly restricted and controlled.”
Xiaomi	Yes	Xiaomi has a section of their privacy policy titled, “Information Safety Safeguards”. The company asserts it stores user data “on secure servers that are protected in controlled facilities”; that data is classified on back ends according to the relative sensitivity of the data; that more sensitive data are kept in more secure rooms/areas; that data exchanged between Xiaomi devices and services are encrypted using SSL ; that there is an optional two-step verification option to access a user’s Mi account; there are regular reviews of security policies; access to data is limited to Xiaomi employees and select third-party contractors who agree to

		<p>confidentiality agreements; Xiaomi employees only have access to select data, as opposed to all of a given user's data. The company also notes that it "will take all practicable steps to safeguard your personal data. Through our protective measures above, especially encrypted storage and transmission, your data is as secure as it can be. Certain details of encrypted data cannot be accessed by anyone except you."</p> <p>(NOTE: there is no indication what data is solely accessible to the end-user.)</p>
--	--	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

B. Are there commitments made to encryption?

ANALYSIS:

- Only 2/9 make commitments to security. **Note, however, that technical analysis actually reveals the use of encryption.**

Company	Short Response	Detailed Response
Apple	Yes	"Your data in the Health app and your Health data on Apple Watch are encrypted with keys protected by your passcode. Your Health data only leaves or is received by your iPhone or Apple Watch when you choose to sync, back up your data, or grant access to a third-party app. Any Health data backed up to iCloud is encrypted both in transit and on our servers."
Basis	No	--
Bellabeat	No	--
Fitbit	No	--
Garmin	No	--
Jawbone	No	--
Mio	No	--

Withings	No	--
Xiaomi	Yes	Xiaomi notes that data between their device and cloud are encrypted with SSL. They also note that some data is solely accessible to end-users because of how encryption has been established.

C. Are there beach notice provisions?

ANALYSIS:

- None

Company	Short Response	Detailed Response
Apple	No	--
Basis	No	--
Bellabeat	No	--
Fitbit	No	--
Garmin	No	--
Jawbone	No	--
Mio	No	--
Withings	No	--
Xiaomi	No	--

VI. Access and Correction

A. Are commitments made to user-access to all collected information?

ANALYSIS:

- Xiaomi is the only company that asserts it will provide access to PII and that has an expansive definition of PII, as noted earlier.

Company	Short Response	Detailed Response
---------	----------------	-------------------

Apple	<p>Yes // Sort of*</p> <p>* data is encrypted such that Apple should not be able to correct it for user</p>	Apple does have a mechanism for contacting the company to have data corrected. However, for the specific data associated with Apple Health/Activity the data is encrypted such that Apple cannot (in theory) read, or provide it, in an unencrypted format.
Basis	Limited	Users can modify their name, address, and contact information in the application. No mention of accessing data which is collected while using the tracker or associated services.
Bellabeat	Yes	The company states that “If you would like to know what personal data we hold about you, please contact us at hi@bellabeat.com ” and that users have “[t]he right to have incomplete, incorrect, outdated, or unnecessary personal data corrected, deleted, or updated. The easiest way to correct, delete, or update the personal data you have provided to the Service is to log in to the Service and enter the necessary changes in the profile settings of the Service. If you have additional questions regarding the correction, deletion, or updating of the personal data we hold about you, please contact us at hi@bellabeat.com .”
Fitbit	Limited	Users can edit or modify data from their dashboard or account preferences. However, any information which does not appear there (e.g. wifi access points recorded, GPS data) are not explicitly discussed in the privacy policy.
Garmin	Limited	While users can request that “erroneous or inaccurate Personal Information be updated” or deleted, Garmin reserves the right to not implement requests where they would “jeopardize the privacy of others, are extremely impractical, or would cause [Garmin] to take any action that is not permissible under applicable laws.”

Jawbone	Limited	Individuals are provided with a link from which they can download their data as a CSV file; this does not include non-fitness band related data.
Mio	No	--
Withings	Limited	Withings includes, as a principle, Rights to access and amend one's own data. However, there is no specificity in how, precisely, a person should engage in requests for their information or amend their data from the privacy policy alone.
Xiaomi	Yes	The company explicitly states that users "have the right to request access and/or correction or any personal data that we hold about you...Once we obtain sufficient information to accomodate your request for access or correction of your personal data, we shall process in accordance with the laws of your country . While we try our utmost in acceding to your requests, unreasonably repetitive or unrealistic requests or those that put others' privacy at risk may be declined." The company reserves the right to charge "a reasonable fee" for requests.

B. Can users export their data? In an open standard?

ANALYSIS:

- While some companies note a right to access data, only Jawbone is explicit about providing it in an open format

Company	Short Response	Detailed Response
Apple	Unclear	<p>No commitment is made to exporting Apple Health information, nor that an exported data would conform to an open standard.</p> <p>More generally, Apple asserts that, "[f]or</p>

		other personal information we hold, we will provide you with access for any purpose including to request that we correct the data if it is inaccurate or delete the data if Apple is not required to retain it by law or for legitimate business purposes. We may decline to process requests that are frivolous/vexatious, jeopardize the privacy of others, are extremely impractical, or for which access is not otherwise required by local law. Access, correction, or deletion requests can be made through the regional Privacy Contact Form.”
Basis	No	No mention of data export in the company’s privacy policy.
Bellabeat	No	No mention of data export in the company’s privacy policy.
Fitbit	No	No mention of data export in the company’s privacy policy or Terms of Service.
Garmin	No	No mention of data export in the company’s Privacy Policy or Terms of Service.
Jawbone	Yes	Fitness data can be exported as a CSV.
Mio	No	No mention of data export in the company’s privacy policy or Terms of Service.
Withings	Sort of	While Withings does note that “[y]our personal data is and shall remain easily accessible. This means that you can always export your personal data in an open format for you to easily keep and access to them.” There is no specific information about exporting data or the formats that data can be exported to. Also, there is no indication about the full extent of information that can be provided, given Withings’ failure to define PII.

Xiaomi	Sort of	While users can request their own data, there is no indication about the data format it will be released in.
--------	---------	--------------------------------------------------------------------------------------------------------------

C. Are costs associated with the export of their data?

ANALYSIS:

- Specific costs are not stated in policies

Company	Short Response	Detailed Response
Apple	Left Unstated	Apple does not mention whether there will, or will not, be cost associated with access, deletion, or export of personal information held by the company.
Basis	N/A	No mention of data export in the company's privacy policy.
Bellabeat	N/A* * There is a right of access	* The right of access can incur some "small processing fee" if less than twelve months has followed since your last access request.
Fitbit	N/A	No mention of data export in the company's privacy policy or ToS.
Garmin	N/A	No mention of data export in the company's privacy policy or ToS.
Jawbone	No	It is freely downloaded one individuals sign into their account through Jawbone's website.
Mio	N/A	No mention of data export in the company's privacy policy or terms of service.
Withings	Unclear	No mention of cost.
Xiaomi	Sort of	The company reserves the right to charge a "reasonable fee" for user access to their own data.

D. Are procedures for accessing and correcting data present?

Company	Short Response	Detailed Response
Apple	Sort of	While Apple does have access/correction/deletion protocols, it is unclear whether or to what extent they would (or could) apply to Apple Health stored information that came from the Apple Watch.
Basis	Sort of	Name, address, and contact information can be modified in application. No mention within the privacy policy of modifying other data.
Bellabeat	Yes	“The right to have incomplete, incorrect, outdated, or unnecessary personal data corrected, deleted, or updated. The easiest way to correct, delete, or update the personal data you have provided to the Service is to log in to the Service and enter the necessary changes in the profile settings of the Service. If you have additional questions regarding the correction, deletion, or updating of the personal data we hold about you, please contact us at hi@bellabeat.com .”
Fitbit	Sort of	The privacy policy notes that users can modify some information through their online account page. However there is no mention being able to correct metadata that is collected, such as location-related data.
Garmin	Sort of	While the privacy policy notes that individuals can request to access, correct, or have deleted the information that Garmin retains there are numerous caveats to such requests. Garmin reserves the right to not implement requests where they would “jeopardize the privacy of others, are extremely impractical, or would cause [Garmin] to take any action that is not permissible under applicable laws.”

Jawbone	Sort of	Individuals can delete activities through the application but the company otherwise does not mention access/correction in the privacy policy or Terms of Use.
Mio	No	No mention in either the company's privacy policy or terms of service.
Withings	Sort of	Withings includes a "Right to amend your data" as one of the company's principles. The company states that, "[a]t any time you may amend, add to, delete or update the personal data produced by an active measurement on your part. This may be done directly in the application or on request."
Xiaomi	Yes	Users can make a request, during which they will have to verify their identify. After doing so Xiaomi will "accommodate" the request. There is no specific details about each step that must be completed, though the broad strokes are identified.