Fitness Wearable Companies

Question 1: information about how data is collected and exchanged by you with other companies or organizations. Can you clarify whether my data, either in an individualized data set or as part of an aggregate data set, has been provided to insurance agencies? And if it has been provided (either voluntarily, as part of a commercial transaction, or on other grounds) please identify to which insurance agencies it has been provided.

Company	2016
Apple	"Apple does not share personal information with insurance companies, in an aggregated form or otherwise."
Basis	"BASIS has not provided your data to insurance companies."
Bellabeat	The data collected from the LEAF (number of steps taken and sleep records) have not been provided to any 3rd parties nor will it be. Prior to any data disclosure, all users will be informed and explicitly asked for permission on sharing their data.
Fitbit	First, we do not provide your identifiable data to third parties outside of the purposes identified in our Privacy Policy, such as with our service providers, for order fulfillment, compliance with applicable laws or a legal obligation. Aggregated data, data that is deidentified and cannot be linked back to our users, is occasionally shared with our partners and the public in the form of research, reports or as part of our Premium membership. We encourage you to review our privacy policy for the full breakdown of our data uses.

Company	2016
Jawbone	We do not rent, sell or otherwise share your individual personal information with third parties, except as follows: • With your consent, for example to connect with a third party app or service. • We use affiliated and unaffiliated service providers all over the world that help us deliver our service and run our business subject to confidentiality agreements. For example, we use third party data analytics platforms to help us understand, among other things, server load and app behavior • We share aggregated usage statistics that cannot be used to identify you individually, for example through data stories on our blog (www.jawbone.com/blog) or through the media. • We may share your personal information for the purposes of a business deal (or negotiation of a business deal) involving sale or transfer of all or a part of our business or assets. These deals can include a merger, financing, acquisition, or bankruptcy transaction or proceeding. • We may disclose your personal information to (a) comply with relevant laws, regulatory requirements and to respond to lawful requests, court orders, and legal process+ (b) to protect and defend the rights or property of us or third parties, including enforcing agreements, policies, and terms of use2 (c) in an emergency, including to protect the safety of our employees or any person, or (d) in connection with investigating and preventing fraud. Many Device users want to connect with friends and colleagues. When you use your Device, the name you supply and profile image is publicly searchable in the UP directory. We use the email address you register with the UP Service and match it with information other people upload from their address books, Facebook contacts or through email address lookup. If there is a match, we share with that person that you are a Device user and allow them to invite you to connect to be part of their UP team. If you choose to be part of an UP team or add people to your UP team, you choose the UP information you wish to share with your team. Be thoughtful of your own privacy needs as you choose what you share and with whom.
Withings	I would like to underline that we do not share any personal information with any third Party without your prior and freely given consent. It is indeed essential for us to obtain your prior agreement when data which can identify you are shared. (unless when obliged by law or if such data sharing is absolutely necessary to provide you with a service you previously requested). As an example, using a partner application such as Runkeeper or any other partner application linked to our API, may require us to share your data. As a consequence, if you had not willingly share your data to an insurance agency, we would never have shared such identifiable personal data.

Company	2016
Xiaomi	[No substantive response to DAR]
Garmin	[No response to DAR]
Mio	[No response to DAR]

Question 2: I live in Canada; am I bound to engage with your company in a non-Canadian arbitration or legal environment? I am not planning on engaging in such a conflict but wanted to better understand my rights.

Company	2016
Apple	"As a Canadian resident, Apple Canada Inc is the responsible entity for any of your personal information held by Apple."
Basis	"We would endeavor to resolve any concerns, complaints, or conflicts amicably without resorting to more formal forums for dispute resolution. Where issues can and should be raised/resolved will depend on, among other things, the specific nature of the issue and the parties involved." [CHECK TOS]
Bellabeat	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	Fitbit and our users agree to a binding arbitration under California law. Please consult an attorney if you have any further questions on the effect of this provision as it pertains to your circumstances.
Jawbone	Binding arbitration with US small claims court exemption and IP exemption. 30 day opt-out period (mail or fax). American Arbitration Association rules apply.
Withings	To allow our customer to efficiently defend their rights, we generally require them to use an arbitration service. We made the choice of using Judicial Arbitration and Mediation Services, Inc. ("JAMS") pursuant to its Streamlined Arbitration Rules and Procedures then in effect as we believe that this arbitration service stands as an efficient and cost effective conflict resolution mean.
Xiaomi	[No substantive response to DAR]
Garmin	[No response to DAR]
Mio	[No response to DAR]

Question 3: What are your policies, practices, or processes for handling requests from authorities from international jurisdictions, such as from Canadian policing organizations? How would you respond if my information was requested as evidence in a Canadian court case or criminal proceeding?

Company	2016
Apple	In its response to the DAR, Apple directed the requester to consult their policy on government information requests at this URL: https://www.apple.com/privacy/government-information-requests/, regarding access to account data, the company writes it requires a search warrant for all US requests, and that international requests for US-hosted data must comply with ECPA. Apple will give prior notice to customers about such disclosures, if not prohibited by law.
Basis	Law enforcement and other third party requests for personal data related to BASIS customers are handled by our Legal Department. BASIS' policy is to comply with applicable laws and regulations in the jurisdictions in which it does business. BASIS does not have access to personal data as it travels between your BASIS watch and your mobile phone. BASIS would not be able to provide such data to third parties.
Bellabeat	"We have forwarded this questions to our legal team and we'll respond as soon as we get the answer." — no response.
Fitbit	as Fitbit is a company in the United States and all of its data is stored in the U.S., Fitbit will only respond to a valid legal process issued by a U.S. Governmental entity or court and when properly served. Governmental entities and private parties outside of the United States should domesticate requests for user data through a U.S. court or by working through an appropriate process for international cooperation, such as through letters rogatory or via a Mutual Legal Assistance Treaty.
Jawbone	We may disclose your personal information to (a) comply with relevant laws, regulatory requirements and to respond to lawful requests, court orders, and legal process+ (b) to protect and defend the rights or property of us or third parties, including enforcing agreements, policies, and terms of use2 (c) in an emergency, including to protect the safety of our employees or any person, or (d) in connection with investigating and preventing fraud.
Withings	As you may know, certain laws, regulations, administrative or court rulings may compel us to communicate some personal data to a third party. Apart from where this is prohibited, we shall inform you as soon as possible shall we have to at some point transmit part of your data.
Xiaomi	[No substantive response to DAR]
Garmin	[No response to DAR]
Mio	[No response to DAR]

Question 4: Is the personal data transmitted between my mobile phone and your web servers secured against potential eavesdroppers? What about between my fitness band and my phone?

Company	2016
Apple	Apple linked the requester to their “Approach to privacy” document, which includes a section about encryption that says “we build privacy into everything we make”, and that “we’re committed to using powerful encryption because you should know the data on your device and the information you share with others is protected.” Furthermore, Apple writes in its “Health and Fitness” section that “When your phone is locked with a passcode or Touch ID, all of your health and fitness data in the Health app is encrypted. And any Health data backed up to iCloud is encrypted both in transit and on our servers.”
Basis	BASIS uses standard industry practices to secure the communications channels between the device and phone and the phone and any servers.
Bellabeat	Personal data transmitted on the relation LEAF smartphone app web server is secured against all potential attacks.
Fitbit	Under normal conditions, traffic between a Fitbit tracker and our site is encrypted, as is traffic between a mobile device and the Fitbit site. The transmission between the tracker and the site is encrypted end-toend, meaning that the mobile device proxying this traffic is unable to read the data.
Jawbone	We apply organizational and technical measures to ensure access to your information is limited to persons with a need to know. Our mobile clients communicate with our servers over a secure protocol (HTTPS) and all band data is sent over an encrypted channel. Even though we have taken steps to protect your personal information, you should know that neither we !! nor any company !! can fully eliminate security risks.
Withings	[No response to question]
Xiaomi	[No substantive response to DAR]
Garmin	[No response to DAR]
Mio	[No response to DAR]

Question 5: Can you describe in more detail what practices you've implemented to ensure Bluetooth data transmissions are privacy-protective?

Company	2016
Apple	Apple wrote "We would also suggest that you examine our white paper about iOS security, which includes detailed information on pages 25-26 on Apple Watch pairing with an iPhone". That document described in detail the security processes in place for pairing the watch with an iPhone.
Basis	Data is only transmitted to mobile phones which have been paired to a specific BASIS device. Such pairing requires user interaction/ permission and physical control of both the BASIS device and phone to be paired.
Bellabeat	Synchronization between LEAF devices and smartphones is performed using Bluetooth Low Energy (BLTE) protocol. Synchronization between smartphones and the LEAF device occurs in an encrypted session over the Internet (WiFi or mobile network). According to the specifications for BLTE, one of the best features it has is privacy awareness, which allows our developers to frequently change the private addresses of devices in order to avoid tracking. It has been suggested that such a feature should be used actively by health monitor devices to preserve privacy of users. We change the private addresses of the LEAF devices on a weekly basis.
Fitbit	we've designed a system where tracker communications that include historic data are encrypted endtoend between a tracker and the Fitbit site under normal conditions.
Jawbone	We apply organizational and technical measures to ensure access to your information is limited to persons with a need to know. Our mobile clients communicate with our servers over a secure protocol (HTTPS) and all band data is sent over an encrypted channel. Even though we have taken steps to protect your personal information, you should know that neither we !! nor any company !! can fully eliminate security risks.
Withings	[No response to question]
Xiaomi	[No substantive response to DAR]
Garmin	[No response to DAR]
Mio	[No response to DAR]

Question 6: Geolocation data collected about me, my devices, and/or my account

Company	2016
Apple	Apple did not provide any geolocation data in its data set.
Basis	Basis does not collect location information with the exception of an optional “playground” feature you may have enabled. If this optional feature was enabled, please follow the instructions below to retrieve an encrypted file with your data.
Bellabeat	Bellabeat indicated it would provide access to data records in a subsequent response, but never followed through.
Fitbit	[None found in data set]
Jawbone	[None found in downloadable data set]
Withings	[None found in data set]
Xiaomi	[No data set provided]
Garmin	[No response to DAR]
Mio	[No response to DAR]

Question 7: Any additional kinds of information that you have collected, retained, or derived from the mobile or website services your provide, or with the fitness-related device your company produces that I use

Company	2016
Apple	Many other types of data pertaining to other services provided to the requester by Apple were provided.
Basis	Basis indicated it would provide access to data records in a subsequent response, but never followed through.
Bellabeat	Bellabeat indicated it would provide access to data records in a subsequent response, but never followed through.
Fitbit	Basic personal info (height weight dob sex)
Jawbone	[None found in downloadable data set]
Withings	Not other types of data explicitly mentioned
Xiaomi	[No substantive response to DAR]
Garmin	[No response to DAR]
Mio	[No response to DAR]

Question 8: Health and fitness data including all records of my step activity, heart rate, sleep patterns, food intake.

Company	2016
Apple	In its response, Apple linked to its “Approach on privacy”, which included a section about “Heath and Fitness” information. That section stated “When your phone is locked with a passcode or Touch ID, all of your health and fitness data in the Health app is encrypted. And any Health data backed up to iCloud is encrypted both in transit and on our servers.” Apple did not provide any encrypted data in its DAR response.
Basis	Basis indicated it would provide access to data records in a subsequent response, but never followed through.
Bellabeat	Bellabeat indicated it would provide access to data records in a subsequent response, but never followed through.
Fitbit	Step counts, aggregated by day; sleep measurements by day (Minutes after wakeup Minutes asleep Minutes in sleep period Minutes to fall asleep Start time End time Woken up times), manual weight measurements, active minutes by day
Jawbone	Age, BMR, body fat, nutrient intake, calories burned, mealtimes, gender boolean, height, weight, fitness goals, steps, mood, sleep patterns, all by date
Withings	steps, distance, elevation, active calories by date. blood pressure by date, height weight, oxymetry, by date
Xiaomi	[No substantive response to DAR]
Garmin	[No response to DAR]
Mio	[No response to DAR]

Question 9: Mobile app data Information collected about me, or persons/ devices associated with my account, using one of your company's mobile device applications

Company	2016
Apple	Apple's provided data included a wide amount of data related to other Apple products and services — such as iTunes downloads, but nothing explicitly tied to fitness records was found.
Basis	Basis indicated it would provide access to data records in a subsequent response, but never followed through.
Bellabeat	Bellabeat indicated it would provide access to data records in a subsequent response, but never followed through.
Fitbit	All data in the data dump pertained specifically to fitness tracking or IP address logs
Jawbone	Data provided by Jawbone's export tool pertained exclusively to fitness measurements.
Withings	Response to DAR included links to various parts of Withings' privacy policy, which mention that "certain data" is collected when the user uses Withings applications: "Identity data", "Body metrics data", "Activity data" and "Cookies & Technical features". No explicit definition of what these categories refer to is present. In its email the Withings privacy officer said he would respond to any additional questions not answered in the policy.
Xiaomi	[No substantive response to DAR]
Garmin	[No response to DAR]
Mio	[No response to DAR]

Question 10: IP address logs associated with me, my devices, and/or my account (e.g. IP addresses assigned to my devices/router, IP addresses or domain names of sites I visit and the times, dates, and port numbers)

Company	2016
Apple	Apple's provided data included a wide range of cases where IP addresses were logged, (related to other Apple products and services — such as iTunes downloads), but nothing explicitly tied to fitness records was found.
Basis	"Basis does not track which IP addresses are used by you, your devices, or accounts."
Bellabeat	Bellabeat indicated it would provide access to data records in a subsequent response, but never followed through.
Fitbit	Timestamped IP address logs were included, with over 27,000 records spanning 5 months provided. Records existed for 176 unique dates. On dates with records, an average of 157 records were present. The records began the day the user first paired their Fitbit, indicating retention since account creation.
Jawbone	Data provided by Jawbone's export tool pertained exclusively to fitness measurements. No IP addresses were mentioned in the DAR response letter nor provided in the data export.
Withings	Response to DAR included links to various parts of Withings' privacy policy, which mention that "certain data" is collected when the user visits the Withings website or use Withings applications, one of which is noted as "Cookies & Technical features". No explicit definition of what "technical features" include is present. In its email the Withings privacy officer said he would respond to any additional questions not answered in the policy.
Xiaomi	[No substantive response to DAR]
Garmin	[No response to DAR]
Mio	[No response to DAR]

Question 11: Disclosures to third parties Any information about disclosures of my personal information, or information about my account or devices, to other parties, including law enforcement and other state agencies

Company	2016
Apple	No more information provided other than response to Question 3
Basis	No more information provided other than response to Question 3
Bellabeat	“The data collected from the LEAF (number of steps taken and sleep records) have not been provided to any 3rd parties nor will it be. Prior to any data disclosure, all users will be informed and explicitly asked for permission on sharing their data.”
Fitbit	No more information provided other than response to Question 3
Jawbone	No more information provided other than response to Question 3
Withings	“I would like to underline that we do not share any personal informatio n with any third Party without your prior and freely given consent. It is indeed essential for us to obtain your prior agree ment when data which can identify you are shared. (unless when obliged by law or if such data sharing is absolutely nec essary to provide you with a service you previously requested).”
Xiaomi	[No substantive response to DAR]
Garmin	[No response to DAR]
Mio	[No response to DAR]

Question 12: Subscriber information that you store about me, my devices, and/or my account

Company	2016
Apple	Provided a PDF called accountDetails.pdf that included a large amount of personally identifiable information including first name, last name, postal address, phone number, email address, registration IP address
Basis	Basis indicated it would provide access to data records in a subsequent response, but never followed through.
Bellabeat	Bellabeat indicated it would provide access to data records in a subsequent response, but never followed through.
Fitbit	Provided access to a Google Sheets document that, under a tab called “User info”, included email address, user account creation date, birth year, and information about the type of Fitbit device used, when the device was first paired and last used
Jawbone	In its response, directed the requester to download their data through an online portal. Data export was structured as a time-based activity log, with no subscriber information provided. Basic personal data present included the user’s age in years (to 15 decimal points of precisio, eg 2*3.505464480874316*) on the particular date for each row in the spreadsheet.
Withings	In its response, directed the requester to use their data export tool, which outputted several CSV spreadsheet files outlining activity records, but no basic subscriber information appeared to be present. The company also invited the requester to send in a written request if the requester wished to have Withings “manually provide” a copy of the data, which didn’t make clear whether or not additional data would be provided using such a process.
Xiaomi	[No substantive response to DAR]
Garmin	[No response to DAR], data export tool provides fitness activity records only.
Mio	[No response to DAR]

Online Dating Companies

Question 1: Can you clarify whether my data, either in an individualized data set or part of an aggregate data set, has been provided to other parties?

Company	2016
Grindr	* No response to this question
OKCupid	* yes, information shared with company's service providers and other Match Group businesses; full listing of specific companies not provided * if made purchases or clicked on advertisements then personal information was shared with business partners at the time(s) of those transaction(s) * aggregated information is shared with other third parties "for various purposes" but does not need to be provided to customer on basis that doesn't meet definition of personal information
Scruff	
Tinder	* yes, information shared with company's service providers and other Match Group businesses; full listing of specific companies not provided * if made purchases or clicked on advertisements then personal information was shared with business partners at the time(s) of those transaction(s) * aggregated information is shared with other third parties "for various purposes" but does not need to be provided to customer on basis that doesn't meet definition of personal information

Question 2: And if my information has been provided (either voluntarily, as part of a commercial transaction, or on other grounds) please identify to which parties it has been provided.

Company	2016
Grindr	* No response to this question
OKCupid	* to service providers: those who fulfil orders, provide customer service, marketing assistance, perform sales and business analysis, ad tracking and analytics, member screenings, credit processing services * to business providers: when you make a purchase or click through advertisements on third party websites and applications then the company many share your personal information with the other organization. * Other Match Group organizations: may share information with Tinder, OurTime.com, BlackPeopleMeet.com, Twoo, POF, Meetic, FriendScout24, Match and HowAboutWe. Shared information may include your profile and personal information such as your name and contact information, photos, interests, activities and transactions on our website, with Match Group companies. As part of our online service, your profile may be registered on and/or appear in search results or other areas of other online dating websites owned by the Match Group. Each Match Group company complies with its Privacy Policy
Scruff	
Tinder	* to service providers: those who fulfil orders, provide customer service, marketing assistance, perform sales and business analysis, ad tracking and analytics, member screenings, credit processing services * to business providers: when you make a purchase or click through advertisements on third party websites and applications then the company many share your personal information with the other organization. * Other Match Group organizations: may share information with Tinder, OurTime.com, BlackPeopleMeet.com, Twoo, POF, Meetic, FriendScout24, Match and HowAboutWe. Shared information may include your profile and personal information such as your name and contact information, photos, interests, activities and transactions on our website, with Match Group companies. As part of our online service, your profile may be registered on and/or appear in search results or other areas of other online dating websites owned by the Match Group. Each Match Group company complies with its Privacy Policy

Question 2: I wanted to understand a bit more about how my data could be disclosed to government authorities. What are your specific policies, practices, or processes for handling requests from authorities from international jurisdictions, such as from Canadian policing organizations? How would you respond if my information was requested as evidence in a Canadian civil or criminal proceeding?

Company	2016
Grindr	* information solely disclosed after receiving subpoena
OKCupid	* disclose information following reception of valid subpoena, court order, warrant or similar investigative demand from a government agency with jurisdiction to make the demand * Canadian organizations will receive information pursuant to MLAT or letters rogatary * also response to LEA requests when believe request is in relation to: connection with efforts to investigate, prevent, or take other action regarding illegal activity, suspected fraud or other wrongdoing; to protect and defend the rights, property or safety of our company, our users, our employees, or others; to comply with applicable law or cooperate with law enforcement; or to enforce our website terms and conditions or other agreements or policies
Scruff	
Tinder	* disclose information following reception of valid subpoena, court order, warrant or similar investigative demand from a government agency with jurisdiction to make the demand * Canadian organizations will receive information pursuant to MLAT or letters rogatary * also response to LEA requests when believe request is in relation to: connection with efforts to investigate, prevent, or take other action regarding illegal activity, suspected fraud or other wrongdoing; to protect and defend the rights, property or safety of our company, our users, our employees, or others; to comply with applicable law or cooperate with law enforcement; or to enforce our website terms and conditions or other agreements or policies

Question 3: Is the data transmitted between the application of yours that I have installed and your servers secured against potential eavesdroppers?

Company	2016
Grindr	* company non-responsive to this question
OKCupid	* assert take “appropriate security measures” to help safeguard personal information but “although we take steps to secure your information, we do not promise, and you should not expect, that your personal information, searches, or other communications will always remain secure. You should take care with how you handle and disclose your personal information online.”
Scruff	
Tinder	* assert take “appropriate security measures” to help safeguard personal information but “although we take steps to secure your information, we do not promise, and you should not expect, that your personal information, searches, or other communications will always remain secure. You should take care with how you handle and disclose your personal information online.”

Question 4: Geolocation data collected about me, my devices, and/or my account

Company	2016
Grindr	* geographical location of the last place a user used the app
OKCupid	* OkCupid collects geolocation data for the purpose of providing you with matches in your area, and it collects information about the devices you use to log in to your account for the purpose of sending you push notifications. * despite above answer, company asserts its possessed no geolocation information for one customer (who used a desktop web interface) and did for another (who used the mobile application and so GPS information was collected and retained)
Scruff	
Tinder	* We automatically collect information from your device when you visit our service. This information could include your IP address, device ID and type, your browser type and language, the operating system used by your device, access times, your mobile device's geographic location while our application is actively running, and the referring website address.

Question 5: Any additional kinds of information that you have collected, retained, or derived from the mobile or website services you provide, including by not limited to: data or records collected using my camera or from my camera roll; social networking information; data collected or retained derived from my microphone; or communications between myself and other users; contact book information

Company	2016
Grindr	* in some cases will possess chat messages
OKCupid	* OKCupid only collects photos that are uploaded to a customer's profile; the company does not collect audio or video recordings * retains all photos ever uploaded, even if deleted from public profile * retains logs of communications; only provides the customers' own communications and not those of whomever they have spoken with * did not possess information concerning the customer's devices * did not possess information about the customers' user-agent when they signed up
Scruff	
Tinder	* OKCupid only collects photos that are uploaded to a customer's profile; the company does not collect audio or video recordings

Question 6: Lifestyle information that you may have about me, such as drinking habits or sexual preference information.

Company	2016
Grindr	* only possess insofar as it's denoted in user's Grindr profile
OKCupid	* Only the information that you post on your profile or share with others on our site, and information that other OkCupid users may post about you.
Scruff	
Tinder	* Only the information that we collect from your public Facebook profile, consistent with your privacy settings in Facebook, plus information that you post on your profile or share with others on our service. We may also collect this information from other Match Group companies, as stated in our privacy policy.

Question 7: Personally identifying information that is unique to me, my devices, and/or my account, such as name, email addresses, phone numbers, responses to relationship questions, or device identifiers;

Company	2016
Grindr	* email address, subscription purchase information (unclear if includes payment information); information associated with a user's profile, "Information related to the user's Grindr profile"
OKCupid	* information that was provided was listed as 'basic information' and included previously under subscriber data question
Scruff	
Tinder	* does not specify. Asserts that information that is publicly shared with Tinder and is accessible via UI is outside of scope of a PIPEDA request

Question 8: Mobile app data Information collected about me, or persons/ devices associated with my account, using one of your company's mobile device applications

Company	2016
Grindr	* nothing mentioned, but company required a subpoena before fully providing information about what it collects
OKCupid	* information not mentioned in logs
Scruff	
Tinder	* see earlier response concerning mobile information

Question 9: IP address logs associated with me, my devices, and/or my account (e.g. IP addresses assigned to my devices/router, IP addresses or domain names of sites I visit and the times, dates, and port numbers)

Company	2016
Grindr	* no mention of retaining this information, though fulsome request would have required a subpoena from LEA
OKCupid	* retains all IP addresses from all logins
Scruff	
Tinder	* does not specify. Asserts that information that is publicly shared with Tinder and is accessible via UI is outside of scope of a PIPEDA request * does not clarify the time forwhich IP address information is retained

Question 10: Subscriber information that you store about me, my devices, and/or my account

Company	2016
Grindr	* email address, subscription purchase information (unclear if includes payment information); information associated with a user's profile, "Information related to the user's Grindr profile"
OKCupid	* basic information includes: name, userId, email address, join date, login count, birth date, gender, orientation, age, education, location (unclear how precise because of redactions), Spamadmin approved, account level, moddate, delete reason
Scruff	
Tinder	* does not specify. Asserts that information that is publicly shared with Tinder and is accessible via UI is outside of scope of a PIPEDA request

Telecom Companies

Question 1: Call logs E.g. numbers dialed, times and dates of calls, call durations, routing information, and any geolocational or cellular tower information associated with the calls)

Company	2016	2014
Bell	* company collects call logs when making or receiving a communication * Bell Canada (i.e. not Mobility) does not generally keep call logs of local calls, though does for long-distance calls * no mention of retention periods	
Fido	* retain text message details and call log details for 13 months * information associated with the aforementioned mobile logs include: times, dates, area information, and cellular tower information/coordinates * maintains separate CDR and VoLT CDR records * outbound calls available on bill, and can see past 18 months online. Available at $15/month if on paper billing * Do not provide incoming calls for privacy reasons * Call routing not classified as personal information * did not provide full retention periods in initial requests; full retention for all items not provided in followups	* Outbound calls available on bill, and can see past 18 months online. Available at $15/month if on paper billing. * Do not provide incoming calls for privacy reasons. * Call routing not classified as personal information * did not provide full retention periods
Koodo		* retain records of telephone numbers, dates, an durations of incoming and outgoing cellular calls “for a limited period of time.” * retained information is for network management and billing * copies of customer bills for approximately seven years
NorthwestTel		* retains detailed call logs for all long distance calls charged to customer, but since this information is provided on bills the company declined to provide information. * does not state retention period

Company	2016	2014
Primus		* N/A for customer who provided records
Rogers	* Outbound calls available on bill, and can see past 18 months online. Available at $15/month if on paper billing. * Do not provide incoming calls for privacy reasons. * Call routing not classified as personal information	* Outbound calls available on bill, and can see past 18 months online. Available at $15/month if on paper billing. * Do not provide incoming calls for privacy reasons. * Call routing not classified as personal information * After followup, noted that call logs are noted on bills and bills are retained for 7 years. Such logs "identify the community within which you place an outbound call and received an inbound call."
Shaw	* archive of outbound calls are accessible at a rate of $250/year requested * Does not consider routing information to be personal information * Does not possess cell tower or geolocation information associated with calls because does not offer a mobile service	
TekSavvy		* customer who provided us with information does not have phone service and, thus, no such logs are maintained for the customer
TELUS		
Virgin		
Wind	* company notes that there is a rolling 90 period that customers can access their log and record of calls and SMS/MMS for 90 days. * company does not indicate its own retention period for records	

Question 2: Mobile app data Information collected about me, or persons/ devices associated with my account, using one of your company's mobile device applications

Company	2016	2014
Bell	* company asserts that, "We retain very little information relating to viewing behavior at an individual level, beyond what is required for billing." * company is non-specific about what these other kinds of information might be, nor how long it would be retained for	
Fido	* session information to communicate with Fido' servers. This sometimes includes email address, IP address, and Universally Unique Identifier (UUID) * session data is deleted when logging out of the app * all settings are deleted when uninstall application	* company responded with N/A
Koodo		* no information provided from customer; unsure if in original message from company to customer
NorthwestTel		* company does not use mobile device applications to collect customers' information
Primus		* N/A for customer who provided records
Rogers	* session information to communicate with Rogers' servers. This sometimes includes email address, IP address, and Universally Unique Identifier (UUID) * session data is deleted when logging out of the app * all settings are deleted when uninstall application	
Shaw	* collects MAC addresses of devices registered as media streaming devices, and thus qualify for FreeRangeTV	
TekSavvy		* the company does not provide such an application and thus does not have information that is responsive to this question

Company	2016	2014
TELUS		
Virgin		
Wind	* company had not collected such information about the customer at time of request	

Question 3: Geolocation data collected about me, my devices, and/or associated with my account (e.g. GPS information, cell tower information)

Company	2016	2014
Bell	* company does not collect geolocation information unless a subscriber sends or receives a communication in a particular location	
Fido	* company states it does not collect geo-locational information unless you have sent or received a phone call or SMS	* Geolocation information not collected save for when make or receive a phone call or SMS.
Koodo		* company does not "currently retain records of customers' satellite GPS location" but if customer phone has GPS capability the company "may be able to determine the location of that device in real time. This may be undertaken in response to a court order or to assist service providers in locating a customer's device." * company also notes that it retained records of communications sent and received by customers; such information includes locations of the cell towers that handled communications. Such records "are retained for limited periods of time for the purposes of network management". * cell towers can be used to determine the approximate location of a mobile device in the "recent past" * specific retention periods are not provided for how long such geolocation-related information is retained * to another customer, verbally informed them that can only access GPS information in real-time, and would only do so in response to a court order to provide real-time GPS information. Otherwise they do not collect or retain this information
NorthwestTel		* company does not collect geolocation information about its customers
Primus		* N/A for customer who provided records

Company	2016	2014
Rogers	* Geolocation information not collected save for when make or receive a phone call or SMS.	* Geolocation information not collected save for when make or receive a phone call or SMS. * Amended in followup to "[t]he business does not retain records of the cell sites accessed by your wireless device **for any length of time,** other than when a wireless phone call or SMS (short messaging service) is completed"
Shaw	* geolocation information is used to identify service areas for media streaming services and for nearby WiFi hotspot locations * geolocation information is not associated with a given account or customer and is retained for statistical purposes only	
TekSavvy		* the company does not provide services capable of GPS or cell tower-based locational information. * the company's routing tables indicate which neighbourhood an IP address is assigned, but no more granular information is available short of looking up a service address
TELUS		
Virgin		
Wind	* company "not collect GPS information on a per customer, device or account basis other than as required to do so in response to E911 calls and under certain conditions, geo-location information is obtained (including GPS under certain conditions) and provided to the Public Safety Answering Point, in compliance with the E911 Phase II CRTC regulatory policy. WIND has not collected any such geolocational information as described above."	

Question 4: IP address logs associated with me, my devices, and/or my account (e.g. IP addresses assigned to my devices/router, IP addresses or domain names of sites I visit and the times, dates, and port numbers)

Company	2016	2014
Bell	* company states it does not collect IP addresses or domain names of sites visited, or the dates, times, or port numbers * not easy for the company to provide the history of IP addresses assigned to a customer and, if they would like that information, contact Bell and the company will determine costing for such a request	
Fido	* retains IP addresses assigned to wireless devices for 7 days, and only releases them pursuant to a court order * retains IP addresses assigned to modems for 13 months. * Do not collect the IP address or domain names that customer visited, or the times, dates, or port numbers * IP addresses assigned to devices are not readily available; must specify times and will be provided at cost	* Do not collect IP addresses or domain names that customer visited, or the times, dates, or port numbers * IP addresses assigned to devices are not readily available; must specify times and will be provided at cost
Koodo		* company retains IP address that customers “use or connect to for a limited period of time for network management purposes.” * company does not specify for how long data is retained * upon customer request, company stated it would take approximately 60 hours at $20/hour (totalling $1,200) to retrieve the logs of IP addresses associated with their device * sample IP logs retained include: date, source IP, source port, destination IP, destination port

Company	2016	2014
NorthwestTel		* Maintains a log of IP addresses linked with modem MAC numbers but cannot in same system link either the IP address or MAC with a subscriber name; a separate system binds the MAC with an account number, and that number is bound to a customer name * no indication of how long any of this information is retained
Primus		* DSL history, with associated IP addresses, provided * kept for 1 year
Rogers	* Do not collect IP addresses or domain names that you've visited, or the time, dates, and port numbers. * IP logs of those assigned to devices not readily available; must specify time available and will be provided at cost	* Do not collect IP addresses or domain names that customer visited, or the times, dates, or port numbers * IP addresses assigned to devices are not readily available; must specify times and will be provided at cost
Shaw	* Does not collect IP addresses or domain name that have been visited, or the time, dates, and port numbers * Archived histories of IP addresses associated with devices are available for $250/year per modem searched * Shaw keeps a record of a customer's MAC address when individuals connect to the Shaw Go WiFi networks	
TekSavvy		* company retains data for 30 days following the end of an IP address lease to either a modem (which is itself associated with a customer account) or a customer account directly (in the case of DSL customers) * though the company could develop the capability to, it has not to date installed equipment to collect transmission information such as sites visited, times visited, dates visited, and relevant port numbers
TELUS		
Virgin		

Company	2016	2014
Wind	* no such logs collected on a per-device basis; they collect relevant information and aggregate it for billing purposes and those billing-related pieces of information are available through Wind's online portal * Wind does not provide publicly-addressable IP addresses and, thus, metadata collected cannot be directly mapped to visits to specific Internet URLs * network equipment (e.g. firewalls, DNS servers) can collect some information but follows Wind's data retention policy and adheres to industry best practices; such logging information may potentially be provided to LEAs * company declines to provide retention period for network equipment collections	

Question 5: Disclosures to third parties Any information about disclosures of my personal information, or information about my account or devices, to other parties, including law enforcement and other state agencies

Company	2016	2014
Bell	* stated would take company 30 days to determine from LEAs whether or not Bell could positively respond to question * did not note whether or not information was shared with non-governmental parties	
Fido	* information shared with Credit Bureau to establish account, and shares payment history each month * checked to see if personal information was shared with LEAs; records found that no request or disclosure was made for the customer's account number	* initially provided customer with a copy of sections of PIPEDA and, subsequently, asserted that in searching their records either no request had been made or Fido was not permitted to advise the customer of the disclosure
Koodo		* company states it only discloses information pursuant to its terms of service, Privacy Commitment, or with a valid court order or other applicable law * notes that under PIPEDA the company may be unable to disclose whether or not a customers' information has been shared with a state agency * company would positively inform a customer they had their information disclosed if it had been shared with a government agency *and* the agency approved of the disclosure; otherwise would hear nothing, regardless of whether information had never been shared or not
NorthwestTel		* company states that it had only disclosed a customers' information if pursuant to the company's privacy policy to disclose information when lawfully compelled to do so * did disclose PII to a credit agency * information was shared with former subsidiary, Northwestel Cable Inc
Primus		* response to customer was non-responsive on this point

Company	2016	2014
Rogers	* informed customer that no request/ disclose was made by a government agency for the account information * information is shared with credit bureau	* initially provided customer with a copy of sections of PIPEDA and, subsequently, asserted that in searching their records either no request had been made or Rogers was not permitted to advise the customer of the disclosure * On followup, company noted that it had not disclosed my information to another third-party company
Shaw	* gave an ambiguous response that information “has or has not” been shared to government agencies between 2013-2016. May have been a typo. * no mention of sharing information with other parties (e.g. credit bureaus or commercial actors)	
TekSavvy		* company asserted to customer that their data had not been shared with a government agency at the time the request was made * personal information was disclosed to the company that provides the customer with service (TekSavvy is an ISP that significantly relies on other parties’ services) *
TELUS		
Virgin		
Wind	* company has disclosed customer information to credit bureaus to conduct a credit check * notes that company may be restricted in its ability to disclose to subscribers whether their information has been shared with a government agency but, that no such disclosure had taken place with this customer	

Question 6: Text & multimedia messages (sent and received, including date, time, and recipient information)

Company	2016	2014
Bell	* company states it does not have access to, or information relating to, the content of messages * bills include information about incoming and outgoing text messages * no information concerning retention periods are provided	
Fido	* do not store the content of SMS or MMS messages * do not show itemized listing of messages on bills; will estimate costs on a per-month basis upon request	* do not store the content of SMS * do not show itemized listing of messages on bills; will estimate costs on a per-month basis upon request
Koodo		* disclosure under geolocation information indicated that transmission data for communications sent to, and received by, customers' device are retained for a period of time * do not retain number being texted * retention period is 150 days NOTE: this is based on aggregating two customers' responses
NorthwestTel		* does not collect text messages or multimedia messages sent or received by customers
Primus		* N/A for customer who provided records
Rogers	* do not store the content of SMS * do not show itemized listing of messages on bills; will estimate costs on a per-month basis upon request	* do not store the content of SMS * do not show itemized listing of messages on bills; will estimate costs on a per-month basis upon request * on followup, company stated it retained the non-content aspects of SMS messages (data of call, duration, number called, redirecting switch, switch, first cell, and last cell) for 13 months * copies of text messages, such as 5-9 sample records, would be provided at cost, with cost equaling $300/month of wireless subscription
Shaw	* no information is available because Shaw does not provide a service that includes SMS/MMS functionality	

Company	2016	2014
TekSavvy		* company does not provide a service offering that includes this data
TELUS		
Virgin		
Wind	* company notes that there is a rolling 90 period that customers can access their log and record of calls and SMS/MMS for 90 days. * company does not note its own retention period for this type of information	

Question 7: Subscriber information that you store about me, my devices, and/or my account

Company	2016	2014
Bell	* includes: customer name, that of authorized users of accounts, service and billing addresses, account numbers associated with different services, identification information such as date of birth, government identification, employer/employee status, other items concerning the services the customer subscribes to	
Fido	* included: name, address, phone number, account number, SIN, date of birth, email address	* included: name, address, phone number
Koodo		* included: SIM card number, EMEI, MSISDN * also: mailing address, name, contact number, date of birth, and SIN NOTE: this is based on two separate subscribers providing information. We have aggregated the information they were provided.
NorthwestTel		* included: name, mailing address, service address, telephone number, email address, account password (customer's date of birth) * also: notes of conversations and communications between customer and CSR representatives * trouble tickets and service orders
Primus		* included: date of birth, SIN, contact information, credit check results, account services provided, modem serial number, other hardware-related details
Rogers	* Included name, address, phone numbers associated with account, account number, credit card number, provincial ID, date of birth, email address	* included name, address, phone numbers associated with account, account number, credit card, date of birth, provincial ID
Shaw	* instructs customers to visit the online portal, where subscriber information is available. Does not clarify which elements, specifically, the company would classify as 'subscriber information'	

Company	2016	2014
TekSavvy		* included: name, address, service address, phone number, email address, usage information, and past bills * additional subscriber information inaccessible to the customer via the online portal includes: billing information, modem type, firmware, and MAC address, current billing cycle usage information, internal notes on file, including call logs
TELUS		
Virgin		
Wind	* included: name, address, birthdate * contact information included: home phone number, email address * device information included: MSISDN, WINDTAB, Device	

Question 8: Other Any additional kinds of information that you have collected, retained, or derived from the telecommunications services or devices that I, or someone associated with my account, have transmitted or received using your company's services

Company	2016	2014
Bell	* company states, "For voice communications, Bell does collect the contents of calls, records of the time and duration of the call and called number are retained for long distance calls for the purposes of billing" * company collects information pertaining to its Related Advertising Program (RAP) if opted into it. The RAP is based on mobile browsing * otherwise states, "We retain very little information relating to viewing behavior at an individual level, beyond what is required for billing." * retention periods are not provided for any of the above mentioned data types	
Fido	* company provided account notes	* company provided account notes
Koodo		* No additional information was provided by the customer in their summarized comments to us
NorthwestTel		* company "has not collected any other information that you have transmitted or received using our services."
Primus		* provided archives of all customer support screens from all service tickets the customer had submitted and their resolution. Tickets included information such as: no connect, disconnects, speed shortfalls, etc. * provided .pdfs of all invoices of customer who provided data, with invoices going back approximately 7 years

Company	2016	2014
Rogers	* capture account remarks made when communicating with the company, and are included for review	* capture account remains made when communicating with he company, and these are included for review * includes information associated with Rogers Phone Finder (name, mobile number, email address, name mobile user) * keeps copies of Finder lookups, and last 10 are available for viewing online * On followup, company noted that Finder lookups are kept in perpetuity and Rogers Alerts related information retained since September 2013 onwards.
Shaw	* no additional information is specified, though CSR logs are available online	
TekSavvy		
TELUS		
Virgin		
Wind	* company states that, “There are no such additional kinds of information so collected, retained or derived.”	